

September 30, 2025

Teresa Badiukiewicz  
Hernando Schools  
919 North Broad Street  
Brooksville, FL 34601

Dear Ms. Badiukiewicz

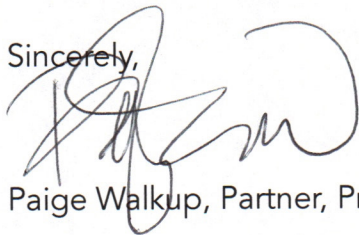
Please find attached the completed DSA agreement for execution on the District side. In accordance with Section 5.3 and based on discussions with the DSA provider David Sallay (4 Access 4 Learning Community) please see enclosed:

- Hubspot Security Overview
- Hubspot 2025 SOC 3 Type 2 Security Report
- Hubspot Compliance FAQs
- FTP Server Security Diagram
- Cyber Security Coverage

These documents address all security parameters required by the District. Additionally, we have completed the data sharing forms to identify the data that will be stored in both HubSpot and our secure FTP server as requested by the DSA requirements.

Please let us know if you have any questions or need additional information. I can be reached at [paige@caissaps.com](mailto:paige@caissaps.com) or at 901.832.5687.

Sincerely,



Paige Walkup, Partner, President

Caissa Public Strategy



# STANDARD STUDENT DATA PRIVACY AGREEMENT

(Florida National Data Privacy Agreement (NDPA) Standard VERSION 2)



And



Version 2

***Authored by Members of the Student Data Privacy Consortium (SDPC) &***

***Mark Williams, Fagen, Friedman & Fulfrost LLP***

Approved as to form & content for HCSD: Kevin M. Sullivan Attorney, BGR&H 2:16 pm, Sep 04, 2024
---

© Access 4 Learning (A4L) Community. All Rights Reserved.

*This document may only be used by A4L Community members and may not be altered in any substantive manner.*

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between:

[ \_\_\_\_\_ ],

located at [ \_\_\_\_\_ ] (the “LEA”)

and

[ \_\_\_\_\_ ],

located at [ \_\_\_\_\_ ] (the “Provider”).

## PREAMBLE

**WHEREAS**, the Provider is providing educational or digital Services, as defined in Exhibit “A”, to LEA, which Services may include: (a) cloud-based Services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

**WHEREAS**, the Provider and LEA have entered into a Service Agreement (as defined herein), to provide certain Services to the LEA as set forth in the Service Agreement, and this DPA (collectively the “Agreement”),

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment (“PPRA”) at 20 U.S.C. 1232h; and the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. 6501-6506 (16 C.F.R. Part 312),

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

### *General Offer of Privacy Terms.*

The Provider has signed Exhibit “E” to the SDPC Standard Clauses, otherwise known as “General Offer of Privacy Terms” enabling other LEAs to enter into the same terms of this DPA with Provider.

### *Special Provisions. (Check if Required)*

☐ If checked, the Supplemental State Terms attached hereto as Exhibit “G” are hereby incorporated by reference into this DPA in their entirety.

*If the Parties desire to change any terms, use the ‘Vendor-Specific’ Agreement or ‘District-Modified’ Agreement.*

The **designated representative for the LEA** for this DPA is:

Name: Ray Pinder Title: Superintendent  
Address: 919 N. Broad Street, Brooksville, FL 34601  
Phone: (352) 797-7001 Email: pinder\_r@hcsb.k12.fl.us

The **designated representative for the Provider** for this DPA is:

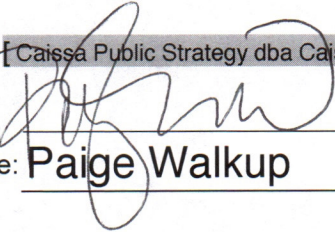
Name: Paige Walkup Title: President  
Address: 5100 Poplar Avenue Suite 1720 Memphis, TN 38137  
Phone: 901.522.1030 Email: paige@caissaps.com

**IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.**

**LEA:** [ Hernando County School Board ]

Signed By: \_\_\_\_\_ Date: \_\_\_\_\_  
Printed Name: Ray Pinder Title/Position: Superintendent

**PROVIDER:** [ Caissa Public Strategy dba Caissa K12 (Caissa K12) ]

Signed By:  \_\_\_\_\_ Date: 09.30.2025  
Printed Name: Paige Walkup Title/Position: President

Each Party is responsible to promptly notify the other Party of changes to the notice information.

**Notices to Provider**

[ Caissa Public Strategy dba Caissa K12 (Caissa K12) ]  
[ Student Recruitment and Communications ]  
[ 5100 Poplar Avenue, Suite 1720 Memphis, TN 38137 ]  
[ paige@caissaps.com ]

With a copy to (if provided):

[ Provider Legal Counsel ]  
[ Provider Legal Counsel Postal Address ]  
[ Provider Legal Counsel Email Address ]

**Security Notices to Provider** (Required per Section 5.3)

[ Paige Walkup and Jackson Connors ]  
[ President and IT Director ]  
[ 5100 Poplar Avenue, Suite 1720 Memphis, TN 38137 ]  
[ paige@caissaps.com jackson@caissaps.com ]

**Notices to LEA**

[ Hernando County School Board ]  
[ Superintendent ]  
[ 919 N. Broad Street, Brooksville, FL 34601 ]  
[ pinder\_r@hcsb.k12.fl.us ]

With a copy to (if provided):

[ Caroline Mockler, Esq. ]  
[ 919 N. Broad Street, Brooksville, FL 34601 ]  
[ mockler\_c@hcsb.k12.fl.us ]

**Security Notices to LEA** (Required per Section 5.3)

[ Joseph G. Amato ]  
[ Director of Technology and Information Services ]  
[ 919 N. Broad Street, Brooksville, FL 34601 ]  
[ amato\_j1@hcsb.k12.fl.us ]

## STANDARD CLAUSES

### ARTICLE I: PURPOSE AND SCOPE

#### 1.1 Purpose of DPA.

The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing Services otherwise provided by the LEA. With respect to its use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA as set forth in this DPA and the Service Agreement.

#### 1.2 Description of Products and Services.

A description of all products and services covered by the Agreement, and information specific to this DPA, are listed in Exhibit "A". If a Provider needs to update any information on Exhibit "A" (such as updating with new provided services), they may do so by completing the Addendum template provided by the A4L Community and sending a copy to the LEA.

Provider may add or delete products or services subject to this DPA under the following circumstances:

1. Deleted products or services: The products or services have been discontinued and are no longer available from the Provider.
2. Added products or services: The added products or services are either:
  - a. a direct replacement, or substantially equivalent to the original products or services listed in the DPA, or
  - b. the added products or services result in enriched new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed.

If an added product or service requires additional Data Elements, Provider must complete the relevant portion of the Addendum template to update Exhibit "B".

Provider may not make any change to Exhibit "A" via an Addendum, except adding or deleting products or services. LEA is under no obligation to acquire added products or services, and has no ability under the DPA to prevent deletion of products or services. Subject to the limitations in this section, an Addendum is automatically incorporated into this DPA when LEA is notified by Provider, in accordance with the notification provisions of this DPA, of the Addendum's existence and contents.

#### 1.3 Student Data to Be Provided.

In order to perform the services, the Provider shall process Student Data as identified by the Provider in the Schedule of Data, attached hereto as Exhibit "B". Student Data may be provided by the LEA or created by students, as set forth fully in the definition of Student Data in Exhibit "C". If a Provider needs to update any information on Exhibit "B", they may do so by completing the Addendum template provided by the A4L Community and sending a copy to the LEA.

Provider may delete data elements from Exhibit "B" if they are no longer used by the Provider.

Provider must add data elements to Exhibit “B”, when a material change has occurred, regardless of whether the added data elements are either one of the following:

1. used to better deliver the original products or services listed in the DPA, or
2. used to deliver added products or services that result in new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed. Such new products or services must be designated in the Addendum template as changes to Exhibit “A”.

The Provider must notify the LEA, in accordance with the notification provisions of this DPA, of the existence and contents of an Addendum modifying Exhibit “B”. The LEA will have thirty (30) days from receipt to object to the Addendum. If no written objection is received it will become incorporated into the DPA between the parties.

#### **1.4 DPA Definitions.**

Capitalized terms used in this DPA shall have the meanings set forth in Exhibit “C”. With respect to the treatment of Student Data, in the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to, the Service Agreement.

## **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

### **2.1 Student Data Property of LEA.**

As between LEA and Provider, all Student Data processed by the Provider, or created by students (as set forth fully in the definition of Student Data in Exhibit “C”), pursuant to the Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data processed by the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA.

### **2.2 Parent, Legal Guardian and Student Access.**

The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student (as defined in FERPA) may review Student Data and request deletion or modification, and request delivery of a copy of the Student Data. In support of this, the Provider shall establish reasonable procedures by which the LEA may access, and correct if necessary, Education Records and/or Student Data, and make a copy of the data available to the LEA or (at the LEA’s direction) to the parent, legal guardian or eligible student directly. If the LEA is not able to review or update the Student Data itself, Provider shall respond in a reasonably timely manner (and no later than thirty (30) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent, legal guardian or student, whichever is sooner) to the LEA’s request for Student Data held by the Provider to view or correct as necessary.

In the event that a parent or legal guardian of a student or eligible student contacts the Provider to correct, delete, review or request delivery of a copy of any of the Student Data collected by or generated through the Services, the Provider shall refer that person to the LEA, who will follow the necessary and proper procedures regarding

the requested information. In the event that any person other than those listed contacts the Provider about any Student Data, the Provider shall refer that person to the LEA, except as provided in Section 4.4.

- 2.2.1 This NDPA does not impede the ability of students to download, export, or otherwise save or maintain their own Student Generated Content directly from Provider or for Provider to provide a mechanism for such download, export, transfer or saving to students, or the student's parent or legal guardian. Nor does it impede the ability of Providers to offer LEAs features to allow such ability.
- 2.2.2 In the event that Student Generated Content is transferred to the control of the student, parent or legal guardian, the copy of such Student Generated Content that is in the control of such person is no longer considered Student Data.

### **2.3 Subprocessors.**

Provider shall enter into a Subprocessor Agreement with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA. Every Subprocessor Agreement must provide that the Subprocessor will not Sell the Student Data. The terms of a Subprocessor Agreement shall not be materially modified by the Subprocessor unless notice is provided to the Provider.

## **ARTICLE III: DUTIES OF LEA**

### **3.1 Provide Data in Compliance with Applicable Laws.**

LEA shall use the Services and provide Student Data in compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time.

### **3.2 Annual Notification of Rights.**

If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.

### **3.3 Reasonable Precautions.**

LEA shall employ administrative, physical, and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure, or acquisition by an unauthorized person.

### **3.4 Unauthorized Access Notification and Assistance.**

LEA shall notify Provider within seventy-two (72) hours of any confirmed Data Breach to the Services, LEA's account or any Student Data that poses a privacy or security risk. If requested by Provider, LEA will provide reasonable assistance to Provider in any efforts by Provider to investigate and respond to such Data Breach.

## ARTICLE IV: DUTIES OF PROVIDER

### 4.1 Privacy and Security Compliance.

The Provider shall comply with all laws and regulations applicable to Provider's protection of Student Data privacy and security, and at the direction of the LEA shall cooperate with any state or federal government initiated audit of the LEA's use of the Services.

### 4.2 Authorized Use.

The Student Data processed pursuant to the Services shall be used by the Provider for no purpose other than performing the Services outlined in Exhibit "A", or as instructed by the LEA.

### 4.3 Provider Employee Obligation.

Provider shall require all of Provider's employees who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee with access to Student Data pursuant to the Service Agreement.

### 4.4 No Disclosure.

Provider acknowledges and agrees that it shall not sell or disclose any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data.

#### 4.4.1 Exceptions to No Disclosure.

- 4.4.1.1 This prohibition against disclosure will not apply to Student Data where disclosure is directed or permitted by the LEA or this DPA.
- 4.4.1.2 The provision to not sell Student Data shall not apply to a Change of Control.
- 4.4.1.3 This prohibition against disclosure shall not apply to Student Data disclosed pursuant to a judicial order or lawfully issued subpoena or warrant.
- 4.4.1.4 This prohibition against disclosure shall not apply to Student Data disclosed to Subprocessors performing Services on behalf of the Provider pursuant to this DPA.
- 4.4.1.5 Should law enforcement or other government entities ("Requesting Party(ies)") provide a judicial order or lawfully issued subpoena or warrant to the Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party.
- 4.4.1.6 Notification under 4.4.1.5 is not required if the judicial order or lawfully issued subpoena or warrant states not to inform the LEA of the request.
- 4.4.1.7 Should the LEA be presented with a judicial order or lawfully issued subpoena or warrant to disclose Student Generated Content or other Student Data, the Provider shall cooperate with the LEA in delivering such data.

- 4.4.1.8 This prohibition against disclosure shall not apply to LEA-authorized users of the Services, which may include parents and legal guardians.
- 4.4.1.9 This prohibition against disclosure shall not apply to protect the safety of users or others, if and only if, an LEA employee who has specifically been authorized to declare a health or safety emergency has done so and all requirements under 34 CFR §§ 99.31(a)(10) and 99.36 have been fulfilled by the LEA.
- 4.4.1.10 This prohibition against disclosure shall not apply to protect the integrity or security of the Service, where such disclosure is made to a Subprocessor engaged by Provider for the specific purpose of investigating a potential Data Breach as set forth in 5.4.

## 4.5 De-Identified Data

Provider agrees not to attempt to re-identify De-Identified Student Data without the written direction of the LEA. De-Identified Student Data may be used by the Provider for those purposes allowed under applicable laws, for the purposes allowed for the processing of Student Data under this DPA, as well as the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research, development, and improvement of the Provider's educational sites, Services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Student Data shall survive termination of this DPA or any request by LEA to return or dispose of Student Data. Except for Subprocessors, Provider agrees not to transfer De-identified Student Data to any third party unless the transfer is expressly directed or permitted by the LEA or this DPA. Such Subprocessors must be subject to equivalent terms of the DPA including this one. Prior to publishing any document that names the LEA, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Student Data is presented. If Provider chooses to create De-Identified Data, its process must comply with either NIST de-identification standards or US Department of Education guidance on de-identification.

## 4.6 Disposition of Data.

Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree.

If the Provider has a standard retention and destruction schedule, that schedule shall apply to Student Data as long as this DPA is active. The Provider's practice relating to retention and disposition of Student Data shall be provided to the LEA upon request.

At the termination of this DPA, the Provider shall, unless directed otherwise by the LEA, dispose of, or delete Student Data obtained by the Provider under the Agreement within sixty (60) days of termination (unless otherwise required by law). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted when directed or permitted by the LEA, according to Provider's standard destruction schedule, or as otherwise required by law. The LEA may provide the Provider with special instructions for the disposition of the Student Data, by transmitting to Provider Exhibit "D", attached hereto. The duty of the Provider to dispose of or delete Student Data shall not extend to De-Identified Data or to Student-Generated Content that has been transferred or kept pursuant to Section 2.2.2.

## **4.7 Advertising Limits.**

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA; or (c) for any commercial purpose other than to provide the Service to the LEA, or as authorized by the LEA or the parent/guardian. Targeted Advertising is strictly prohibited. However, this section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to account holders that are not considered Targeted Advertising (this exception does not apply where the Provider is relying on the LEA to provide consent on behalf of the parent under COPPA); or (iii) to notify account holders about new education product updates, features, or Services that are not considered Targeted Advertising or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

Before making product recommendations under section (ii) above, Provider must disclose the existence of those recommendations to LEA in writing, in sufficient detail that LEA can fulfill any obligations under applicable law (e.g. PPRA).

# **ARTICLE V: DATA SECURITY AND BREACH PROVISIONS**

## **5.1 Data Storage.**

If Student Data is stored outside the United States, Provider will provide a list of Countries where data is stored, in Exhibit "B".

## **5.2 Security Audits.**

Provider will conduct a security audit or assessment no less than once per year, and upon a Data Breach. Upon 10 days' notice and execution of confidentiality agreement, Provider will provide the LEA with a copy of the audit report, subject to reasonable and appropriate redaction.

## **5.3 Data Security.**

The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security of Student Data. The Provider shall implement an adequate Cybersecurity Framework that incorporates one or more of the nationally or internationally recognized standards set forth in Exhibit "F". Additionally, Provider may choose to further detail its security programs and measures in Exhibit "F". Provider shall provide, in the Preamble to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

## **5.4 Data Breach.**

In the event that Provider confirms a Data Breach, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the Data Breach, unless notification within these time limits would disrupt investigation of the Data Breach by law enforcement. In such an event, notification shall be made within a reasonable time after the Data Breach. Provider shall follow the following process:

- (1) The Data Breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
  - (a) The name and contact information of the Provider subject to this section,
  - (b) the date of the notice,
  - (c) the date of the Data Breach, the estimated date of the Data Breach, or the date range within which the Data Breach occurred,
  - (d) Whether the notification was delayed as a result of a law enforcement investigation, if legally permissible to share that information,
  - (e) A general description of the Data Breach, if that information is possible to determine at the time the notice is provided,
  - (f) A description of the Student Data reasonably believed to have been the subject of the Data Breach; and
  - (g) Identification of impacted individuals.
- (2) Provider agrees to adhere to all applicable federal and state laws with respect to a Data Breach related to the Student Data, including any required responsibilities and procedures for notification and mitigation of any such Data Breach.
- (3) Provider further acknowledges and agrees to have a written Data Breach response plan that is consistent with applicable industry standards and federal and state law for responding to a Data Breach, involving Student Data and agrees to provide LEA, upon reasonable written request, with a summary of said written Data Breach response plan.
- (4) LEA shall provide notice and facts surrounding the Data Breach to the affected students, parents, or guardians.
- (5) In the event of a Data Breach originating from LEA's use of the Service or otherwise a result of LEA's actions or inactions, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data and may request costs incurred as a result of such Data Breach.

## CONTRACT TERMS

**Term and Termination.** In the event that either Party seeks to terminate this DPA, they may do so by written notice if the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Service Agreement or contract if the other party breaches any terms of this DPA. This DPA shall stay in effect for as long as the Provider retains the Student Data, as set forth in section Article IV, Section 4.6. In the case of a “Change of Control” the LEA has the authority to terminate the DPA if it reasonably believes that the successor cannot uphold the terms and conditions herein or having a contract with the successor would violate the LEA’s policies or state or federal law.

**Data Disposition on Service Agreement Termination.** If the Service Agreement is terminated, the Provider shall dispose of all of LEA’s Student Data pursuant to Article IV, Section 4.6 of the Standard Clauses.

**Notices.** All notices or other communication required or permitted to be given hereunder must be made in writing and may be given via e-mail transmission, or first-class mail, or mutually agreed upon method sent to the designated representatives documented in the Preamble.

**Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. With respect to the treatment of Student Data only, in the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit “H”, the SDPC Standard Clauses, and/or the Supplemental State Terms in Exhibit “G”, Exhibit “H” will control, followed by Exhibit “G”. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

**Entire Agreement.** This DPA and the Service Agreement (“the Agreement”) constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties.

**Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

**Governing Law; Venue and Jurisdiction.** This DPA will be governed by and construed in accordance with the laws of the state of the LEA, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the state and federal courts for the county of the LEA for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.

**Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a Change of Control. In the event of a Change of Control, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of such Change of Control. Such notice shall include

a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement.

**Authority.** Each signatory confirms they are authorized to bind their institution to this DPA in its entirety.

**Waiver.** No delay or omission by either party to exercise any right here under shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

## EXHIBIT A: PRODUCTS AND SERVICES

This DPA covers access to and use of [ ]'s existing Services that collect, process, or transmit Student Data, as identified below:

## EXHIBIT B: SCHEDULE OF STUDENT DATA

All Data Elements identified in this Exhibit are correct at time of signature.

Data Elements Collected by Product (required and optional):

Category of Data / Data Elements							
<b>Application Technology MetaData</b>							
IP Addresses of users, use of cookies, etc.							
Other application technology metadata							
<i>If 'Other' checked, please specify below checked box:</i>							
<b>Application Use Statistics</b>							
Meta data on user interaction with application							
<b>Assessment</b>							
Standardized test scores							
Observation data							
Voice recordings							
Other assessment data							
<i>If 'Other' checked, please specify below checked box:</i>							
<b>Attendance</b>							
Student school (daily) attendance data							

Category of Data / Data Elements							
Student class attendance data							
<b>Communication</b>							
Online communication captured (emails, blog entries)							
<b>Conduct</b>							
Conduct or behavioral data							
<b>Demographics</b>							
Data of birth							
Place of birth							
Gender							
Ethnicity or race							
Language information (native, or primary language spoken by student)							
Other demographic information							
<i>If 'Other' checked, please specify below checked box:</i>							
<b>Enrollment</b>							
Student school enrollment							
Student grade level							
Homeroom							
Guidance counselor							
Specific curriculum programs							
Year of graduation							

Category of Data / Data Elements							
Other enrollment information							
<i>If 'Other' checked, please specify below checked box:</i>							
<b>Parent/Guardian Contact Information</b>							
Address							
Email							
Phone							
<b>Parent/Guardian ID</b>							
Parent ID number (created to link parents to students)							
<b>Parent/Guardian Name</b>							
First and/or last							
<b>Schedule</b>							
Student scheduled courses							
Teacher names							
<b>Special Indicator</b>							
English language learner information							
Low-income status							
Medical alerts/health data							
Student disability information							
Specialized education Services (IEP or 504)							
Living situations (homeless/foster care)							
Other indicator information							

Category of Data / Data Elements							
<i>If 'Other' checked, please specify below checked box:</i>							
<b>Student Contact Information</b>							
Address							
Email							
Phone							
<b>Student Identifiers</b>							
Local (school district) ID number							
State ID number							
Provider/app assigned student ID number							
Student app username							
Student app passwords							
<b>Student Name</b>							
First and/or last							
<b>Student In App Performance</b>							
Program/application performance (e.g. typing program – student types 60 wpm, reading program – student reads below grade level)							
<b>Student Program Membership</b>							
Academic or extracurricular activities a student may belong to or participate in							

Student Survey Responses							
Student responses to surveys or questionnaires							
Student Work							
Student generated content; writing, pictures, etc.							
Other student work data							
<i>If 'Other' checked, please specify below checked box:</i>							
Transcript							
Student course grades							
Student course data							
Student course grades/performance scores							
Other transcript data							
<i>If 'Other' checked, please specify below checked box:</i>							
Transportation							
Student bus assignment							
Student pick up and/or drop off location							
Student bus card ID number							
Other transportation data							

<i>If 'Other' checked, please specify below checked box:</i>							
<b>Other</b>							
Other data collected							
<i>If 'Other' checked, please list each additional data element used, stored, or collected by your application below checked box:</i>							
<b>None</b>							
No student data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.							

If Student Data is stored outside the United States, Provider shall list below the Countries where data is stored:

No data is stored outside the US.

## EXHIBIT C: DEFINITIONS

**Change of Control:** Any merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of Provider or of the portion of Provider that performs the Services in the Service Agreement.

**Contextual Advertising:** Contextual advertising is the delivery of advertisements based upon a current visit to a Web page or a single search query, without the collection and retention of data about the consumer's online activities over time.

**De-Identified Data:** Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific student, including, but not limited to, any information that, alone or in combination is linkable to a specific student.

**Data Breach:** An unauthorized release, access to, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider in violation of applicable state or federal law.

**Educational Records:** Educational Records shall have the meaning set forth under FERPA 20 U.S. C. 12 32 g(a)(5)(A). For additional context see also the 'Student Data' definition.

**LEA:** For the purpose of this DPA, the LEA is the educational entity that is a Party to this Agreement. An LEA can be a state agency, an educational service agency, a charter school or school system or a private school or school system, in addition to the federal definition of Local Education Agency (LEA).

**Metadata:** Means information that provides meaning and context to other data being collected including, but not limited to date and time records and purpose of creation. Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information or Student Data.

**Originating LEA:** An educational entity otherwise meeting the definition of LEA that originally executes the DPA in its entirety (including the marked checkbox enabling Exhibit "E") with the Provider.

**School Official:** For the purposes of this DPA and pursuant to FERPA 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Educational Records; and (3) Is subject to FERPA 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Educational Records.

**Service Agreement:** Refers to the quote, corresponding contract, purchase order or terms of service and/or terms of use.

**Student Data:** Student Data includes any data, whether gathered, created or inferred by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student's Educational Record, persistent unique identifiers, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed

to be collected or processed by the Provider pursuant to the Services. Student Data shall not include properly De- Identified Data or anonymous usage data regarding a student's or LEA's use of Provider's Services.

**Student Generated Content:** The term "Student Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content. "Student Generated Content" does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment.

**Subprocessor:** For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to or storage of Student Data, including security, storage, analytics, and other processing activities necessary to perform a Provider business purpose.

**Subprocessor Agreement:** An agreement between Provider and a third party Subprocessor. A Subprocessor Agreement includes either a written agreement or an acceptance of terms and conditions (e.g., click through agreements).

**Subscribing LEA:** An educational entity otherwise meeting the definition of LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms by executing Exhibit "E".

**Targeted Advertising:** Targeted Advertising means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Provider Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include Contextual Advertising.

## EXHIBIT D: SPECIAL INSTRUCTIONS FOR DISPOSITION OF DATA

After this DPA takes effect, if the LEA has special requirements for the disposition of Student Data that are not expressed in 4.6 Disposition of Data, the LEA may fill in this form and deliver it to the Provider.

**The Provider and the LEA must not fill in this form at the initiation of the DPA.**

The Provider shall act on Exhibit “D” from the designated representative of the LEA or their designee (Preamble or Exhibit “E” for Subscribing LEA).

\_\_\_\_ (“LEA”) instructs Provider to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

### 1. Extent of Disposition

☐ Disposition is partial. The scope of Student Data to be disposed of is set forth below or found in an attachment to this Directive:  
\_\_\_\_\_

☐ Disposition is complete. Disposition extends to all Student Data.

### 2. Nature of Disposition

☐ Disposition shall be by destruction or deletion of Student Data.

☐ Disposition shall be by a transfer of Student Data. The Student Data shall be transferred to the following site as follows:  
\_\_\_\_\_

### 3. Timing of Disposition

Student Data shall be disposed of by the following date:

☐ As soon as commercially practicable

☐ On Provider’s standard destruction schedule

☐ By \_\_\_\_\_

### 4. De-Identified Data

☐ The Provider certifies that they have De-Identified the data, as defined elsewhere in this Agreement, and disposed of all copies of Student Data that were not De-Identified in accordance with this Schedule and the DPA. The Provider will notify LEA in accordance with the notification requirements of the DPA using this form.

As of \_\_\_\_\_

### 5. Other:

**Signature(s)**

**Notice of Verified Disposition of Data**

\_\_\_\_\_  
Authorized Representative of  
LEA

\_\_\_\_\_  
Date

\_\_\_\_\_  
Authorized Representative of  
Provider

\_\_\_\_\_  
Date

## Page 1 of 2: OFFER OF TERMS

**Exhibit “E” (continued)**

Originating LEA: \_\_\_\_\_

Resource Names: \_\_\_\_\_

Provider Name: \_\_\_\_\_

**Page 2 of 2:**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Originating LEA and the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER.\*\***

Please note, by signing this Exhibit you are also agreeing to any language that may be included in Exhibits to the Originating DPA beyond this Exhibit “E”. The below signatory confirms they are authorized to bind their institution to this DPA as in its entirety.

Subscribing LEA: \_\_\_\_\_

Signed By: \_\_\_\_\_

Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title/Position: \_\_\_\_\_

School District Name: \_\_\_\_\_

**Designated Representative of LEA:**

Name: \_\_\_\_\_ Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Email: \_\_\_\_\_

**Notices to Subscribing LEA:** The Provider and Subscribing LEA are each responsible to promptly notify the other Party of changes to the notice information.

**Security Notices to Subscribing LEA**

[ \_\_\_\_\_ ]  
[ \_\_\_\_\_ ]  
[ \_\_\_\_\_ ]  
[ \_\_\_\_\_ ]

[ \_\_\_\_\_ ]  
[ \_\_\_\_\_ ]  
[ \_\_\_\_\_ ]  
[ \_\_\_\_\_ ]

With a copy to (if provided):

[ \_\_\_\_\_ ]  
[ \_\_\_\_\_ ]  
[ \_\_\_\_\_ ]

## EXHIBIT F: ADEQUATE CYBERSECURITY FRAMEWORKS

Provider must mark one or more frameworks with which it complies.

The Provider may change which framework it complies with without invalidating or changing the DPA, but must notify the LEA of such change in accordance with the notification requirements of the DPA.

FRAMEWORK(S)	
	Global Education Security Standard - <a href="https://sdpc.a4l.org/gess/">https://sdpc.a4l.org/gess/</a>
	NIST Cybersecurity Framework (CSF)
	NIST SP 800-53 Security and Privacy Controls for Information systems and organizations
	NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
	ISO 27000 series, Standards for implementing organization security and management practices
	CIS Center for Internet Security Critical Security Controls
	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

This space is provided for optional security programs and measures as noted in section 5.3:

### Addendum 5.3 – Hernando DSA

In accordance with Section 5.3 and based on discussion with the DSA provider David Sallay (4 Access 4 Learning Community) on 09.30.25 please see enclosed:

- Hubspot Security Overview
- Hubspot 2025 SOC 3 Type 2 Security Report
- Hubspot Compliance FAQs
- FTP Server Security Diagram
- Cyber Security Coverage

## EXHIBIT G: Supplemental SDPC State Terms for Florida

Providers/Operators are to comply with section 1002.22, Florida Statutes.

Providers/Operators are to comply with the Florida Student Online Personal Information Protection Act, Florida Statute 1006.1494. This Act (effective 7/1/2023 and initiated from SB 662 in 2023) establishes new and different terms than those outlined in the National Student Data Privacy Agreement contained herein. Providers/Operators are subject to all of the Act's privacy terms, including, but not limited to the following:

**1. An operator may not knowingly do any of the following:**

- a. Engage in targeted advertising on the operator's site, service, or application, or targeted advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, which the operator has acquired because of the use of that operator's site, service or application for K-12 school purposes.
- b. Use covered information, including persistent unique identifiers, created, or gathered by the operator's site service, or application to amass a profile of a student, except in furtherance of k-12 school purposes.
- c. Share, sell, or rent a student's information, including covered information

**2. An operator shall do all the following:**

- a. Collect no more covered information that is reasonably necessary to operate an Internet website, online service, online application, or mobile application.
- b. Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information which are designed to protect it from unauthorized access destruction, use, modification, or disclosure.
- c. Unless a parent or guardian expressly consents to the operator retaining a student's covered information, delete the covered information at the conclusion of the course, or corresponding program and no later than 90 days after a student is no longer enrolled in a school within the district, upon notice by the school district.

## **Addendum 5.3 – Hernando DSA**

**In accordance with Section 5.3 and based on discussion with the DSA provider David Sallay (4 Access 4 Learning Community) please see enclosed:**

- **Hubspot Security Overview**
- **Hubspot 2025 SOC 3 Type 2 Security Report**
- **Hubspot Compliance FAQs**
- **FTP Server Security Diagram**
- **Cyber Security Coverage**

## **Hubspot Security Overview**



Last Update: February 2025

# Security & Compliance Overview



# Table of Contents

Introduction	4
Our Company and Products	4
HubSpot Security and Risk Focus	4
Document Scope and Use	5
Our Security, Compliance, and Privacy Objectives	5
HubSpot Security Controls	6
Infrastructure Security	6
Cloud Hosting Provider	6
Network and Perimeter	7
Configuration Management	7
Logging	8
Alerting and Monitoring	8
Application Security	8
Web Application Defenses	8
Development and Release Management	9
Vulnerability Management	9
Customer Data Protection	10
Data Classification	10
Sensitive Data	11
Tenancy	12
Encryption	12
Key Management	12
Artificial Intelligence & Machine Learning	13
Data Backup and Disaster Recovery	14
System Reliability and Recovery	14
Disaster Recovery	15
Backup Strategy	15
System Backups	15
Physical Backup Storage	16
Backup Protections	16
Customer Data Backup Restoration	16
Identity and Access Control	16

Product User Management	16
Product Login Protections	17
Portal Login Settings	18
Product API Authorization	18
Portal Activity & Alerting	18
HubSpot Employee Access to Customer Data	19
Access to Production Infrastructure	19
Access to Customer Portals	20
Organizational and Corporate Security	21
Corporate Network Protections	21
Corporate Authentication and Authorization	21
Endpoint Protection	22
Security Awareness Training	22
Risk Management	22
Vendor Management	22
Policy Management	23
Corporate Physical Security	23
Background Checks and Onboarding	23
Incident Management	24
Incident Response	24
Compliance	24
General Data Protection Regulation (GDPR)	24
Sarbanes-Oxley (SOX)	25
Systems and Organization Controls (SOC 2)	25
Sensitive Data Processing and Storing	25
Privacy	26
Data Retention and Data Deletion	26
Privacy Program Management	27
Breach Response	27

# Introduction

## Our Company and Products

HubSpot provides a customer platform that helps businesses connect and grow better. We deliver seamless connection for customer-facing teams with a unified platform that includes three layers: AI-powered engagement hubs, a Smart CRM, and a connected ecosystem that extends the customer platform with app marketplace integrations, a community network, and educational content.

Our engagement hubs include Marketing Hub, Sales Hub, Service Hub, Operations Hub, Content Hub and Commerce Hub, as well as other tools and integrations that enable companies to attract, engage, and delight customers throughout the customer experience. Our customer platform features a central database of lead and customer interactions and integrated applications designed to help businesses attract visitors to their websites, convert visitors into leads, close leads into customers, transact with those customers, and delight them so they become promoters of those businesses.

The HubSpot products are offered as Software-as-a-Service (SaaS) solutions. These solutions are available to customers through purpose-built web applications, mobile applications, Application Programming Interfaces (APIs), and email productivity tools.

## HubSpot Security and Risk Focus

HubSpot's primary security focus is to safeguard our customers' data. To this end, HubSpot has invested in the appropriate controls to protect and service our customers. This investment includes the implementation of dedicated Corporate, Product, Infrastructure, and Physical Security programs. These Security teams are responsible for HubSpot's comprehensive security program, partnering with our Compliance, Legal, and Privacy teams to own the governance process. Our Chief Information Security Officer, Alyssa Robinson, oversees the implementation of security safeguards across the HubSpot enterprise.

## Document Scope and Use

HubSpot values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document (including any related communications) are not intended to create a binding or contractual obligation between HubSpot and any parties, or to amend, alter or revise any existing agreements between the parties.

## Our Security, Compliance, and Privacy Objectives

We have developed our security framework using best practices for the SaaS industry. Our key objectives include:

- Security-Minded Growth – deliver innovative products and services on a foundation of security, privacy and compliance standards.
- Availability and Continuity of Service – ensure availability of the service and minimize risks to service continuity.
- Data Integrity – make sure that the customer data entrusted to HubSpot is never corrupted or altered inappropriately.
- Compliance with Standards – aim to comply with or exceed industry standard best practices. Our controls governing the availability, confidentiality, and security of customer data meet or exceed the applicable SOC 2 (Service Organization Control Type 2) Trust Service Principles (TSPs) established by the American Institute of Certified Public Accountants (AICPA).
- Privacy - apply consistent, effective programs to ensure that customer data stays private. We take the protection of customer data seriously, and our Customer [Data Processing Agreement](#) describes the commitments we make to comply with applicable global data privacy laws.

# HubSpot Security Controls

In order to protect the data that is entrusted to us, HubSpot utilizes a defense-in-depth approach to implement layers of administrative, technical, and physical security controls throughout our organization. The following sections describe some of our most frequently asked-about controls.

## Infrastructure Security

### Cloud Hosting Provider

HubSpot does not host any product systems or data within its corporate offices.

HubSpot outsources hosting of its product infrastructure to a leading cloud infrastructure provider, Amazon Web Services (AWS). HubSpot's US product infrastructure resides in AWS data centers located in the United States. The primary region in the US (East) is located in Virginia and the secondary region is located in Ohio. Customers also have the option to have their HubSpot data hosted in the European Union, with the primary region located in Germany and the secondary located in Ireland.

In Q1 of 2025, HubSpot is expanding its data hosting locations to include Australia, Canada, and an additional hosting location in the United States (West) in Oregon. While these new data center locations leverage the same core infrastructure and security architecture as our existing data center offerings, they will not be reflected in HubSpot's SOC 2 report until our updated report is released that will cover the period of May 1, 2024 through April 30, 2025.

We place reliance on AWS's audited security and compliance programs for the efficacy of their physical, environmental, and infrastructure security controls. AWS guarantees between 99.95% and 100% service availability, ensuring redundancy to all power, network, and HVAC services. The business continuity and disaster recovery plans for the AWS services we use have been independently validated as part of their SOC 2 Type 2 report and ISO 27001 certification.

AWS's compliance documentation and audit reports are publicly available at the [AWS Cloud Compliance Page](#) and the [AWS Artifacts Portal](#). HubSpot is unable to deliver these documents on your behalf; you may obtain them directly from the [AWS Artifacts portal](#).

Additional information regarding HubSpot's cloud infrastructure can be found on our [Cloud Infrastructure Frequently Asked Questions](#) page and in our [Customer Terms of Service](#).

## Network and Perimeter

The HubSpot product infrastructure enforces multiple layers of filtering and inspection on all connections across our Web Application Firewall (WAF), logical firewalls, and security groups.

Network-level access control lists are implemented to prevent unauthorized access to our internal product infrastructure and resources. By default, firewalls are configured to deny network connections that are not explicitly authorized, and traffic monitoring is in place to alert on anomalous activity.

Changes to our network and perimeter systems are actively monitored and controlled by standard change control processes. Firewall rulesets are reviewed on an annual basis to help ensure that only necessary connections are configured.

## Configuration Management

Automation drives HubSpot's ability to scale with our customers' needs, and rigorous configuration management is baked into our day-to-day infrastructure processing. The product infrastructure is a highly automated environment that expands capacity as needed.

All server configurations are embedded in images and configuration files, which are used when new server instances are built. Each instance type includes its own hardened configuration, and changes to the configuration and standard images are managed through a formal change management process. Server instances are tightly controlled from provisioning through deprovisioning, ensuring that deviations from configuration baselines are detected and reverted at a predefined cadence. In the event that a production server deviates or drifts from the baseline configuration, it will be overwritten with the baseline within 30 minutes.

HubSpot's IT and Security teams adhere to structured patch management schedules using automated configuration management tools and by replacing server instances that are no longer compliant with the expected baseline.

## Logging

HubSpot logs actions and events that occur within the application for performance and risk management purposes. These logs are indexed and stored in a central logging solution hosted in HubSpot's AWS environment. Security-relevant logs are also retained, indexed, and stored to facilitate investigation and response activities. The retention period of logs depends on the nature of the data logged.

Write access to the storage service in which logs are stored is tightly controlled and limited to a small subset of engineers who require access.

## Alerting and Monitoring

HubSpot invests heavily in automated build procedures, monitoring, alerting, and response capabilities to continuously address potential issues. The HubSpot product infrastructure is instrumented to alert engineers and administrators via automated triggers when anomalies occur. For example, error rates, file quarantines, process terminations, abuse scenarios, application attacks, and other anomalies trigger automatic responses or alerts to the appropriate teams for response, investigation, and correction.

## Application Security

### Web Application Defenses

HubSpot has implemented a Web Application Firewall (WAF) to protect all customer content hosted on the platform as well as [HubSpot APIs](#). These tools actively monitor real-time traffic at the application layer and can alert on or deny malicious behavior based on behavior type and session rate.

The rules used to detect and block malicious traffic are aligned to the best practice guidelines documented by the Open Web Application Security Project (OWASP), specifically the OWASP Top 10 and similar recommendations. Protections from Distributed

Denial of Service (DDoS) attacks are also incorporated, helping to ensure customers' web sites and other parts of the HubSpot products are continuously available.

## Development and Release Management

One of HubSpot's greatest advantages is a rapidly advancing feature set, and we optimize our products through a modern continuous delivery approach to software development. To accomplish this, our developers adhere to secure SDLC standards and procedures.

New code is deployed thousands of times each day. Code review, testing, and merge approval are performed before deployment. Static code analysis blocks known misconfigurations from entering the code base. Once approved, code is automatically submitted to HubSpot's continuous integration environment where compilation, packaging, and unit testing occur. Dynamic scanning for security vulnerabilities is performed against our applications on a routine basis.

Newly developed code is first deployed to a dedicated and separate Quality Assurance (QA) environment for the testing before being promoted to production. Network-level segmentation prevents unauthorized access between QA and production environments.

All code deployments create archives of existing production code in case failures are detected by post-deployment hooks. The deploying team manages notifications regarding the health of their applications and if a failure occurs, rollback processes are immediately engaged.

We use software gating and traffic management to control features based on customer preferences (private beta, public beta, full launch). HubSpot features seamless updates and, as a SaaS application, there is no downtime associated with releases. Major feature changes are communicated through in-app messages and/or [product update posts](#).

## Vulnerability Management

The HubSpot Security team manages a multi-layered approach to vulnerability management, using a variety of industry-recognized tools and threat feeds to ensure comprehensive coverage of our technology stack. Adherence to Service Level Agreements (SLAs) is accomplished via automation of ticket generation and closure, as well as escalation paths when appropriate.

Vulnerability scans are configured to scan for vulnerabilities on a daily basis, using adaptive scanning inclusion lists for asset discovery as well as the latest vulnerability detection signatures.

In addition to our Security Operations Center (SOC), HubSpot also has an internal team dedicated to penetration testing, red team exercises, and vulnerability management that works to systematically discover any vulnerabilities and ensure that best practices are in place to secure our product.

We bring in industry-recognized third parties to perform annual penetration tests against our applications and infrastructures. The goal of these programs is to identify vulnerabilities that may present security-related risks. Relevant findings are assessed, mitigations are prioritized according to risk, and both are incorporated in the reports available to our customers. Additionally, HubSpot manages a [bug bounty program](#) where independent security researchers may submit potential issues for review.

To track and manage these identified risks across the HubSpot product, we've implemented our [Mainsail framework](#) which sets HubSpot's Security, Privacy, and Compliance standards as a top priority, or guardrail, across all Product teams. When vulnerabilities are identified, Mainsail allows us to measure the associated risk to our product and customers, assign a risk-based SLA, and align autonomous engineering teams to collaborate and prioritize remedial steps.

## Customer Data Protection

### Data Classification

HubSpot's applications allow customers to define the type of information to be collected and stored on their behalf. Per the HubSpot [Terms of Service](#) and [Acceptable Use Policy](#), our customers are responsible for ensuring they only capture appropriate information to support their marketing, sales, services, content management, and operations processes.

The HubSpot product may be used to collect or store sensitive information – such as the last four digits of credit or debit card numbers, financial account information, Social Security numbers, passport numbers, or health information—only in accordance with the [HubSpot](#)

[Sensitive Data Terms](#). To accomplish this, customers must enable HubSpot's [sensitive data](#) feature.

Further detail on HubSpot's data classification scheme can be found within our SOC 2 report which can be downloaded from our [Trust Center](#).

## Sensitive Data

HubSpot's sensitive data product feature allows users to identify certain properties as "sensitive" and store and access sensitive data in certain places within your portal. This functionality allows enterprise customers to store sensitive personal data, financial data, and/or Protected Health Information (PHI).

To learn about how these features work, please review the [Knowledge Base article for storing sensitive data in HubSpot](#), the [KB article for storing PHI in HubSpot](#), and the KB article for [storing highly sensitive data in HubSpot](#).

Sensitive property values and CRM attachments are encrypted when they reach HubSpot's backend systems, typically within the first or second hop. The properties and CRM attachments are encrypted using AES-256 with unique encryption keys for each customer. The root keys are managed via AWS Key Management Service (KMS), and no one has access to these keys. HubSpot engineers cannot view sensitive properties. However, a small and tightly constrained group of engineers are able to decrypt the data in order to support these services. There are also HubSpot services that need to decrypt the data. To do this, a given service must invoke a specific scope to be able to decrypt a sensitive property.

For [highly sensitive data](#), data remains encrypted even when viewed within the HubSpot portal. A click-to-decrypt feature ensures that the data is readable only on an as-needed basis. Further limitations exist to limit downstream decryption by engineers and HubSpot services due to the limited functionality available for highly sensitive properties.

Please also review the [Sensitive Data Terms](#), as they govern usage of this feature.

## Tenancy

HubSpot provides a highly scalable, multi-tenant SaaS solution where customer data is logically separated using unique portal IDs to associate data and objects to specific customers.

Authorization rules are incorporated into the design architecture and validated on a continuous basis. Additionally, we log application authentication and associated changes, application availability, and user page views.

## Encryption

All sensitive interactions with the HubSpot products (e.g. API calls, authenticated sessions, etc.) are encrypted in transit with Transport Layer Security (TLS) version 1.2 or 1.3 and 2,048 bit keys or better. TLS is also a default for customers who host their websites on the HubSpot platform.

See our [website setup guide](#) and our KB article on [SSL and domain security](#) for more information about configuring TLS for your HubSpot-hosted site.

HubSpot leverages several technologies to ensure stored data is encrypted at rest. Platform data is stored using AES-256 encryption. User passwords are hashed following industry best practices, and are encrypted at rest.

For [sensitive data types](#), we add application layer encryption, also using AES-256, with unique encryption keys for each customer and provide stricter access controls than for non-sensitive data.

## Key Management

Encryption keys for both in-transit and at rest encryption are securely managed by the HubSpot platform. TLS private keys for in-transit encryption are managed through our content delivery partner. Volume and field level encryption keys for at rest encryption are stored in a hardened Key Management System (KMS). Keys are rotated at varying frequencies, depending upon the sensitivity of the data they govern. In general, TLS

certificates are renewed annually. For sensitive data stores, unique encryption keys are used for each customer.

HubSpot is unable to support customer-supplied encryption keys at this time.

## Artificial Intelligence & Machine Learning

HubSpot provides an AI-native customer platform with [Breeze](#), our complete AI solution that delivers a fast, easy, and unified AI experience for marketing, sales, and service teams. To this end, our AI tools and underlying systems are included within our annual SOC 2 Type 2 report as they are released into general availability (GA). HubSpot may release future beta and alpha AI product offerings as we continue to evolve and improve our customer platform. Although these are not scoped into our SOC 2 report at this stage, they are generally supported by HubSpot's core infrastructure and security architecture.

We implement appropriate technical and organization measures to protect and secure personal data used in our AI products. This approach involves collaboration between dedicated product, engineering, and legal teams to maintain compliance with regulatory and industry standards, as well as a broad commitment to preventing unauthorized access to customer data.

Customer Data remains secure and private when using our AI features, regardless of whether your data is used as part of HubSpot's machine learning processes. Data is never shared between HubSpot users or accounts. Our AI-generated outputs are specific to each customer; in other words, one customer's data will not be exposed to any other customers when using our AI products. Additionally, when using AI products, customer prompts, generated content, and usage metrics are logged and managed to support continuous product improvement. Your AI usage data is stored in approved HubSpot data storage locations, where access is restricted to relevant engineering and product teams on an as-needed basis. Access to the data is subject to review and approval.

HubSpot's AI products are moderated against harmful content such as hate speech, harassment, self-harm, sexual content, and violence using open source moderation solutions. We identify and eliminate harmful content to create a safe and positive environment for our users.

The underlying technology behind HubSpot's AI functionality consists of our own machine learning models as well as those of our trusted third party vendors like OpenAI. While customer prompts may be shared with such third parties to enable certain functionalities, these submissions are not used by third parties to train or improve its models. HubSpot may use customer data to train our own models; however, if you enable HubSpot's sensitive data features, the sensitive properties that you create will not be used to train HubSpot's AI models. Customers may also opt out of having their data used to build and train our AI models by having a super admin on the user's account email [privacy@hubspot.com](mailto:privacy@hubspot.com). Once you have opted out, your data will not be used to train our internally built models and you may still use our AI products.

Customers have options to control their use of certain AI products including the ability to opt in and opt out of specific functionalities. For more information on AI choices and rights, please visit our [Product-Specific Terms - AI Products](#).

For additional information and transparency around HubSpot's use of AI and how our AI systems interact with your data, please visit [behindhubspot.ai.com](https://behindhubspot.ai.com). The AI model cards provided here feature specific details about Breeze-powered AI features.

## Data Backup and Disaster Recovery

### System Reliability and Recovery

HubSpot is committed to ensuring the availability of our systems by using commercially reasonable efforts to meet a target service uptime of 99.95% for our subscription service in a given calendar month. Please reference section 8 of the [Product Specific Terms](#) for more information.

Additionally, we provide real-time updates and historical data on system status via [HubSpot's status site](#).

We build our platform so that HubSpot is available and accessible in a variety of disaster scenarios. To this end, all HubSpot product services are built with full redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure providers, and all web, application, and

database components are deployed with a minimum of n+1 supporting server instances or containers.

Services within HubSpot's distributed microservices architecture are designed to reduce system interdependence, and each service has a corresponding test environment where changes are deployed and validated before they are migrated to production.

HubSpot utilizes a worldwide Content Delivery Network (CDN) to distribute content to a location closest to users, enabling quick and consistent access wherever users may be.

Additionally, we have a dedicated Reliability engineering team committed to the scalability and reliability of the HubSpot application.

## Disaster Recovery

HubSpot maintains a disaster recovery plan that details how we sustain key product infrastructure and internal corporate systems in the event of a disaster. The disaster recovery plan is documented, updated, and tested annually as part of our SOC 2 compliance. Please refer to our SOC 2 report (downloadable from our [Trust Center](#)) for more detail.

## Backup Strategy

### System Backups

Systems are backed up on a regular basis with established schedules and frequencies. Seven days' worth of backups are kept for any database in a way that ensures that restoration can occur easily. Backups are monitored for successful execution, and alerts are generated in the event of any exceptions. Failure alerts are escalated, investigated, and resolved.

Data is backed up daily to the local region. Additionally, backups are copied regularly to a separate AWS region for recovery in the event of a primary regional outage. Monitoring and alerting is in place for replication failures and triaged accordingly.

All production data backups are stored on a highly available file storage facility like Amazon S3.

### Physical Backup Storage

Because we leverage public cloud services for hosting, backup, and recovery, HubSpot does not implement physical infrastructure or physical storage media within its products. HubSpot does not generally produce or use other kinds of hard copy media (such as paper, tape, etc.) as part of making our products available to our customers.

### Backup Protections

By default, all backups are encrypted at rest and immutability is ensured through access control restrictions and Write Once Read Many (WORM) protections on HubSpot product infrastructure networks. Strict access control lists are used to protect backup file storage.

### Customer Data Backup Restoration

HubSpot customers don't have access to the product infrastructure in a way that would allow a customer-driven failover event. Disaster recovery and resiliency operations are managed by HubSpot product engineering teams.

In most cases, customers can use the recycle bin to directly recover and restore [contacts](#), [companies](#), [deals](#), [tickets](#), and [custom object records](#), [activity](#), and [workflows](#) up to 90 days after they were deleted. Changes to web pages, blog posts, or emails can be restored to [previous versions of content](#) using version history.

For customers who wish to additionally back up their data, the HubSpot platform provides many ways of ensuring that you have what you need. By using [Data Backup and Restore](#), customers can create backups of their CRM data and seamlessly recover to a restore point. Additionally, many of the features within your HubSpot portal contain export options, and the [HubSpot library of public APIs](#) can be used to synchronize your data with other systems. For further details about backing up your data, please review our KB article about [exporting your content](#).

## Identity and Access Control

### Product User Management

The HubSpot products allow for granular authorization rules. Customers are encouraged to actively administer their accounts. Customers can create and manage the users in their portals, assign the privileges that are appropriate, and limit access to only what is necessary

in order to reduce risk. For more information about user roles, please see [the HubSpot User Permission Guide](#).

For additional guidance, the in-app [Security Center](#) provides recommendations on an account's unique configuration and compares settings against security best practices. Configurations that can present security risks are given risk scores and can be reviewed and remediated from one convenient location. This includes risky user permissions, 2FA status, inactive apps, and more.

## Product Login Protections

The HubSpot product features many options for users to securely log in to their HubSpot accounts. The built-in HubSpot login with email and password enforces a uniform password policy which requires a minimum of 12 characters and a combination of lower letters, uppercase letters, and numbers, symbols, or whitespace characters. Customers who use HubSpot's built-in login cannot change the default password policy. HubSpot checks user passwords against publicly leaked passwords and automatically prevents the use of a matching compromised password.

Customers using the built-in login on paid HubSpot plans are required to use [two-factor authentication](#). Two-factor Authentication can be configured via authenticator app, the HubSpot Mobile App, or SMS text message. For free plans, portal administrators are encouraged to set up and require two-factor authentication for all users.

Additionally, HubSpot allows users to log in with common services using the "Sign In with Google," "Sign In with Microsoft," or "Sign In with Apple" options at the login screen. Customers can configure a password policy within their settings with these respective providers.

Enterprise customers can take advantage of SAML-based Single Sign-On (SSO) integrations with any SAML-based Identity Provider. Instructions for setting up SSO are available in [this knowledge base article](#) and in the [HubSpot Academy](#). By default, after turning on SSO, all users will be required to log in via your configured SSO method.

For customers who prefer passwordless authentication, HubSpot allows users to [set up and use passkeys](#) for logging in via browser and the iOS app.

## Portal Login Settings

Portal Admins have the ability to set additional login security controls that align with the needs of their organization:

- **Allowed Login Methods:** Allows an admin to enforce what login methods are allowed for accessing the portal. For example, if the organization uses Google Workspace, you can set Allowed Login Methods to only allow Google sign-in and disallow all other login types.
- **Inactivity Timeout:** Allows an admin to set a time duration between 8 hours and 72 hours that will automatically log a user out of their session if they are inactive.
- **IP Restrictions:** Allows an admin to set IP ranges in which their users access HubSpot from to provide greater level of control of how your portal is being accessed.

## Product API Authorization

API access is enabled through either OAuth (version 2) or Private App access tokens. Both HubSpot's OAuth 2.0 and Private App implementations provide strong approaches to authenticating and authorizing API requests. These methods offer granular control over your integrations and account data. We require OAuth for all featured integrations.

Select HubSpot APIs may be used for public and private app developers to interact with [sensitive data](#). More information can be found within our [Overview of Sensitive Data in HubSpot CRM for Developers](#), and also within our [Developer Doc for Sensitive Data App Scopes](#).

For more information about API use and authentication, please see the [Developers portal](#).

Previously, API keys (also known as Hapikeys or HubSpot API keys) were a supported authentication method for the HubSpot APIs. Support for API keys was discontinued on November 30, 2022.

## Portal Activity & Alerting

Customers can [enable notifications](#) within the HubSpot portal for a range of account activity including unusual logins, data imports and exports, and more.

HubSpot also provides customers with the ability to view and export comprehensive audit logs on account activity. Customers can review or investigate activity within a portal, export

audit logs manually, or [export logs via API](#) for integration with a security information and event management (SIEM) solution. Audit log types include:

- User logins
- Security activity
- Views or edits of highly sensitive data properties
- Content activity
- HubSpot employee access history for customer support

A [centralized audit log](#) of all user actions is available to Enterprise subscribers.

## HubSpot Employee Access to Customer Data

### Access to Production Infrastructure

HubSpot's production infrastructure and restricted or customer data can only be accessed from company-owned and managed computers, and require phish-resistant Multi-factor Authentication (MFA). User access is strictly controlled. HubSpot employees are granted access using a Role-Based Access Control (RBAC) model.

Day-to-day access to systems hosting customer data is restricted. Access is available only to HubSpot personnel that require access to certain systems to perform their respective job duties. Persistent administrative access is restricted. For temporary or emergency access to administrative functions (such as alert responses and troubleshooting), HubSpot's system uses a Just-In-Time-Access (JITA) model to grant users privileged access for a limited duration.

Each Engineering JITA request is logged along with the reason for access. After the configured session limit, access to the account expires and is automatically revoked. Daily Engineering JITA usage is available for retroactive review by Engineering management. Management reviews activities performed during JITA sessions in key datastores and the reason for access, and monitors for anomalous behavior.

Additionally, direct network connections to product infrastructure devices over SSH or similar protocols is prohibited, and engineers are required to authenticate first through a bastion host or "jump box" before accessing QA or production environments. Server-level authentication uses user-unique SSH keys and token-based two-factor authentication.

## Access to Customer Portals

By default, Customer Support, Services, and other customer engagement staff can obtain limited access to parts of your HubSpot account to help you use your HubSpot portal.

The HubSpot application also uses a JITA model to grant employees access to a customer's portal for a limited duration (Portal JITA). Each Portal JITA request is logged and requires a business reason for access. Note that access is automatically granted for certain use cases, such as an open Support ticket. Other Portal JITA requests initiate an exception process which requires manager or manager-equivalent approval. Access is limited to a specific customer's portal for a maximum 24-hour period. HubSpot also utilizes risk-based monitoring to detect unusual Portal JITA activity. HubSpot support employees must be on HubSpot-owned and managed devices, which require SSO and phish-resistant MFA, in order to access Portal JITA.

When accessing a portal using Portal JITA, HubSpotters are unable to perform high-risk actions such as:

- viewing [sensitive data](#) fields
- changing domain or SSO settings
- exporting users/contacts
- viewing/creating/deleting/rotating private app keys
- importing data to the CRM
- deleting contacts, companies, deals, and tickets

User logins, HubSpot employee access, security activity, and content activity is logged. The last 90 days of these logs are available as the ['Export HubSpot employee access history' option within your portal](#).

Customers may choose to disable HubSpot employee access to their portal entirely by following [the steps outlined in this article](#). Please note that while this disables HubSpot employees from accessing your HubSpot portal, it does not disable all HubSpot employees from accessing customer data. Customer data may still be accessed internally via Engineering JITA by a limited number of Engineering personnel for supporting, troubleshooting, and improving the HubSpot product. Additionally, HubSpot's Trust & Safety team may temporarily re-enable the Portal JITA feature to access your portal if an investigation is necessary. This step is only taken when there is a safety or security issue

such as a potential security breach, fraud, or other Terms of Service violations, and Trust & Safety team members disable this feature when their work is completed.

## Organizational and Corporate Security

### Corporate Network Protections

Centrally managed application firewalls are deployed in a High Availability architecture at HubSpot Corporate offices. Our guest networks are separate and isolated from our corporate network, and all firewalls are configured to block all inbound connections unless the session is explicitly identified and allowed. HubSpot enforces system authorization checks via digital certificates prior to allowing a device to connect to the Corporate network. Unauthorized devices are moved to a containment VLAN with no access to the internal network.

### Corporate Authentication and Authorization

Access to the HubSpot Corporate network, both remotely and while in office, requires device validation and FIDO2-compliant MFA. Access to corporate systems is based on RBAC and the principle of zero trust. Users can only access what is necessary for their role and job function.

Password policies follow industry best practices for required length, complexity, and rotation frequency. Password vaults are in place to manage certain administrative account passwords, and access to the vault is managed through RBAC or through the JITA process.

We have built an extensive support system to streamline and automate our security management and compliance activities. Several times each day, this system collects and analyzes logs from across our product and corporate infrastructure and initiates manual reviews where appropriate. This is done to ensure that permission grants are appropriate, employee events are managed, access revocations are timely, change logs are effectively collected, and compliance evidence is preserved. Employee access and permissions to key internal systems are manually reviewed semi-annually to help ensure access granted is necessary for their job function.

## Endpoint Protection

Company-issued laptops are centrally managed and feature hardened configurations that include full disk encryption, a Privileged Access Management (PAM) solution, and routine security posture assessments.

Endpoints are also protected by a market-leading Endpoint Detection and Response (EDR) solution and we incorporate extensive automation into our detection and response capabilities, capitalizing on signaling from our robust security stack to create a highly integrated ecosystem that is continually optimized to detect anomalous behavior.

## Security Awareness Training

Security culture is foundational to a strong security program. We start building that culture with mandatory security training for every new HubSpot employee. After that, all HubSpot employees are required to complete annual awareness training. For certain jobs with specific risks, we have role-specific training.

Finally, we give all HubSpot employees a chance to put this training into practice with quarterly simulated phishing and reporting exercises.

## Risk Management

HubSpot has an Enterprise Risk Management (ERM) program that includes a documented ERM policy, recurring risk assessments, and a risk escalation process.. Risk mitigation and remediation activities are tracked and reviewed at a designated cadence.

Further detail on the risk assessment and risk management program can be found within the SOC 2 report (downloadable from our [Trust Center](#)).

## Vendor Management

We leverage a number of third party service providers at HubSpot to support the development of our product as well as internal operations. We maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support HubSpot.

Appropriate safeguards are assessed relative to the service being provided and the type of data being exchanged. For example, our protocol is to require vendors that handle customer data to maintain business continuity and disaster recovery programs for added assurance of customer data protection. Ongoing compliance with expected protections is managed as part of our contractual relationship with them. Our Security, Privacy, Legal, and Compliance teams coordinate with our business stakeholders as part of the vendor management review process.

We maintain a list of our sub-processors within our [Data Processing Agreement \(DPA\)](#).

## Policy Management

To help keep all our employees on the same page with regard to protecting data, HubSpot documents and maintains a number of written security policies and procedures. HubSpot maintains a core Written Information Security Policy, which covers a variety of topics such as data handling requirements, privacy considerations, and disciplinary actions for policy violations.

Policies are reviewed and approved at least annually and stored in the company policy repository.

### Corporate Physical Security

HubSpot offices are secured in multiple ways. Security services are leveraged at each of HubSpot's global locations to help create a safe environment for HubSpot employees. Door access is controlled using RFID tokens tied to individuals, which are automatically deprovisioned if lost or when no longer needed (for example, employee termination, infrequent use, etc). Video surveillance and other protective measures are implemented across HubSpot offices.

### Background Checks and Onboarding

HubSpot employees in the US undergo an extensive third-party background check prior to formal employment offers. In particular, employment, education, and criminal checks are performed for potential employees. Outside of the US, employment checks are performed. Reference verification is performed at the hiring manager's discretion.

Upon hire, all employees must read and acknowledge HubSpot's corporate Acceptable Use Policy (AUP) and Code of Use Good Judgement (COUGJ), which help to define employees' security responsibilities in protecting company assets and data.

## Incident Management

### Incident Response

HubSpot's Security Operations Center (SOC) team provides 24x7x365 coverage to respond quickly to all security and privacy events. HubSpot's rapid incident response program is responsive and repeatable. Predefined incident types, based on historical trending, are used to facilitate timely incident tracking and consistent task assignment, escalation, and communication. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others.

Our Security Leadership reviews all security related incidents, either suspected or proven, and we coordinate with affected customers using the most appropriate means based on the nature of the incident.

## Compliance

### General Data Protection Regulation (GDPR)

The HubSpot platform has a number of features that enable our customers operating in the European Union to achieve and maintain their GDPR compliance requirements, including the ability to perform a GDPR delete in response to a Data Subject Access Request (DSAR) ([see the KB article here](#)). Please refer to our [GDPR page for more information](#). While use of the HubSpot product can enable your GDPR compliance efforts, use of the HubSpot product alone does not make you GDPR compliant.

## Sarbanes-Oxley (SOX)

As a publicly-traded company in the U.S., HubSpot's key IT controls are audited on a recurring basis as part of its SOX compliance.

Public information about HubSpot's SOX compliance and our annual financial statements are available as part of our SEC filings. You can find more information on our [Investor Relations](#) page.

## Systems and Organization Controls (SOC 2)

HubSpot undergoes rigorous SOC 2 Type 2 and audits on an annual basis to attest to the controls that we have in place governing the security, availability, and confidentiality of customer data and the HubSpot products. These controls map to Trust Service Principles (TSPs) established by the American Institute of Certified Public Accountants (AICPA). Our SOC 2 Type 2 and SOC 3 reports are available for download from the HubSpot [Trust Center](#).

## Sensitive Data Processing and Storing

Please see our [Sensitive Data Terms](#) for details about prohibited data types. HubSpot provides privacy and security protections that enable our customers to operate our products in compliance with HIPAA. These include security features like comprehensive audit logging, advanced authentication features, inactive session timeout, account security recommendations, per tenant application level encryption, and more. Please refer to our [Trust Center](#) for resources on storing Sensitive Data, such as HubSpot's [Sensitive Data Implementation Guide](#), to ensure that you use our products and features in a way that supports your HIPAA obligations. Also, be sure to refer to the requirements in the "Use and Disclosure of PHI" section of the Business Associate Agreement in our [Sensitive Data Terms](#).

While HubSpot provides security features which enable your use of the product in a HIPAA-compliant manner, HubSpot does not currently offer independent attestation against the HIPAA Security Rule requirements or HITRUST certification. For news and

announcements regarding HubSpot's compliance posture, we encourage you to subscribe to our [Trust Center Updates](#).

Additionally, while HubSpot customers pay for the service by credit card, HubSpot does not store, process or collect credit card information submitted to us by customers and is not PCI-DSS compliant. We leverage trusted and PCI-compliant payment card processors to ensure that our own payment transactions are handled securely. You may access HubSpot's PCI SAQ-A report on the HubSpot [Trust Center](#).

## Privacy

The privacy of our customers' data is one of HubSpot's primary considerations. The protections described in this document and other protections that we have implemented are designed to ensure that your data stays private and unaltered. The HubSpot products are designed with a privacy-first approach and built with customer needs in mind. Our privacy program incorporates best practices, customers' and their contacts' needs, as well as regulatory requirements.

## Data Retention and Data Deletion

Customer data is retained for as long as you remain an active customer. The HubSpot platform provides active customers with the tools to delete their data (see the '[Deletion or Return of Personal Data](#)' section outlined in our [DPA](#)), and export their data (see the [KB article on how to export your content and data](#)).

Former customers' data is removed from live databases upon a customer's written request or after an established period following the termination of all customer agreements. Freemium customers' data is purged when the portal is no longer actively used, and former paying customers' data is purged 90 days after all customer relationships are terminated.

Information stored in replicas, snapshots, and backups is not actively purged but instead naturally ages itself from the repositories as the data lifecycle occurs. HubSpot retains certain data like logs and related metadata in order to address security, compliance, or statutory needs.

HubSpot does not currently provide customers with the ability to define custom data retention policies.

## Privacy Program Management

HubSpot's Legal, Security, and Privacy teams collaborate to ensure an effective and consistently-implemented privacy program. Information about our commitment to the privacy of your data is described in greater detail in our:

- [Privacy Policy](#)
- [Data Processing Agreement](#)

## Breach Response

You can find our breach reporting policies, process, and obligations outlined in our SOC 2 Report under our "Incident Response" section.

HubSpot will notify customers without undue delay after it becomes aware of any Customer Personal Data Breach and will provide timely information relating to the Customer Personal Data Breach as it becomes known or reasonably requested by the customer. We further outline our obligations regarding Customer Personal Data Breaches in [our DPA](#). Reporting obligations for our HIPAA Customers are outlined in our [Business Associate Agreement](#).

## **Hubspot 2025 SOC 3 Type 2 Security Report**



**HUBSPOT, INC.**

**INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT**

**FOR THE**

**HUBSPOT PLATFORM**

**FOR THE PERIOD OF MAY 1, 2024, TO APRIL 30, 2025**

**Attestation and Compliance Services**



**Proprietary & Confidential**

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

## INDEPENDENT SERVICE AUDITOR'S REPORT

To HubSpot, Inc.:

### *Scope*

We have examined HubSpot, Inc.'s ("HubSpot") accompanying assertion titled "Assertion of HubSpot, Inc. Service Organization Management" ("assertion") that the controls within the HubSpot Platform system ("system") were effective throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that HubSpot's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

HubSpot uses various subservice organizations for cloud storage, compute services, and data center hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at HubSpot, to achieve HubSpot's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

### *Service Organization's Responsibilities*

HubSpot is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that HubSpot's service commitments and system requirements were achieved. HubSpot has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, HubSpot is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

### *Service Auditor's Responsibilities*

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve HubSpot's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve HubSpot's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

### *Inherent Limitations*

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that HubSpot's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

### *Opinion*

In our opinion, management's assertion that the controls within the HubSpot Platform system were effective throughout the period May 1, 2024, through April 30, 2025, to provide reasonable assurance that HubSpot's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Washington, District of Columbia  
June 11, 2025

## ASSERTION OF HUBSPOT SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within HubSpot, Inc.'s ("HubSpot") HubSpot Platform system ("system") throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that HubSpot's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that HubSpot's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. HubSpot's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period May 1, 2024, to April 30, 2025, to provide reasonable assurance that HubSpot's service commitments and systems requirements were achieved based on the applicable trust services criteria.

# DESCRIPTION OF THE BOUNDARIES OF THE HUBSPOT PLATFORM SYSTEM

## Company Background

HubSpot, Inc. ("HubSpot") provides software and support through a cloud-based platform to help organizations grow better. The Company's platform includes marketing, sales, service, and content management products. HubSpot's products contain features, tools, and integrations that enable businesses to attract, engage, and delight customers throughout the customer lifecycle. Over 250,000 total customers in more than 120 countries use HubSpot's software, services, and support to transform the way they attract, engage, and delight customers.

HubSpot was founded in 2005 and is based in Cambridge, Massachusetts.

## Description of Services Provided

HubSpot's Platform consists of several integrated products that are bundled into integrated software packages:

- HubSpot CRM
- Breeze
- Marketing Hub
- Sales Hub
- Service Hub
- Content Hub (formerly Content Management System (CMS) Hub)
- Ops Hub
- Commerce Hub

### HubSpot CRM

The core of HubSpot's Platform, the HubSpot CRM, is a single database of lead and customer information that allows businesses to track their interactions with contacts and customers, manage their sales activities, and report on their pipeline and sales. This allows a complete view of lead and customer interactions across HubSpot's integrated applications, giving the CRM substantial power. This integration makes it possible to personalize every aspect of the customer interaction across web content, social media engagement, and email messages across devices, including mobile. The integrated applications on the CRM have a common user interface, are accessed through a single login, and are based on the CRM database. HubSpot CRM is a free product that can be used standalone, or with any combination of Marketing Hub, Sales Hub, Service Hub, CMS Hub, and/or Ops Hub.

### Breeze

Breeze is HubSpot's comprehensive suite of AI tools and features that power the customer platform, including our Smart CRM, engagement Hubs, and the connected ecosystem. Breeze includes Breeze Copilot, an AI-powered companion to boost productivity and make work easier; Breeze Agents to help teams automate work, end-to-end, from strategy to execution; and Breeze Intelligence, a data enrichment solution to provide a complete and unified view of the customer, and features across the CRM and Hubs built on Breeze.

### Marketing Hub

Marketing Hub is an all-in-one toolset for marketers to attract, engage, and nurture new leads towards sales readiness over the entire customer lifecycle. Marketing Hub is available in both free and paid tiers, and can be used standalone, with HubSpot CRM, and/or any version of Sales Hub or Service Hub. Features include marketing automation and email, social media, search engine optimization (SEO), CRM Sync, and reporting and analytics.

### Sales Hub

Sales Hub was introduced to enhance the productivity and effectiveness of sales representatives. Businesses can empower their teams with tools that deliver a personalized experience for prospects with less work for sales representatives. Sales Hub is available in both free and paid tiers, and can be used with HubSpot CRM, a third-party CRM, and/or any version of Marketing Hub or Service Hub. Features include: email templates and tracking, conversations and live chat, meeting and call scheduling, lead and website visit alerts, sales automation, and lead scoring.

### Service Hub

Service Hub is our customer service software that is designed to help businesses manage and connect with customers. Service Hub is available in free and paid tiers, and can be used standalone, with HubSpot CRM Free, and/or any version of Marketing Hub or Sales Hub. Features include: conversations and live chat functionality, conversational bots, tickets and help desk, automation and routing, knowledge base, team emails, feedback and reporting tools, and customer goals.

### Content Hub (formerly CMS Hub)

Content Hub combines the power of customer relationship management and a content management system into one integrated platform. HubSpot artificial intelligence (AI)-powered content tools enable businesses to create and manage new and existing web content while also personalizing their websites for different visitors and optimizing their websites to convert more visitors into leads and customers. Content Hub can be purchased as a standalone product and/or with any version of Marketing Hub, Sales Hub, or Service Hub. Features include: website pages, business blogging, smart content, landing pages and forms, SEO tools, forms and lead flow, web analytics reporting, calls-to-action, and file manager.

### Ops Hub

Ops Hub is an operations software that lets users easily sync, clean, and curate customer data, and automate business processes. Ops Hub enables entire teams to stay aligned with a clean, connected source of truth for customer data. Features include: programmable automation, data sync, data curation, and data quality tools.

### Commerce Hub

Commerce Hub includes all the tools and integrations necessary to manage payments in HubSpot. Request and collect payments, streamline subscriptions, and increase efficiency with automation and reporting.

## **System Boundaries**

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Included within the scope of this report are controls over systems and subprocessors supporting functionality (including AI-powered features and functionality) within the covered services that have publicly launched in general availability.

Excluded from the scope of this report are security controls under the purview of the third-party data center colocation facilities. Currently, alpha and beta systems are excluded from the scope of this report; however, they are supported by HubSpot's core infrastructure.

## **Principal Service Commitments and System Requirements**

HubSpot designs its processes and procedures related to the HubSpot Platform to meet its objectives for its HubSpot Platform services. Those objectives are based on the service commitments that HubSpot makes to user entities, the laws and regulations that govern the provision of the HubSpot Platform services, and the financial, operational, and compliance requirements that HubSpot has established for the services. The HubSpot Platform services are subject to the relevant regulatory and industry information and data security requirements in which HubSpot operates.

Security, availability, and confidentiality commitments to user entities are documented and communicated in customer agreements and in the Data Processing Agreement, which is published online. The principal security, availability, and confidentiality commitments are standardized, and include, but are not limited to, the following:

## Security

- Maintain administrative and logical safeguards to protect the security and integrity of the HubSpot Platform and customer data in accordance with HubSpot's security requirements.
- Use formal access management processes for the request, review, approval, and provisioning of HubSpot personnel with access to production systems.
- Use formal HR processes including: security awareness training, security and acceptable use policy, and a formal code of conduct.
- Use commercial industry standard secure encryption methods to protect customer data at rest and in transit.
- Maintain secure software development processes to help ensure consistent quality that goes across policy, people, processes, and technology.
- Employ a dedicated product security incident response team that follows industry best practices in managing and responding to security vulnerabilities to minimize customers' risk of exposure.
- Maintain anti-virus protection, perform vulnerability scanning, and conduct periodic penetration testing to detect and prevent security vulnerabilities from being introduced into production systems.
- Use Web Application Firewall (WAF) solutions to protect hosted customer websites and other internet-accessible applications.

## Availability

- Employ infrastructure providers who use commercially reasonable efforts to help ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and heating, ventilation, and air conditioning (HVAC) services.
- Use backup and replication strategies that are designed to help ensure redundancy and fail-over protections during a significant processing failure.
- Maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes.

## Confidentiality

- Maintain customer data as confidential and not disclose information to any unauthorized parties without written consent and notify customers should there be a breach of their data.
- Delete or return customer data upon contract termination or expiration in accordance to specified timeframes set out in the customer agreements.
- Delete customer data outside of scheduled data disposal periods upon request.

HubSpot establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements.

Such requirements are communicated in HubSpot's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These policies include ones around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the HubSpot Platform.

In accordance with HubSpot's assertion and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to system users individually.

## Infrastructure and Software

HubSpot uses cloud storage and compute services from Amazon Web Services (AWS) and Google Cloud Platform (GCP), and data center hosting services from TierPoint, LLC. HubSpot does not own or maintain hardware located in the AWS and GCP data centers and operates under a shared security responsibility model, where AWS and GCP are responsible for the security of the underlying cloud infrastructure (i.e., physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer and storage) and HubSpot is responsible for securing the application platform deployed in AWS and GCP (i.e., applications, identity access management, operating system and network virtual security groups configuration, network traffic, server-side encryption). HubSpot also does not own or maintain hardware located in the TierPoint data center and does not own any of the underlying infrastructure. Production servers and client-facing applications are logically and physically secured from HubSpot's internal corporate information systems.

A combination of internally-developed, externally-supported, and wholly-purchased applications support the HubSpot application platform, and is summarized as follows:

- The production infrastructure is centralized in AWS and GCP cloud hosting facilities and is managed by the HubSpot engineering team.
- The application platform utilizes containerized applications in a clustered environment for many services for security and reliability.
- Infrastructure Automation services are used to deploy and manage the lifecycle of public cloud instances with appropriate configuration and to prevent configuration drift.
- The job scheduler platform manages data feeds that run continuously, on-demand, or on a configured schedule.
- Automated segregation of duties (SoD) tools utilize branch protections in GitHub to enforce independent peer review and sign-off on high-risk changes as well as to perform evaluation tasks to detect potential security changes in a pull request before it is eligible for deployment to production.
- HubSpot's compliance system hosts, aggregates, and reports on access, change, and employee events.
- Multiple security zones are utilized to segment and administer the production environment.

HubSpot's core infrastructure is spread across multiple availability zones, with data centers in the United States (US), European Union (EU), Canada, and Australia. HubSpot's Infrastructure team monitors the performance of infrastructure resources and provides additional resources as capacity requires.

HubSpot has selected several vendors to provide important aspects of the application hosting framework used to support a robust cloud infrastructure for HubSpot applications. The production stack leverages the following services, provided by third parties:

- AWS: Core cloud hosting infrastructure based on AWS
- GCP: Supplemental cloud hosting infrastructure based on GCP
- Single Sign-On (SSO)
- Cloud based data warehousing: Customer reporting across data sets

These vendors help provide the platform with secure and reliable access to users, manageability by system administrators, and seamless upgradeability.

## People

The following groups contribute to the management and oversight of our internal control environment:

- Board of Directors – responsible for overseeing the business on behalf of shareholders.

- Executive Leadership – responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
- Systems Operations – responsible for managing and supporting HubSpot's corporate network and infrastructure.
- Legal – responsible for overseeing all legal matters affecting HubSpot, developing team strategy, and advising senior leadership.
- Internal Audit - Comprised of Internal Audit and Enterprise Risk:
  - Internal Audit – responsible for independent, objective assurance and consulting services designed to add value and improve HubSpot's operations.
  - Enterprise Risk – responsible for ensuring risks to the business are identified and effectively managed throughout the growth and evolution of the company.
- PeopleOps – responsible for developing and implementing HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- Engineering (Compliance Assurance) – responsible for identifying and monitoring technology risks, managing the assessment and mitigation of said risks and enforcing compliance of security issues and incidents throughout the service delivery infrastructure.
- Engineering (Product) – responsible for developing applications and services that compose the HubSpot Platform.
- Engineering (Platform Infrastructure) – responsible for managing and supporting tooling to build, deploy, run, and monitor the microservices and frontends that make up the HubSpot Platform.
- Engineering (Security) – responsible for managing and supporting tooling around the authentication, authorization, and provisioning for both internal use as well as for third-party cloud providers. Responsible for identifying, detecting, assessing, responding, and remediating security risks and incidents.
- Engineering (Data Infrastructure) – responsible for managing and supporting HubSpot's unified data platform.
- Customer Services – responsible for supporting and onboarding customers.
- Customer Support – responsible for providing technical support for customers to assist with the proper use of the HubSpot platform.

## Procedures

### *Authentication and Authorization*

Access to HubSpot internal systems is protected by multiple authentication layers. A valid unique username and password is required to access the HubSpot corporate network. To access key in-scope systems from outside the office, HubSpot personnel are required to first connect via encrypted remote access tools or Identity Aware Proxy (IAP) system using a username and password with non-replayable multi-factor authentication (MFA). The corporate platform is managed through AD and many key systems are integrated with AD. HubSpot employees are able to access the integrated systems through SSO. The engineering environment is logically segregated from the corporate environment and provides HubSpot personnel access to product infrastructure. Authentication to the product infrastructure is managed through an IDAM system. Authentication to the IDAM follows the same process of authenticating through a unique username and password as when in the HubSpot office. When accessing the IDAM remotely, a secure remote connection and MFA are required. Once authenticated, HubSpot personnel can access production systems. The authentication of each integrated system to the IDAM can vary, where certain systems are configured with a lightweight directory access protocol (LDAP) binding to the IDAM, while others use a privileged access management tool requiring an active IDAM account with specific group memberships. AWS requires a separate username and password paired with MFA. Tokens for application access to the secrets management system are distributed via the Infrastructure Automation system.

Management has restricted administrative access privileges within the production environment to authorized personnel. Administrative access to each in-scope system may be derived from assignment to privileged groups in AD or the IDAM; however, certain systems are restricted from having continuous administrative access. For these systems, a Just-In-Time Access (JITA) process is in place to request temporary administrative access for the purpose of performing job duties. Each JITA request is documented, tracked, and reviewed. Access is temporarily allowed and activity is logged for high risk actions performed during the session. After the configured session limit, access to the account expires and is automatically revoked.

A privileged access management (PAM) system is used to control access to secrets and passwords associated with service accounts, integrations, and interactive administrative accounts on supporting systems outside of the production Product environment. The PAM system permits members of small, trusted teams to access these secrets and passwords on a temporary basis which is preceded by an approved request. Access attempts are logged and the activity is monitored & reviewed retroactively.

#### *Access Requests and Access Revocation*

Processes have been established by HubSpot to manage user access requests, modifications, and deletions. The process varies based on the type of access needed and whether the system is related to corporate or product infrastructure. Administrative and high-risk access is either pre-authorized based on the employee's functional role in the Company or authorized through an in-workflow approval prior to provisioning. Users requesting a modification for additional access will follow the same process.

New access is detected automatically by the compliance system and, if appropriate, routed to the appropriate personnel for retroactive approval as well. Additionally, user access and permissions to the key in-scope systems are reviewed semi-annually to help ensure that only authorized individuals have access to key in-scope systems and that the access granted to these users is necessary for their job function. The same access review and re-approval process is automatically triggered when employees transfer to new roles, as reported in the HubSpot Human Resources Management System (HRMS).

Logical and physical access removal to the in-scope systems upon employee termination is also triggered automatically based on the integration with the HubSpot HRMS. If automated access removal is not technically possible, an automated notification is sent to the team responsible for access management requesting access removal.

#### *Network and Data Security*

Multiple access control lists (ACLs) are in place to protect the production network and are utilized to restrict access and filter unauthorized traffic. Restrictions are put in place for certain traffic to pass through the firewall to communicate with the production servers. Each firewall is configured to deny connections that are not explicitly authorized by the security groups ruleset. In addition, the firewall rulesets are reviewed on an annual basis to help ensure that only necessary connections are configured. The reviews certify that the implemented firewall policies and rules function as intended. A WAF solution is also in place to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services. Instances within the HubSpot production environment are hardened in accordance with applicable benchmark settings issued by the Center for Internet Security (CIS). Operating systems used in production are scanned on a monthly basis for compliance against the CIS benchmark.

To further protect the network, endpoint detection and response solutions are installed on the company-owned laptops and corporate network Windows/Linux servers. The endpoint detection and response solutions are configured to detect and prevent malicious activity on registered endpoints, including scanning for and blocking access to malicious content and execution of high-risk applications. Endpoints are configured for full disk encryption and to time-out a user's session after 20 minutes of inactivity. Security checks are also performed on company and personal (BYOD) endpoints attempting to connect to the SSO provider. Devices that do not meet security standards are blocked from logging into the SSO provider. Encryption is also utilized on web servers for web communication sessions. Additionally, an email security solution is used to monitor for and block malicious email, and scan for malicious URLs and attachments within emails. HubSpot also performs periodic phishing simulation exercises to refresh and reinforce employee training and awareness of phishing attacks.

To protect customer data, HubSpot stores data on encrypted disks where access to the cryptographic keys is restricted to authorized personnel. Data residing both in AWS and in GCP is encrypted at rest.

### *Media Handling and Disposal of Data*

Asset disposal procedures are in place to guide personnel in disposing of technology equipment when they reach the end of their life. HubSpot relies on disk encryption and the established AWS and GCP secure media disposal processes to help ensure safe decommissioning.

HubSpot maintains a data subject request form for requests from customers and prospects regarding data deletion, portability, and general inquiries. The HubSpot Legal and Compliance team monitors and tracks the requests through completion. Datastores that contain customer data are configured to listen for message streams that indicate a deletion request and delete the data. This configuration is monitored, and any discrepancies in configuration will generate a ticket for investigation and remediation.

### *Change Management*

The HubSpot system development process is a formalized, process-driven approach intended to maintain the stability of production systems. This process dictates how changes to HubSpot-developed systems are documented, tested, reviewed, approved, and deployed. Program change documents and security best practices are documented on the HubSpot intranet and within the Engineering documentation repository.

HubSpot follows a standard GitHub Pull Request development process for internally developed high-risk system changes wherein engineers create feature branches, work on them until a change is ready to be released, and then create a pull request. The pull request is used as a mechanism to seek feedback from other engineers, acquire approvals for high-risk changes, and discuss any changes before the code is merged back into the master branch of the code repository. HubSpot uses a combination of GitHub features such as status checks and protected branches to automatically enforce a series of checks that must be completed before a pull request is eligible to be merged into the master branch. Checks include code review, testing (where applicable), and merge approval from an engineer who did not author the change or commit the code. To automate the deploy process, continuous integration and deploy tools are used, including building, testing, tagging, versioning and releasing deployable artifacts to production. Access to implement changes into the production environment is restricted to authorized personnel and segregated from the development environment. For internally developed changes, only signed deployables are allowed to run in the production environment.

Emergency changes follow a similar process to standard development with the exception that approvals do not need to be provided in advance of a production deployment. In an emergency scenario, engineers have the ability to “self-sign” their code which will trigger the creation of an incident in HubSpot’s compliance system. Each such incident requires retroactive review and approval by Engineering management.

HubSpot utilizes a configuration management tool to help ensure baseline configurations are consistently applied. In the event that a production server deviates from the baseline configuration, it will be overwritten with the baseline configuration within 30 minutes.

Manual/third-party system configuration changes are authorized, designed, developed, and managed through change ticket approval workflows or compliance system review workflows.

### *Data Backup and Disaster Recovery (DR)*

Key systems are backed up on a regular basis with established schedules and frequencies. Backups are monitored for successful execution, and alerts are generated in the event of an unsuccessful execution. Failure alerts are escalated, investigated, and resolved.

Data is backed up at least daily, and most data is backed up more frequently to AWS in order to permit the resumption of operations in the event of a disaster. Monitoring is in place and alerts automatically inform the responsible team if the replication job fails so teams can triage. Additionally, backups are copied periodically to an alternate AWS region located within the jurisdiction of the primary AWS data center to help ensure recovery in the event of a complete regional outage.

HubSpot has a disaster recovery plan that details how the Company sustains internal corporate and product infrastructure in the event of a disaster. The disaster recovery plan is documented, updated, and tested annually.

Each system has mapped-out recovery test steps and is tested against a predefined Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Disaster recovery testing methods include:

- Desk check – stakeholders review the content of a disaster recovery plan.
- Automated Backup Testing – a scheduled job is developed to automate the restoration of a recent backup as a test of the recovery process.
- Table-top exercise – members of the disaster recovery team gather and roleplay a disaster scenario.
- Simulation test – support personnel meet while a disaster is simulated.

### *Incident Response*

Data breach response and incident response policies and procedures are in place to manage unexpected incidents impacting the business and are provided to internal users to aid in identifying and reporting failures, incidents, concerns, and other complaints. These procedures are reviewed and tested on an annual basis to help ensure they are effectively meeting business objectives.

The identification of and response to a critical situation (CritSit) follows multiple steps. When an event is first reported, the event is triaged and classified. For events that are classified as incidents, personnel utilize a CritSit repository to document the incident and subsequent steps. Individuals are involved as necessary for containment, eradication, recovery, and corrective action to restore services and mitigate risks. For each CritSit, a postmortem is run to identify actions that can be taken to prevent future outages. Corrective measures or changes that occur because of CritSits and identified deficiencies follow the standard change control process.

CritSits are classified by severity. CritSits range from SEV-1 to SEV-5, and additionally include a SEV-NA category. A classification of SEV-1 is critical while SEV-5 is minor customer impact; SEV-NA indicates no customer impact. Triage and tactical members, including members of the Legal - Privacy, Security & Risk, Corporate Security, Trust & Safety and/or Infrastructure Security teams are notified when CritSits are further escalated as the result of potential or confirmed unauthorized access to HubSpot Product or Corporate infrastructure. Potential and confirmed personal data breaches are managed through closure in a system that facilitates both legal and security responses and the documentation of any such breach.

### *System Monitoring*

HubSpot utilizes monitoring software to help detect potential anomalous activity related to security, such as product abuse, malicious activity, and login/user anomalies, as well as availability-related issues. Anomalous events are flagged within the software and organized by severity, time of appearance, and the search that detected them. Each event is reviewed by the impacted system's owning team and is tracked through closure. If an event indicates significant Customer impact, a CritSit may be opened. Anomalous activity has also been defined to include policy/configuration changes and anomalies in critical systems impacting the availability of the HubSpot product.

Additional system monitoring includes internal vulnerability scans over AWS, web application vulnerability scans over the HubSpot product, as well as penetration testing for HubSpot products and infrastructure. Vulnerability scans are configured to scan for exploitable vulnerabilities on a daily basis. Remediation tickets are automatically created from the vulnerability scans. Findings from the vulnerability scans are triaged for false positives, and tickets are created for true vulnerabilities and monitored through resolution. Remediation tickets are created from the penetration testing report findings and are triaged and monitored through resolution.

## Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Customer contract information Disaggregated / identified Customer contact data Customer Intellectual Property or business data Customer communications (chat transcripts, AI prompts, email bodies, email attachments, etc.)	Private Customer and Company Data	Restricted
Customer "Deal Data" App usage data – Identified Customer support requests Online identifiers (IP addresses, cookie info, etc.) for HubSpot users Aggregated / de-identified customer data Metadata about customer communications (time, to/from, etc.)	Contact Insights and Browsing Information	Confidential
Customer names Aggregated / de-identified HubSpot usage data	Anonymized Data	Internal Only
Company names Other general information	Public Data	Public

## Subservice Organizations

The cloud storage, compute services, and data center hosting services provided by AWS, GCP, and TierPoint were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, GCP, and TierPoint, alone or in combination with controls at HubSpot, and the types of controls expected to be implemented at AWS, GCP, and TierPoint to meet those criteria.

Control Activities Expected to be Implemented at Subservice Organizations	Applicable Trust Services Criteria
AWS and GCP are responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where HubSpot applications reside.	CC6.1 – CC6.3, CC6.6
AWS, GCP, and TierPoint are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
AWS and GCP are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where HubSpot systems reside.	CC6.7
AWS and GCP are responsible for monitoring anomalies that are indicative of natural disasters within the data centers as well as physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC7.2

Control Activities Expected to be Implemented at Subservice Organizations	Applicable Trust Services Criteria
AWS, GCP, and TierPoint are responsible for ensuring the data center facility is equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

### Complementary Control Responsibilities at User Entities

HubSpot's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

However, in order for user entities to benefit from the HubSpot Platform system and its controls, the following responsibilities should be considered by user entities:

#	Control Responsibilities to be Considered by User Entities	Related Applicable Trust Services Criteria
1.	User entities are responsible for implementing controls to ensure that identity and entitlement grants on their HubSpot instance are appropriately authorized prior to provisioning.	CC6.2 - CC6.3
2.	User entities are responsible for enforcing multi-factor authentication (through HubSpot or Single Sign-On) to access their HubSpot portal and avoid simple password-based authentication.	CC6.1, CC6.6 - CC6.7
3.	User entities are responsible for implementing controls to ensure that access is deprovisioned when users are no longer authorized to access their HubSpot portal.	CC6.2 - CC6.3
4.	User entities are responsible for the integrity, accuracy, and completeness of data entered into HubSpot.	CC6.7
5.	User entities are responsible for reviewing events in their portal logs and reporting suspicious account activity or potential security incidents to HubSpot.	CC6.6, CC6.8, CC7.1 - CC7.2
6.	User entities are responsible for reviewing and authorizing third-party integrations, including those in the HubSpot Marketplace.	CC6.6
7.	User entities are responsible for adhering to HubSpot's terms of service.	CC6.7
8.	User entities are responsible for reviewing HubSpot's subprocessors relevant to features used by the user entity and opting in to subprocessor change notifications.	CC9.2

### Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the HubSpot Platform system.

## **Hubspot Compliance FAQs**

# HubSpot Compliance FAQs

Last Update: June 2025

We get a number of questions about HubSpot's compliance posture, and so have created this guide to address queries that come up frequently. For more information about HubSpot's security, privacy, and compliance programs, please see the [HubSpot Trust Center](#).

## SOC 2 Report

### 1. What is new in our 2025 SOC 2 report?

- HubSpot has added enhancements to several existing controls and added several net-new controls to the 2025 SOC 2 Type 2. These enhancements were made to strengthen HubSpot's posture on security, availability, and confidentiality and to enhance customer trust and assurance that their data is protected.

Control Activity Specified by the Service Organization	Applicable Trust Services Criteria	Change from 2023 SOC 2 Type II
Corporate and security policies are stored within a centralized repository and made available to employees.	CC1.4 CC2.2 CC5.3	Net-New Control
Control owners or other responsible parties review and provide updates to key control narratives on a quarterly basis. The Compliance Assurance team reviews the suggested changes and updates the control narratives if applicable.	CC4.1	Net-New Control
Documented electronic session policies and procedures are in place that includes the termination of sessions after a predetermined time of inactivity.	CC6.1	Net-New Control
Security checks are performed on mobile devices and laptops prior to accessing	CC6.7	Net-New Control

company systems and data. Non-compliant devices are blocked.	CC6.8	
Disk encryption software is utilized on all workstations to help ensure that data is secured in the event that a workstation is lost or stolen.	CC6.7 CC6.8	Net-New Control
HubSpot runs a bug bounty program which allows external parties to identify and report vulnerabilities or bugs within the HubSpot product. Confirmed findings are tracked to remediation.	CC7.1 CC7.2	Net-New Control
Management requires full-time employees to complete the Code of Business Conduct and Ethics training as part of the employee onboarding process and annually thereafter. Legal personnel review the training log quarterly to help ensure that new hires completed the onboarding training within 90 days of hire and followed up on any exceptions.	CC1.1	Control updated (see bold for additions)

- Our report covers all systems and subprocessors that support and deliver feature functionality for all features that have launched in General Availability (GA) on or before 4/30/2025. Features and functionality that have launched in GA on or before 4/30/2025 (Including [Breeze](#) and our three new Regional Data Centers) are now covered by our report.
  - Note: Any features that were in alpha or beta as of 5/1/2025 are not covered under the scope of the report. Please refer to the Useful Resources section below for a link to subscribe to [HubSpot Subprocessor updates](#).

## 2. What is SOC 2 and what value does it bring to HubSpot?

SOC stands for "Service Organization Control," and its associated report is issued by an independent auditor. The independent auditor uses the SOC 2 framework to assess how well a service provider complies with one or more of the following trust principles: security, availability, confidentiality, processing integrity and privacy. The SOC 2 examination process is used to demonstrate that the service organization (in this case HubSpot) has

effective controls in place to reduce the risks associated with the delivery of products or services they provide.

HubSpot has obtained a SOC 2 Type 2 report, which attests to the controls in place governing the availability, confidentiality, and security of customer data. These controls map to the Trust Service Principles (TSPs) established by the American Institute of Certified Public Accountants (AICPA). We invite our customers to review a copy of our SOC 2 Type 2 report by downloading it from [HubSpot Trust Center](#).

### 3. What is the difference between SOC 2 Type 1 and SOC 2 Type 2 report?

The key difference between the two reports is that a SOC 2 Type 1 report verifies that the service provider has the right controls in place. A SOC 2 Type 2 report attests that the right controls are in place, and also that the controls operate effectively over time. We can see this difference in how each report is audited. A SOC 2 Type 1 report is audited at one specific point in time. A SOC 2 Type 2 report is audited over a period of time, typically six months or one year.

### 4. Does HubSpot have a SOC 1 report?

HubSpot does not currently offer a SOC 1 report. However, a SOC 2 Type 2 report covers a number of related (and at times, overlapping) IT risks. Please refer to the [HubSpot Trust Center](#) to obtain our SOC 2 Type 2 report.

### 5. What is the difference between a SOC 2 report and a SOC 3 report?

The key difference between a SOC 2 and a SOC 3 report is the level of detail and accessibility of the information provided.

A SOC 2 report is a more comprehensive examination of an organization's internal controls related to security, availability, confidentiality, processing integrity, and/or privacy. A SOC 2 report is more detailed and provides a more comprehensive understanding of an organization's controls. SOC 2 reports are issued to the organization being audited and can be requested from the organization, but are not generally available to the public.

On the other hand, a SOC 3 report is a simplified version of the SOC 2 report and provides only a summary of the organization's controls and processes. It focuses on the organization's controls at a high-level, without providing the same level of detail as the SOC 2 report. SOC 3 reports are typically made available to the public.

## 6. Does HubSpot have a SOC 3 report?

Yes. The SOC 3 report can be downloaded from the [HubSpot Trust Center](#).

## 7. When is the SOC 2 report released?

HubSpot SOC 2 reports are usually released on an annual basis. The availability of the new report depends upon the audit period. HubSpot's most current SOC 2 report can be found in the [HubSpot Trust Center](#). You can subscribe to the Trust Center updates within the Trust Center and be notified when new reports are released.

## 8. What period of time does the SOC 2 report cover and does it expire?

SOC 2 Type 2 reports cover a specific lookback period, typically a year. For HubSpot's report, the lookback period is May 1 - April 30. Once the period ends, the audit begins and takes a few months, and then the new report is released. SOC 2 reports don't "expire," because they are always going to cover a previous time period. Please see FAQ #8 for more information.

## 9. What is a bridge letter and why would a customer request them?

A bridge letter is a document used to "bridge" the gap between the end of a prior reporting period and the issuance of the new SOC 2 report.

The purpose of a bridge letter is to provide an understanding of the changes, if any, that have taken place between reporting periods and to ensure continuity of information for customers and prospects.

You may obtain HubSpot's bridge letter directly from the [HubSpot Trust Center](#). Updated bridge letters are published on a quarterly cadence.

## 10. Can HubSpot provide other vendor's SOC 2 reports?

No. Due to our agreements with our service providers, HubSpot is unable to share their confidential compliance documentation on their behalf. HubSpot's third party risk management controls are included in the scope of our SOC 2 report, and include initial and annual security reviews for vendors which process customer data.

## HIPAA

HubSpot undergoes an annual HIPAA Type 1 assessment with an independent assessor to demonstrate our adherence to the HIPAA Security and Breach Notification Rules.

The attestation applies to covered services for Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA). Please see our Sensitive Data Terms for the full list of permitted services and covered data:

<https://legal.hubspot.com/sensitive-data-terms>.

## Other Regulations and Frameworks

### 1. Does HubSpot have ISO 27001 certification?

No. HubSpot and its products are not certified against ISO 27001 standards. However, our SOC 2 Type 2 provides assurance of the security, availability, and confidentiality of the HubSpot Platform. We encourage you to obtain and review a copy of our SOC 2 report from the [HubSpot Trust Center](#).

### 2. Is HubSpot PCI DSS compliant? Does HubSpot process credit card information?

Yes, HubSpot is PCI DSS compliant because HubSpot does not directly process or store credit card information.

Commerce Hub offers two payment processing options to customers: HubSpot payments and Stripe payment processing. Both of these options use infrastructure provided by Stripe, Inc., a leading provider of digital payments infrastructure. Stripe's infrastructure is certified

to comply with the Payment Card Industry's Data Security Standards (PCI-DSS) Level 1, the payment industry's highest level of protection. As part of our payments offerings, HubSpot does not store, process, or collect credit card information submitted to us by customers. For HubSpot payments and Stripe payment processing, we qualify for completion of a SAQ-A which we submit to our payment processor. The SAQ-A report for each payment product is available on the [HubSpot Trust Center](#).

Customers who have a Stripe account may obtain Stripe's compliance documentation, including PCI AOC, SOC 1, and SOC 2 reports, from their Stripe portal.

HubSpot is unable to provide Stripe's SOC 1 or SOC 2 reports to customers or prospects who do not have a direct relationship with Stripe. Stripe's PCI compliance status can be found on the [Visa PCI service provider registry](#).

### 3. Is HubSpot SOX compliant?

Yes. Public information about HubSpot's SOX compliance is available as part of our SEC filings. Our SEC filings and financial reports are publicly available on our [Investor Relations](#) page.

### 4. Is HubSpot FedRamp compliant?

No. HubSpot is not a FedRAMP authorized provider. However, has obtained SOC 2 Type 2 certification. We invite customers to obtain a copy of our SOC 2 Type 2 and SOC 3 reports by downloading it from the [HubSpot Trust Center](#).

### 5. Is HubSpot ITAR compliant?

HubSpot is not ITAR compliant and has never been formally or informally assessed against NIST 800-171. However, we do incorporate NIST recommendations into our security program and controls.

## Useful Resources

### HubSpot Trust Center Documents

Security & Compliance Overview	Details the Security Controls that we use to safeguard our customers' and users' data.
Network Diagram	<p>HubSpot maintains detailed information and diagrams about its network architecture.</p> <p>A high level Customer Network Diagram is available for customers and prospects.</p>
Penetration Test Reports	<p>HubSpot engages with industry-recognized, third-party penetration testing vendors to perform penetration tests against HubSpot's corporate infrastructure and web applications at least once per year.</p> <p>Our latest Corporate and Application Penetration Test Summaries are available for download.</p>
SOC 2 Report Type 2	<p>HubSpot is audited annually as part of SOC 2 compliance to attest to our controls in the domains of security, availability, and confidentiality.</p> <p>Our SOC 2 Report is available for request.</p>
SOC 3 Report	The SOC 3 is a general-use report that attests to HubSpot's completion of our SOC 2, and our commitment to the security, availability, and confidentiality of customer data.
SOC 2 Report Bridge Letter	A bridge letter is a document that informs users of our SOC 2 report of

	changes, if any, regarding HubSpot's services and the related controls, for the period of time that has elapsed since the end of the review period.
Transfer Impact Assessment (TIA)	Our Transfer Impact Assessment contains more in depth information to support customers conducting a risk assessment of transferring data outside of the EU.
Certificate of Liability	Our Certificate of Insurance outlines our coverage.
Data Processing Agreement	Our Data Processing Agreement sets out how we process Personal Data on your behalf in connection with the Subscription Services provided to you under our agreement with you and how we process Controller Personal Data when you use certain enrichment products and our Hubspot tracking code.  We've also made a signed version available for public download.
Data Privacy FAQ	The Data Privacy FAQ further provides information to address common questions regarding our Data Processing Agreement (DPA) and is available.
CAIQ	We have a pre-completed CAIQ questionnaire available for download.
SIG Lite	We have a pre-completed SIG Lite questionnaire available for download.

## Legal Documents

HubSpot Data Processing Agreement	<a href="https://legal.hubspot.com/dpa">https://legal.hubspot.com/dpa</a>
HubSpot Regional Hosting Policy	<a href="https://legal.hubspot.com/hubspot-regio">https://legal.hubspot.com/hubspot-regio</a>

	<a href="#">nal-data-hosting-policy</a>
HubSpot Privacy Policy	<a href="https://legal.hubspot.com/privacy-policy">https://legal.hubspot.com/privacy-policy</a>
HubSpot Customer Terms of Service	<a href="https://legal.hubspot.com/terms-of-service">https://legal.hubspot.com/terms-of-service</a>
Product Specific Terms	<a href="https://legal.hubspot.com/product-specific-terms">https://legal.hubspot.com/product-specific-terms</a>
HubSpot Cookie Policy	<a href="https://legal.hubspot.com/cookie-policy">https://legal.hubspot.com/cookie-policy</a>

## Relevant Knowledge Base Articles

Knowledge Base: Data Privacy Resources	<a href="https://knowledge.hubspot.com/privacy-and-consent/gdpr-resources">https://knowledge.hubspot.com/privacy-and-consent/gdpr-resources</a>
Knowledge Base: Cookies Set in a Visitor's Browser	<a href="https://knowledge.hubspot.com/privacy-and-consent/what-cookies-does-hubspot-set-in-a-visitor-s-browser">https://knowledge.hubspot.com/privacy-and-consent/what-cookies-does-hubspot-set-in-a-visitor-s-browser</a>
Knowledge Base: Cookies Set on HubSpot's Websites	<a href="https://knowledge.hubspot.com/privacy-and-consent/hubspot-cookie-security-and-privacy">https://knowledge.hubspot.com/privacy-and-consent/hubspot-cookie-security-and-privacy</a>
Knowledge Base: Customize Your Cookie Tracking Settings	<a href="https://knowledge.hubspot.com/privacy-and-consent/customize-your-cookie-tracking-settings-and-consent-banner">https://knowledge.hubspot.com/privacy-and-consent/customize-your-cookie-tracking-settings-and-consent-banner</a>
Knowledge Base: HubSpot Cloud Infrastructure and Data Hosting FAQs	<a href="https://knowledge.hubspot.com/account/hubspot-cloud-infrastructure-and-data-hosting-frequently-asked-questions">https://knowledge.hubspot.com/account/hubspot-cloud-infrastructure-and-data-hosting-frequently-asked-questions</a>
Knowledge Base: Perform a Permanent Delete in HubSpot	<a href="https://knowledge.hubspot.com/privacy-and-consent/how-do-i-perform-a-gdpr-delete-in-hubspot">https://knowledge.hubspot.com/privacy-and-consent/how-do-i-perform-a-gdpr-delete-in-hubspot</a>
Knowledge Base: Resources to Export Customer Data	<p>Export Your Content Data:  <a href="https://knowledge.hubspot.com/account/export-your-content-and-data">https://knowledge.hubspot.com/account/export-your-content-and-data</a></p> <p>Export Contacts, Companies, Deals, or Tickets:  <a href="https://knowledge.hubspot.com/crm-setup/export-contacts-companies-deals-or-tickets">https://knowledge.hubspot.com/crm-setup/export-contacts-companies-deals-or-tickets</a></p>

	<a href="#">kets</a>  Export Your Ads Campaign Data: <a href="https://knowledge.hubspot.com/ads/export-your-ads-campaign-data">https://knowledge.hubspot.com/ads/export-your-ads-campaign-data</a>  Export Your Overall Email Performance Data: <a href="https://knowledge.hubspot.com/email/how-do-i-export-my-overall-email-performance-data">https://knowledge.hubspot.com/email/how-do-i-export-my-overall-email-performance-data</a>
--	---

## Other Resources

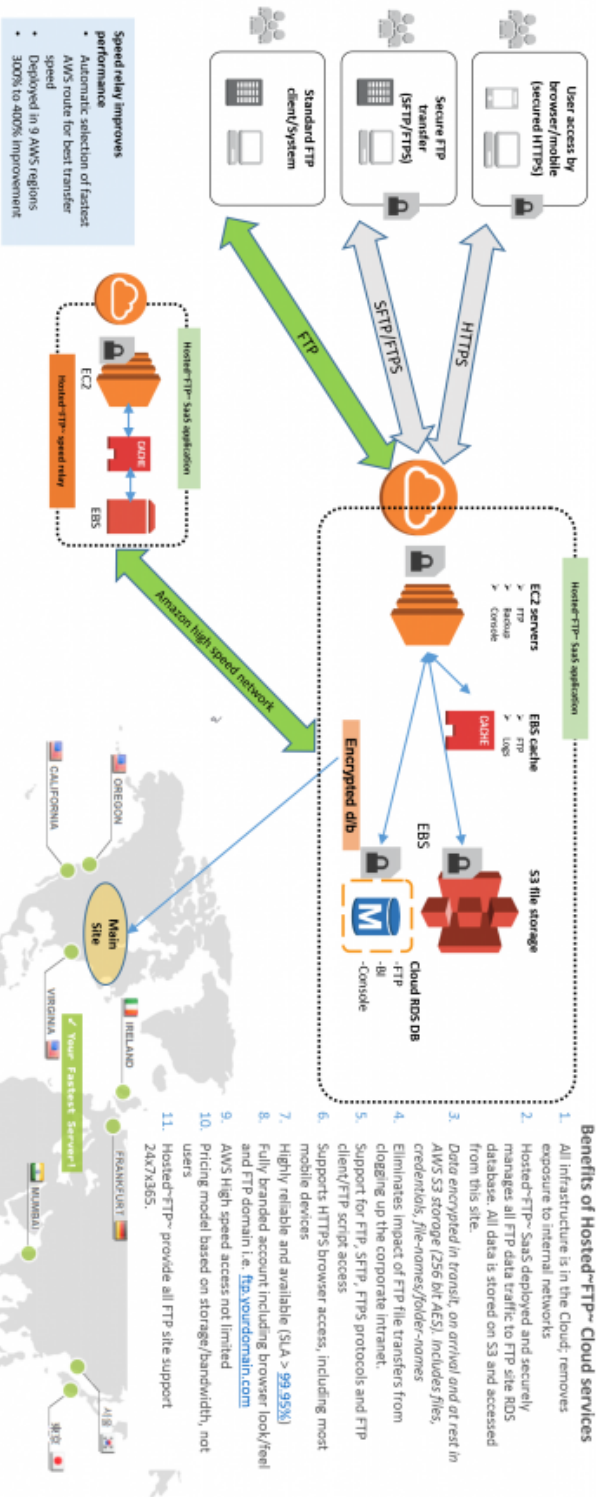
HubSpot Investor Relations	<a href="https://ir.hubspot.com">https://ir.hubspot.com</a>
HubSpot GDPR Guidance	<a href="https://www.hubspot.com/data-privacy/gdpr">https://www.hubspot.com/data-privacy/gdpr</a>
HubSpot Security, Privacy and Control	<a href="https://legal.hubspot.com/security">https://legal.hubspot.com/security</a>
HubSpot's EU Data Center FAQs	<a href="https://www.hubspot.com/eu-data-centre">https://www.hubspot.com/eu-data-centre</a>
Hubspot's GDPR Product Readiness	<a href="https://www.hubspot.com/data-privacy/gdpr/product-readiness">https://www.hubspot.com/data-privacy/gdpr/product-readiness</a>
HubSpot Data Disclosure Policy and Transparent Report	<a href="https://legal.hubspot.com/en/data-disclosure-policy-and-transparency-report">https://legal.hubspot.com/en/data-disclosure-policy-and-transparency-report</a>
Subscribe to Subprocessor Updates	<a href="https://legal.hubspot.com/subscribe-subprocessor-updates">https://legal.hubspot.com/subscribe-subprocessor-updates</a>

## **FTP Server Security Diagram**

# Hosted~FTP~ Multi-tenant Cloud Solution

## Hosted~FTP~ SaaS configuration

High Speed FTP site infrastructure in secure, reliable Amazon Web Services (AWS) locations only.



**Major features & options**  
**FTP Speed relay performance**  
 our unique speed relay infrastructure automatically selects the closest entry point for maximum speed/transfer performance



## **Cyber Security Coverage**

at  
— bay

# Cyber Insurance Policy





# Cyber Insurance Policy Declarations

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

This insurance contract is with an insurer not licensed to transact insurance in this state and is issued and delivered as a surplus lines coverage pursuant to the Tennessee insurance statutes.

This Cyber Insurance **Policy** is issued and delivered as surplus lines coverage pursuant to applicable surplus lines statutes. The surplus lines broker responsible for placement of this coverage is responsible for compliance with applicable surplus lines laws and regulations including completion of any declarations/affidavits and payment of any taxes.

This **Policy** contains one or more Insuring Agreements, some of which provide liability for **Claims** first made against any **Insured** during the **Policy Period**, or any applicable Extended Reporting Period, and reported to us pursuant to the terms of this **Policy**. **Claim Expenses** shall reduce the applicable **Aggregate Limit of Insurance** and Sub-Limits of Insurance and are subject to the applicable **Retentions**. Please read the entire **Policy** carefully.

<b>Policy Number:</b>	AB-6617380-04
<b>Policy Issue Date:</b>	12/30/2024
<b>Home State:</b>	TN
<b>Licensed Surplus Lines Producer:</b>	Pathpoint Insurance Services 200 Pine Street, Suite 200 San Francisco, CA 94104

This Declaration is attached to and forms part of the **Policy**.

<b>ITEM 1: Named Insured:</b>	Caissa Public Strategy, LLC
<b>DBA:</b>	Not Applicable
	5100 Poplar Avenue, Ste 1720
	Memphis, TN38137

<b>ITEM 2: Policy Period:</b>	
<b>Effective Date:</b>	01/13/2025 at 12:01 AM local time of the <b>Named Insured</b>
<b>Expiration Date:</b>	01/13/2026 at 12:01 AM local time of the <b>Named Insured</b>

<b>ITEM 3: Policy Premium:</b>	\$1,483.00
<b>Embedded Security Fee:</b>	\$60.00
<b>Total Policy Cost:</b>	\$1,543.00

Premium:	\$1,483.00
Broker Fee:	\$ 150.00
Carrier Fee:	\$ 60.00
Surplus Lines Tax (5%):	\$ 84.65
Clearinghouse Fee :	\$ 2.96
<b>Total Cost to Insured:</b>	<b>\$1,780.61</b>

<b>ITEM 4: Aggregate Limit of Insurance:</b>	\$1,000,000.
<b>ITEM 5: Notice of Claim or Cyber Event</b>	claims@at-bay.com

At-Bay Insurance Services, LLC  
1 Post Street, 14th Floor  
San Francisco, California 94104

If the amount for ITEM 3, Embedded Security Fee is displayed as "N/A", there is no charge and no **Embedded Security** applicable to this **Policy**. **Embedded Security** includes access to At-Bay Stance™ Exposure Manager and At-Bay Stance™ Managed Security as described in the Embedded Security endorsement.

ITEM 6: Insuring Agreements, Sub-Limits of Insurance, and **Retentions** included:

Insuring Agreements:	Inclusion:	Sub-Limits of Insurance:	Retentions:
A. Information Privacy			
A.1. Information Privacy Liability	Included	\$1,000,000.	\$2,500.
A.2. Regulatory Liability	Included	\$1,000,000.	\$2,500.
A.3. Event Response and Management	Included	\$1,000,000.	\$2,500.
A.4. PCI-DSS Liability	Included	\$1,000,000.	\$2,500.
B. Network Security			
B.1. Network Security Liability	Included	\$1,000,000.	\$2,500.
B.2. Event Response and Recovery	Included	\$1,000,000.	\$2,500.
C. Business Interruption			
C.1. Direct Business Interruption	Included	\$1,000,000.	\$2,500.
C.2. Contingent Business Interruption	Included	\$1,000,000.	\$2,500.
D. Cyber Extortion			
D.1. Cyber Extortion	Included	\$1,000,000.	\$2,500.
E. Financial Fraud			
E.1. Social Engineering	Included	\$100,000.	\$2,500.
E.2. Computer Fraud	Included	\$100,000.	\$2,500.
F. Media Content			
F.1. Media Liability	Included	\$1,000,000.	\$2,500.
F.2. Media Event Response	Included	\$1,000,000.	\$2,500.

If any Inclusion field for an Insuring Agreement is displayed as "Not Included," there is no coverage for such Insuring Agreement.

ITEM 6: Continued

Insuring Agreement:	Inclusion:	Sub-Limit of Insurance:	Retention:
G. Reputational Harm			
G.1. Reputational Harm	Included	\$1,000,000.	\$2,500.

If, in ITEM 6 Continued, the Inclusion field for the G.1. Reputational Harm Insuring Agreement is displayed as “Not Included,” there is no coverage for such Insuring Agreement.

Reputational Harm Indemnity Period:
180 days.

System Failure Enhancement to Business Interruption Insuring Agreements I.C.1. and I.C.2.

System Failure <b>Policy</b> Form:	Inclusion:
Contingent and Direct System Failure:	Included
System Failure Coverage Details:	Value:
<b>Direct System Failure Limit:</b>	\$1,000,000.
<b>Contingent System Failure Limit:</b>	\$1,000,000.
<b>System Failure Waiting Period:</b>	8 hours.
<b>Contingent Non-IT Provider Business Interruption Limit</b>	\$1,000,000.
<b>Contingent Non-IT Provider System Failure Limit</b>	\$1,000,000.

If the Inclusion field for the Contingent and Direct System Failure **Policy** Form is displayed as “Not Included,” it is not included as part of this **Policy**.

Ransomware Event Coverage Details:	Value:
Ransomware Event Sub-Limit Endorsement	
Ransomware Sublimit	Full Limit

ITEM 7: Claims Made Dates:

Claims Made Dates:	Date:
Retroactive Date:	Not Applicable
Continuity Date:	01/13/2022
Prior and Pending Litigation Date:	01/13/2022

ITEM 8: **Policy** Forms:

Form Title:	Form Identification:	Form Edition Date:
Cyber Insurance Policy Declarations	AB-CYB-004	05/2024
Cyber Insurance Policy	AB-CYB-001.2	08/2023
Service of Process Endorsement	AB-CYB-029.2	12/2023
Reputational Harm Insuring Agreement	AB-CYB-034	03/2022
War & Cyber Terrorism Enhancement	AB-CYB-064	03/2022
California Consumer Privacy Act Enhancement	AB-CYB-062	03/2022
Law Enforcement Cooperation Enhancement	AB-CYB-066	03/2022
Voluntary & Preventative Shutdown Coverage	AB-CYB-063	03/2022
Financial Fraud Funds or Securities Endorsement	AB-CYB-050	03/2022
Social Engineering Forged Instruments Carveback	AB-CYB-065	03/2022
Explicit Bricking Coverage Endorsement	AB-CYB-044	03/2022
Affirmative Pay-On-Behalf Intent (1st Party)	AB-CYB-058	03/2022
HIPAA/HITECH Betterment Coverage (\$25,000)	AB-CYB-060	03/2022
PCI-DSS Betterment Coverage (\$25,000)	AB-CYB-081	03/2022
Enhanced Settlement Provision (90/10)	AB-CYB-054	03/2022

Affirmative Voluntary Notification Costs (\$100k)	AB-CYB-056	03/2022
Contingent Bodily Injury Coverage (Sub-Limit)	AB-CYB-068	03/2022
Invoice Manipulation Coverage	AB-CYB-059	05/2024
Funds Transfer Fraud Coverage	AB-CYB-061	03/2022
CryptoJacking & Utility Coverage (Full Limits)	AB-CYB-067	03/2022
Breach Costs Outside (Additional Limit)	AB-CYB-069	03/2022
OFAC Exclusion Endorsement	AB-CYB-095	03/2022
Government Action & Licensing Exclusion	AB-CYB-096	03/2022
Amendment to Pollution and Nuclear, Biological, and Chemical Contamination Exclusions Endorsement	AB-CYB-097	03/2022
Biometric Privacy Violation Exclusion	AB-CYB-098	08/2023
Business Interruption Waiting Period Endorsement	AB-CYB-084	05/2023
Contingent and Direct System Failure (for use with Business Interruption Waiting Period Endorsement)	AB-CYB-085	05/2024
Contingent Non-IT Provider System Disruption (for use with Direct and Contingent System Failure Endorsement)	AB-CYB-117	05/2024
Embedded Security Endorsement	AB-CYB-111	05/2023
Notice to Policyholders - Disclosure Pursuant to Terrorism Risk Insurance Act	ABC-XXX INT N0001 SL	06/2024



Authorized Signature: At-Bay Specialty Insurance Company

	
<b>Rotem Iram</b> President	<b>Roman Itskovich</b> Chief Risk Officer

In witness whereof, At-Bay Specialty Insurance Company has caused this **Policy** to be signed by its authorized officers.

## At-Bay Cyber Incident Roadmap



Notify claim to **claims@at-bay.com**



If you're experiencing a ransomware attack or other system interruption that requires immediate attention, call the At-Bay breach coach: **650.850.5408**



At-Bay Claims will reach out to the insured and determine which, if any, partners are needed



At-Bay Claims (and the breach coach in the event of a ransomware attack or other system interruption) assembles a response team and initiates response to the incident



**At-Bay Claims provides an aligned incident response team to handle all aspects of the incident from the beginning to the end of the claim**



# Cyber Insurance Policy

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

## Considerations:

Wherever appearing throughout this **Policy**, the words "we," "us," and "our" refer to the insurer providing this insurance and "Declaration" and "Declarations" refer to the Cyber Insurance Policy Declarations. Terms which appear in bold face type shall have the meanings set forth in Section V. Definitions.

In consideration of payment of the premium, in reliance upon all information provided to us within the **Application**, and pursuant to the terms, conditions, exclusions, limitations, restrictions, and applicable **Retentions** of this **Policy**, we and the **Insureds** agree as follows:

# I. Insuring Agreements

Coverage is afforded pursuant to those Insuring Agreements included under this **Policy**, displayed as “Included” in ITEM 6 of the Declarations, and for **Claims** and **Cyber Events** reported to us pursuant to the terms of this **Policy**:

## A. INFORMATION PRIVACY

### 1. Information Privacy Liability

We shall pay on behalf of the **Insured**, all **Claim Expenses** and **Damages** resulting from a **Claim** first made against any **Insured** during the **Policy Period** or, if exercised, during the Extended Reporting Period, for an **Information Privacy Wrongful Act**.

### 2. Regulatory Liability

We shall pay on behalf of the **Insured**, all **Claim Expenses**, **Damages**, including **GDPR Penalties**, **Regulatory Penalties**, and **Regulatory Assessments and Expenses** resulting from a **Regulatory Claim** first made against any **Insured** during the **Policy Period** or, if exercised, during the Extended Reporting Period, for an **Information Privacy Wrongful Act**.

### 3. Event Response and Management

We shall pay the **Insured Organization** for **Technical Response Loss**, **Legal Services Loss**, **Public Relations Loss**, **Notification Loss**, **Reward Expense Loss**, and **Credit Monitoring Loss** incurred by the **Insured Organization** as a result of an **Information Privacy Event** first discovered during the **Policy Period**.

### 4. PCI-DSS Liability

We shall pay the **Insured Organization**, all **PCI-DSS Penalties**, **PCI-DSS Response Expenses**, and **Claim Expenses** resulting from a **PCI-DSS Claim** first made against the **Insured Organization** during the **Policy Period** or, if exercised, during the Extended Reporting Period, for an **Information Privacy Wrongful Act**.

## B. NETWORK SECURITY

### 1. Network Security Liability

We shall pay on behalf of the **Insured**, all **Claim Expenses** and **Damages** resulting from a **Claim** first made against any **Insured** during the **Policy Period** or, if exercised, the Extended Reporting Period, for a **Network Security Wrongful Act**.

### 2. Event Response and Recovery

We shall pay the **Insured Organization** for **Technical Response Loss**, **Public Relations Loss**, **Data Recovery Loss**, **Reward Expense Loss**, and **System Restoration Loss** incurred by the **Insured Organization** as a result of a **Network Security Event** first discovered during the **Policy Period**.

## C. BUSINESS INTERRUPTION

### 1. Direct Business Interruption

We shall pay the **Insured Organization** for **Business Interruption Loss, Extra Expense, Reward Expense Loss, and Public Relations Loss** incurred by the **Insured Organization** as a direct result of a **System Disruption** which first occurs during the **Policy Period**.

### 2. Contingent Business Interruption

We shall pay the **Insured Organization** for **Contingent Business Interruption Loss, Extra Expense, Reward Expense Loss, and Public Relations Loss** incurred by the **Insured Organization** as a direct result of a **System Disruption** which first occurs during the **Policy Period**.

## D. CYBER EXTORTION

### 1. Cyber Extortion

We shall pay the **Insured Organization** for **Extortion Loss, Reward Expense Loss, and Public Relations Loss** incurred by the **Insured Organization** as a direct result of an **Extortion Threat** first discovered during the **Policy Period**.

## E. FINANCIAL FRAUD

### 1. Social Engineering

We shall pay the **Insured Organization** for **Fraudulent Inducement Loss and Reward Expense Loss** incurred by the **Insured Organization** as a direct result of **Fraudulent Inducement Instructions** it receives and accepts and which are first discovered during the **Policy Period**.

### 2. Computer Fraud

We shall pay the **Insured Organization** for **Computer Crimes Loss and Reward Expense Loss** incurred by the **Insured Organization** as a direct result of **Computer Crimes** first discovered during the **Policy Period**.

## F. MEDIA CONTENT

### 1. Media Liability

We shall pay on behalf of the **Insured**, all **Claim Expenses and Damages** resulting from a **Claim** first made against any **Insured** during the **Policy Period** or, if exercised, during the Extended Reporting Period, for a **Media Wrongful Act**.

### 2. Media Event Response

We shall pay the **Insured Organization** for **Public Relations Loss and Reward Expense Loss** incurred by the **Insured Organization** as a result of a **Media Wrongful Act** first discovered during the **Policy Period**.

## II. Limits of Insurance

Regardless of the number of **Claims** first made, **Cyber Events** first discovered, or number of Insuring Agreements purchased under this **Policy**:

### A. AGGREGATE LIMIT OF INSURANCE

1. The **Aggregate Limit of Insurance** is our maximum liability under this **Policy** for the duration of the **Policy Period** or, if exercised, the Extended Reporting Period.
2. We shall have no further obligations or liability under this **Policy** upon exhaustion of the **Aggregate Limit of Insurance**, including the continuation of payment of **Loss, Damages**, or **Claims Expenses** or the duty to defend or investigate any **Claim**.

### B. SUB-LIMITS OF INSURANCE

1. The amounts stated as Sub-Limits of Insurance in ITEM 6 of the Declarations, which are part of and not in addition to the **Aggregate Limit of Insurance**, are the most we shall pay for all **Loss, Damages**, and **Claims Expenses** with respect to the Insuring Agreement to which each such Sub-Limit of Insurance applies, and we shall not be responsible to pay any **Loss, Damages**, or **Claims Expenses** under such Insuring Agreement upon exhaustion of such Sub-Limit of Insurance.
2. Subject to II.A.1., II.A.2., and II.B.1. above, the most we shall pay for all **Loss, Damages**, and **Claim Expenses** shall be:
  - a. with respect to any **Cyber Events** or **Claims** which are covered under more than one Insuring Agreement, the sum of the Sub-Limits of Insurance available under the Insuring Agreements to which such **Cyber Events** or **Claims** apply; and
  - b. with respect to any **Related Incidents**, the sum of the Sub-Limits of Insurance available under the Insuring Agreements to which such **Related Incidents** apply.

### III. Retention

1. Our liability shall apply only to that portion of **Loss, Damages, and Claims Expenses** arising from each **Claim** or **Cyber Event** which exceeds the **Retention** applicable to the Insuring Agreement affording coverage to such **Claim** or **Cyber Event**. Payment of such **Retention** is the **Named Insured's** responsibility and remains uninsured under this **Policy**.
2. If a **Claim** is covered under more than one **Third Party Coverage**, each **Retention** shall apply separately but the sum of such **Retentions** shall not exceed the largest applicable **Retention**.
3. If a **Cyber Event** is covered under more than one **First Party Coverage**, each **Retention** shall apply separately but the sum of such **Retentions** shall not exceed the largest applicable **Retention**.
4. The largest applicable **Retention** amount shall apply as a single **Retention** for all **Claims** or **Cyber Events** resulting from **Related Incidents** covered under more than one **Third Party Coverage** or **First Party Coverage**.
5. Solely with respect to **Third Party Coverage** and **Insured Persons**, the **Retention** shall not apply to an **Insured Person** if the **Insured Organization** is:
  - a. not legally permitted to provide indemnification to such **Insured Person**; or
  - b. unable to provide indemnification solely by reason of its financial insolvency, including such **Insured Organization** becoming a debtor in possession under Chapter 11 of the United States Bankruptcy Code, as amended, or the foreign equivalent of such; provided, however, that the applicable **Insured Organization** agrees to repay us any **Retention** amounts we pay on its behalf, as described in this paragraph III.5.b., at the time such **Insured Organization** emerges from financial insolvency or bankruptcy.

## IV. Defense & Settlement of Claims

### A. DEFENSE

1. We shall have the right and duty to defend any **Claim** covered by a **Third Party Coverage** even if the allegations are groundless, false, or fraudulent.
2. We shall consult and attempt to reach an agreement with the **Insureds** regarding the appointment of counsel in the investigation and defense of any **Claim**, but we retain the right to appoint counsel and to investigate and defend any **Claim** as we deem necessary.

### B. SETTLEMENT

1. We shall not settle any **Claim** without the written consent of the **Insured**. In the event the **Insured** refuses to consent to a settlement recommended by us and acceptable to the claimant(s), then:
  - a. we shall pay the sum of all **Damages** for which the **Claim** could have settled plus all **Claim Expenses** incurred up to the time we made our recommendation to the **Insured**; and
  - b. we shall pay and maintain responsibility for eighty percent (80%) of all **Claim Expenses** and **Damages** that are in excess of the amount referenced in paragraph IV.B.1.a. above.

This condition, IV.B. Settlement, shall not apply if the total incurred **Damages** and **Claim Expenses** do not exceed the applicable **Retention** amount.

### C. ALLOCATION

1. If a **Claim** includes both covered and uncovered matters, then coverage shall apply as follows:
  - a. One hundred percent (100%) of **Claim Expenses** incurred by the **Insureds** who are afforded coverage for such **Claim** shall be considered covered; and
  - b. All remaining **Damages** incurred by such **Insureds** from such **Claim** shall be allocated between covered **Damages** and uncovered damages based upon the relative legal and financial exposures and benefits of the parties to such matters.

## V. Definitions

Wherever appearing throughout this **Policy**, the following terms appearing in bold face type, whether used in their singular or plural form, shall have the meanings set forth in this Section V. Definitions:

1. **Aggregate Limit of Insurance** means the amount stated in ITEM 4 of the Declarations.
2. **Application** means all applications, including any information and statements attached thereto, submitted to us by, or on behalf of, any **Insured** in connection with the underwriting and issuance of this **Policy**. All such applications, attachments, information, and materials are deemed attached to and incorporated into this **Policy**.

With respect to publicly held companies, **Application** also means each and every public filing made with the Securities Exchange Commission by or on behalf of any **Insured**, including but not limited to any **Insured Organization's** Annual Report(s), 10-Ks, 8-Ks, and proxy statements, provided that such public filing was filed during the period of time:

- a. beginning at the start of the twelve (12) month period immediately preceding the first submission to us in connection with the underwriting of this **Policy**; and
  - b. ending at the effective date of the **Policy Period**.
3. **Bodily Injury** means physical injury, sickness, or disease and any resulting mental anguish, mental injury, shock, humiliation, or death.
  4. **Business Interruption Loss** means the following amounts incurred by an **Insured Organization** during the **Period of Restoration**:
    - a. net profit before income taxes that would have been earned had no **System Disruption of Insured Computer Systems** occurred;
    - b. net loss before income taxes that would have been avoided had no **System Disruption of Insured Computer Systems** occurred;
    - c. the **Insured Organization's** continuing normal operating and payroll expenses; and
    - d. costs to retain the services of a third party forensic accounting firm to determine the amounts of **Business Interruption Loss** described in paragraphs V.4.a.–V.4.c. above, subject to our prior consent.
  5. **Change of Control** means:
    - a. the acquisition by another person, entity, or group of person or entities acting together, of more than fifty percent (50%) of the outstanding securities, or ownership interests representing the majority and present right to control, elect, appoint or designate the Board of Directors, Board of Trustees, Board of Managers, or functional equivalent thereof, of the **Named Insured**;
    - b. the acquisition by another person, entity, or group of person or entities acting together of all, or substantially all, of the **Named Insured's** assets such that the **Named insured** is not the surviving entity; or
    - c. the merger or consolidation of the **Named Insured** into or with another entity or group of entities acting together such that the **Named Insured** is not the surviving entity.

6. **Claim** means any:
  - a. written demand, request, or assertion seeking monetary damages, or non-monetary or injunctive relief;
  - b. civil proceeding, investigation, or suit commenced by service of a complaint, notice, request for information, or similar proceeding seeking monetary damages or non-monetary or injunctive relief;
  - c. arbitration, mediation, or similar alternative dispute resolution proceeding commenced by the receipt of a complaint, written demand, or similar proceeding seeking monetary damages or non-monetary or injunctive relief;
  - d. criminal proceeding commenced by the filing of charges, arrest or detainment, or a return of an indictment or similar document;
  - e. request to toll or waive a statute of limitations applicable to a **Claim** referenced in paragraphs V.6.a.-V.6.d. above;
  - f. formal appeal of a **Claim** referenced in paragraphs V.6.a.-V.6.d. above;
  - g. with respect to Insuring Agreement I.A.2., any **Claim** referenced in paragraphs V.6.a.–V.6.f. above which is a **Regulatory Claim**; or
  - h. with respect to Insuring Agreement I.A.4., any **Claim** referenced in paragraphs V.6.a.–V.6.f. above which is a **PCI-DSS Claim**.
7. **Claim Expenses** means reasonable and necessary:
  - a. attorneys' fees, mediation and arbitration expenses, expert witness and consultant fees and attendance expenses, and other fees and costs incurred by us, or by an **Insured** with our prior written consent, in the investigation and defense of a **Claim**; and
  - b. premiums for any appeal bond, injunction bond, attachment bond, or any similar bond, although we shall have no obligation to furnish such bond.

**Claim Expenses** shall not include salaries, wages, or other compensation of any **Insured Person**; except to the extent that such **Claim Expenses** are expenses incurred to secure and obtain a member of the **Control Group's** attendance at any mediation, arbitration, hearing, depositions, or trial in connection to the investigation and defense of a **Claim**.
8. **Computer Crimes** means the intentional, fraudulent, or unauthorized input, destruction, or modification of electronic data or computer instructions into **Computer Systems** by any entity which is not an **Insured Organization** or person who is not an **Insured Person**, provided that such **Computer Crimes** cause:
  - a. **Funds or Securities** to be transferred, paid, or delivered; or
  - b. an account of the **Insured Organization**, or of its customer, to be added, deleted, debited, or credited.
9. **Computer Crime Loss** means the **Insured Organization's** loss of **Funds or Securities**.
10. **Computer System** means **Insured Computer Systems** and **External Computer Systems**.

11. **Contingent Business Interruption Loss** means the following amounts incurred by an **Insured Organization** during the **Period of Restoration**:
  - a. net profit before income taxes that would have been earned had no **System Disruption of External Computer Systems** occurred;
  - b. net loss before income taxes that would have been avoided had no **System Disruption of External Computer Systems** occurred;
  - c. the **Insured Organization's** continuing normal operating and payroll expenses; and
  - d. costs to retain the services of a third party forensic accounting firm to determine the amounts of **Contingent Business Interruption Loss** described in paragraphs V.11.a.–V.11.c. above, subject to our prior consent.
12. **Control Group** means an **Insured Organization's** Chief Executive Officer, Chief Financial Officer, Chief Security Officer, Chief Technology Officer, Chief Information Officer, Risk Manager, General Counsel, or any functionally equivalent positions, regardless of title.
13. **Corporate Information** means any confidential or proprietary information of an entity, other than an **Insured Organization**, which:
  - a. an **Insured Organization** is contractually or legally required to hold or maintain in confidence; or
  - b. is not known or accessible by the general public.

**Corporate Information** does not include **Protected Personal Information**.
14. **Credit Monitoring Loss** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to:
  - a. establish and maintain call center services to be used by natural persons whose **Protected Personal Information** was impacted in an **Information Privacy Event**;
  - b. provide credit monitoring, freezing, or thawing services to natural persons whose **Protected Personal Information** was impacted in an **Information Privacy Event**;
  - c. provide identity theft identification and restoration services to those natural persons whose **Protected Personal Information** was impacted in an **Information Privacy Event**; and
  - d. retain the services of a **Cyber Response Firm** to provide consultative and professional services related to **Credit Monitoring Loss** described in paragraphs V.14.a.–V.14.c. above.

**Credit Monitoring Loss** includes costs and expenses incurred in order to comply with applicable **Privacy Regulations** and shall follow the law of the applicable jurisdiction which most favors coverage for such costs and expenses. Those costs and expenses not required to comply with **Privacy Regulations** require our prior consent.
15. **Cyber Event** means an **Information Privacy Event, Network Security Event, Extortion Threat, Fraudulent Inducement Instructions, Computer Crimes, System Disruption**, and, with respect to Insuring Agreement I.F.2. only, a **Media Wrongful Act**.
16. **Cyber Response Firm** means:
  - a. any firm listed on our pre-approved response provider list, available upon request from us; or
  - b. a firm not part of paragraph V.16.a. above, but only with our prior written consent.

17. **Damages** means any amounts an **Insured** becomes legally obligated to pay on account of any **Claim**, including:
- a. compensatory damages, settlements, and judgments;
  - b. awards of prejudgment and post-judgment interest;
  - c. sums for deposit in a consumer redress fund as equitable relief for the payment of consumer claims due to an adverse judgment or settlement;
  - d. punitive, exemplary, or multiplied damages and awards; provided, however, that punitive, exemplary, or multiplied damages and awards shall only be included as **Damages** to the extent insurable under the applicable laws of any jurisdiction which most favors coverage and which has a substantial relationship to an **Insured**, us, this **Policy**, or the **Claim** giving rise to such **Damages**;
  - e. with respect to a **PCI-DSS Claim** under Insuring Agreement I.A.4., any **PCI-DSS Penalties** and **PCI-DSS Response Expenses**; and
  - f. with respect to a **Regulatory Claim** under Insuring Agreement I.A.2., any **Regulatory Penalties**, **GDPR Penalties**, and **Regulatory Assessments and Expenses**.
- Damages** shall not include:
- g. fines, penalties, taxes, or sanctions imposed against an **Insured**; except to the extent such fines, penalties, taxes, or sanctions are insurable under the applicable laws of any jurisdiction which most favors coverage and which has a substantial relationship to an **Insured**, us, this **Policy**, or the **Claim** giving rise to such **Damages**, are **PCI-DSS Penalties** otherwise covered under Insuring Agreement I.A.4., or **Regulatory Penalties**, **GDPR Penalties**, or **Regulatory Assessments and Expenses** otherwise covered under Insuring Agreement I.A.2. of this **Policy**;
  - h. costs to comply with any injunctive, remedial, preventative, or other non-monetary or declaratory relief; or
  - i. any matters deemed uninsurable under the laws pursuant to which this **Policy** is construed.
18. **Data Recovery Loss** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to:
- a. replace and restore corrupted, destroyed, lost, or stolen software;
  - b. re-create and recover corrupted, destroyed, lost, or stolen data in electronic form which is, or was, stored on a **Computer System**;
  - c. re-create and recover corrupted, destroyed, lost, or stolen data in non-electronic form for which there is no electronic source available; and
  - d. to retain the services of a **Cyber Response Firm** to provide consultative and professional services related to **Data Recovery Loss** described in paragraphs V.18.a.–V.18.c. above.
19. **Employee** means any natural person whose work or service is or was guided and engaged by an **Insured Organization**, including full-time or part-time laborers, interns, volunteers, seasonal or temporary laborers, or laborers whose service or work is or was leased by or to an **Insured Organization**.

20. **External Computer Systems** means any computer hardware, software, firmware, wireless device, voice based telecommunication system, operating system, virtual machine, as well as any data stored thereon, and:
- a. associated input, output, processing, data storage, and mobile devices, networks, operating systems, application software, networking equipment, storage area networks, and other electronic data storage or backup facilities;
  - b. includes, but is not limited to, associated telephone systems (including “PBX”, “CBX,” “Merlin,” or “VoIP”), remote access systems (including “DISA”), peripheral communication equipment and systems, industrial control systems (including “SCADA”), Internet of things (commonly referred to as “IoT”), media libraries, extranets, and offline electronic data storage facilities; and
  - c. includes, but is not limited to, associated application hosting, cloud services, cloud computing platforms, data hosting, data storage, co-location, data back-up, data processing, and infrastructure as a service;
- which are operated for an **Insured’s** benefit by a third party under written contract between such third party and **Insured**.
21. **Extortion Loss** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to:
- a. make payment of any funds, digital currencies (“crypto-currencies”), marketable goods, services, or other assets to the person or group which is believed to be responsible for, and to have made, such **Extortion Threat**;
  - b. reduce or mitigate the severity of **Extortion Loss** described in paragraph V.21.a. above; and
  - c. retain the services of a **Cyber Response Firm** to provide consultative and professional services related to **Extortion Loss** described in paragraphs V.21.a. and V.21.b. above.
22. **Extortion Threat** means any credible threat or series of related threats made to an **Insured** by a third party person or group, or by a rogue **Employee** who is not a member of the **Control Group** and who is acting in a manner not authorized by the **Insured Organization**, which threatens to take any of the following actions unless an **Insured** pays such group or person the funds demanded, or meet some other non-monetary demand, in exchange for the mitigation or removal of such threat:
- a. cause an **Information Privacy Event** or **Network Security Event**;
  - b. alter, corrupt, damage, manipulate, misappropriate, encrypt, delete, or destroy any **Computer System**, **Corporate Data**, or **Protected Personal Information**;
  - c. restrict or inhibit access to a **Computer System**; or
  - d. any action connected to the continuation or furthering of any already commenced action referenced in paragraphs V.22.a.-V.22.c. above.
23. **Extra Expense** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to:
- a. reduce the **Period of Restoration**;
  - b. mitigate or reduce expenses resulting from the **System Disruption** of a **Computer System**;
  - c. secure **Computer Systems** such that a similar **System Disruption** is avoided in the future; and
  - d. retain the services of a **Cyber Response Firm** to provide consultative and professional services related to **Extra Expense** described in paragraphs V.23.a.–V.23.c. above.

24. **First Party Coverage** means Insuring Agreement(s) I.A.3., I.B.2., I.C.1., I.C.2., I.D.1., I.E.1., I.E.2., and I.F.2..
25. **Fraudulent Inducement Instructions** means the misrepresentation of one or more facts by a third-party person or entity via email or other means of electronic communication with the intent of misleading an **Insured** into transferring **Funds or Securities**.
26. **Fraudulent Inducement Loss** means an **Insured Organization's** loss of **Funds or Securities**.
27. **Funds or Securities** means any medium of exchange, including any written negotiable or non-negotiable instruments representative of such, which is authorized or adopted by a foreign or domestic government and in current use, including bank notes, travelers' checks, registered check, money orders, currency, bullion, and coins.  
  
**Funds or Securities** does not include any crypto-currencies or crypto-assets.
28. **GDPR Penalties** means **Regulatory Penalties** an **Insured** becomes legally obligated to pay as a result of a **Regulatory Claim** for such **Insured's** actual, alleged or reasonably suspected non-compliance with the General Data Protection Regulation Standard, as amended.
29. **Independent Contractor** means any natural person, agent, or single person entity who is not an **Employee** but performs work for an **Insured Organization** pursuant to a written contract or agreement.
30. **Information Privacy Event** means any actual or reasonably suspected:
  - a. failure to prevent unauthorized access to **Protected Personal Information**;
  - b. failure to properly manage, handle, store, protect, disclose, destroy, control, or collect **Protected Personal Information**;
  - c. violation of any **Privacy Regulations**, including, but not limited to, the wrongful collection or disclosure of **Protected Personal Information**;
  - d. failure to comply with those portions of a **Privacy Policy** which govern the collection, dissemination, confidentiality, integrity, accuracy, disclosure, sale, access, or availability of **Protected Personal Information**;
  - e. failure to provide natural persons whose **Protected Personal Information** an **Insured** stores or maintains to access, delete, or amend their **Protected Personal Information** as required by any **Privacy Regulation**, including, but not limited to, the "Right to be Forgotten" or "Right to Erasure" as described in the General Data Protection Regulation Standard, as amended;
  - f. failure to provide notification of any **Information Privacy Event** as required by any **Privacy Regulation**;
  - or
  - g. failure to disclose an actual or potential **Information Privacy Event** as required by any **Privacy Regulation**.
31. **Information Privacy Wrongful Act** means any actual or alleged error, misstatement, misleading statement, act, omission, neglect, breach of duty, or other offense committed or attempted by an **Insured**, based upon or resulting in an **Information Privacy Event**.
32. **Insured** means the **Insured Organization** and any **Insured Person**.

33. **Insured Computer Systems** means any computer hardware, software, firmware, wireless device, voice based telecommunication system, operating system, virtual machine, as well as any data stored thereon, and:
- a. associated input, output, processing, data storage, and mobile devices, networks, operating systems, application software, networking equipment, storage area networks, and other electronic data storage or backup facilities; and
  - b. includes, but is not limited to, associated telephone systems (including “PBX”, “CBX,” “Merlin,” or “VoIP”), remote access systems (including “DISA”), peripheral communication equipment and systems, industrial control systems (including “SCADA”), Internet of things (commonly referred to as “IOT”), media libraries, extranets, and offline electronic data storage facilities;

which are rented, leased, owned, or operated by an **Insured** or which are operated solely for an **Insured’s** benefit by a third party under written contract between such third party and **Insured**.

34. **Insured Organization** means the **Named Insured** and any **Subsidiaries**.

**Insured Organization** also means any entity as a debtor in possession or the bankruptcy estate of such **Insured Organization** under the United States bankruptcy law, or foreign equivalent.

35. **Insured Person** means any past, current or future natural person:

- a. **Employee**, director, officer, trustee, partner, general partner, managing partner, managing member, LLC member, or principal of an **Insured Organization**, but only with respect to a **Wrongful Act** or **Cyber Event** committed within the scope of such natural person’s duties performed on behalf of such **Insured Organization**; or
- b. **Independent Contractor**, but only with respect to a **Wrongful Act** or **Cyber Event** committed within the scope of such **Independent Contractor’s** duties performed on behalf of the **Insured Organization** and only if the **Insured Organization** indemnifies such **Independent Contractor**.

36. **Legal Services Loss** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to:

- a. determine the applicability of any notifications, communications, actions, or other services required or necessary for the **Insured Organization** to comply with applicable **Privacy Regulations**;
- b. draft and develop letters, documents, or other materials to properly notify the natural persons whose **Protected Personal Information** was, or may have been, wrongfully disclosed, accessed, acquired, or otherwise compromised or impacted as a result of the applicable **Information Privacy Event**;
- c. provide any legally required communications and reporting services to any regulatory, administrative, or supervisory authority; and
- d. retain the services of a **Cyber Response Firm** to provide legal, consultative, and professional services related to **Legal Services Loss** described in paragraphs V.36.a.–V.36.c. above.

**Legal Services Loss** includes costs and expenses incurred in order to comply with applicable **Privacy Regulations** and shall follow the law of the applicable jurisdiction which most favors coverage for such costs and expenses. Those costs and expenses not required to comply with any applicable **Privacy Regulations** require our prior consent.

37. **Loss** means:

- a. **Reward Expense Loss, Technical Response Loss, Public Relations Loss, Legal Services Loss, Notification Loss, Credit Monitoring Loss, Data Recovery Loss, System Restoration Loss, Business Interruption Loss, Contingent Business Interruption Loss, Extra Expense, Extortion Loss, Fraudulent Inducement Loss, and Computer Crimes Loss.**

**Loss** shall not include:

- b. salaries, benefits or other compensation payable to **Insured Persons**, except to the extent covered under Insuring Agreement(s) I.C.1. and I.C.2.;
- c. an **Insured Organization's** internal operating costs, expenses, or fees, except to the extent covered under Insuring Agreement(s) I.C.1. and I.C.2.;
- d. taxes, fines, penalties, or amounts for injunctive relief or sanctions;
- e. **Funds or Securities** in the care, custody, or control of an **Insured**, except to the extent covered under Insuring Agreement(s) I.D.1., I.E.1., and I.E.2.; or
- f. costs or expenses incurred to update, improve, enhance, or replace privacy or network security controls, policies or procedures, or **Computer Systems** to a level beyond that which existed prior to the applicable **Cyber Event**, except to the extent we have recommended and provided prior consent to incur such costs or expenses, including:
  - i. claim avoidance related costs or expenses anticipated under **Extra Expense**; and
  - ii. incremental improvement costs or expenses anticipated under **System Restoration Loss**.

38. **Malicious Code** means any software or computer program that is:

- a. purposefully designed to adversely affect, intentionally harm, or dishonestly monetize any computer hardware, software, firmware, wireless device, operating system, virtual machine, and the data stored thereon or any components thereof, including, but not limited to, industrial control systems (SCADA), IoT, VoIP telephone systems, media libraries, extranets, offline storage facilities (to the extent electronic data is held), mobile devices, input and output devices, data storage devices, networking equipment, and electronic data backup facilities or networks; or
- b. capable of affecting that which is referenced in paragraph V.38.a. above by inserting itself by a variety of forms, causing damage, possessing the ability to replicate itself, or possessing the capability of spreading copies of itself.

**Malicious Code** includes, but is not limited to, auto-reproduction programs, computer viruses, worms, Trojan horses, spyware, dishonest adware, crime-ware, mine-ware, script or any other software program, computer program, or virus that is functionally equivalent to **Malicious Code** described in paragraphs V.38.a. and V.38.b. above.

39. **Media Content** means data, text, images, graphics, music, sounds, photographs, advertisements, video, streaming content, webcasts, podcasts, blog posts, and online forum posts.

**Media Content** does not include computer software, software technology, or the actual goods, products, or services described, illustrated, or displayed in such **Media Content**.

40. **Media Wrongful Act** means any actual or alleged error, misstatement, misleading statement, act, omission, neglect, breach of duty, or other offense committed or attempted by an **Insured**, or by any third party entity or natural person for whom the **Insured** is legally responsible, in the public dissemination, posting, or display of **Media Content**, by or on behalf of an **Insured**, on a voice or video based communication medium, including radio, internet streaming, satellite, cable, television, or any similar communications broadcast, or on an **Insured's** website, printed material, social media site, or anywhere else on the internet, which results in the following:
- a. defamation, libel, slander, or other tort related to disparagement or harm to the character, reputation or feelings of any person or organization, including product disparagement, trade libel, infliction of emotional distress, malicious falsehood, outrage, or outrageous conduct;
  - b. infringement or dilution of title, slogan, logo, trademark, trade name, metatag, domain name, trade dress, service mark, or service name;
  - c. copyright infringement, passing off, plagiarism, piracy, or other misappropriation of intellectual property rights;
  - d. invasion, infringement, or interference with rights of privacy or publicity, including public disclosure of private facts, breach of confidence, intrusion, false light, and commercial appropriation of name or likeness;
  - e. false detention or arrest, harassment, trespass, wrongful entry or eviction, eavesdropping, or other invasion of the right of private occupancy;
  - f. improper deep framing or linking; or
  - g. unfair trade practices or competition, including misrepresentations in advertising, but solely when alleged in conjunction with the alleged conduct referenced in paragraphs V.40.a.–V.40.f. above.
41. **Named Insured** means the entity displayed in ITEM 1 of the Declarations.
42. **Network Security Event** means any actual or reasonably suspected:
- a. propagation of **Malicious Code** from a **Computer System**;
  - b. attack by **Malicious Code** which infects a **Computer System**;
  - c. denial of service attack:
    - i. originating from a **Computer System**; or
    - ii. made against a **Computer System**;
  - d. gaining of access or use of a **Computer System** by:
    - i. an unauthorized person; or
    - ii. an authorized person for purposes not authorized by an **Insured Organization**;
  - e. acquisition, access, loss, or disclosure of **Corporate Information** not authorized by an **Insured Organization**;
  - f. theft of a password or access code by electronic or non-electronic means from a **Computer System**, the **Insured Organization's** premises, or directly from an **Insured Person**;
  - g. the failure to provide any authorized user access to the **Insured Organization's** website or **Computer System** due to the failure or violation of the security of a **Computer Systems**; or

- h. the failure to protect **Computer Systems** which results in, or is based upon, a **Network Security Event** referenced in paragraphs V.42.a.-V.42.g. above.

**Network Security Event** includes any of the foregoing, regardless of whether such **Network Security Event** is a specifically targeted attack or a generally distributed attack.

- 43. **Network Security Wrongful Act** means any actual or alleged error, misstatement, misleading statement, act, omission, neglect, breach of duty, or other offense committed or attempted by an **Insured**, based upon or resulting in a **Network Security Event**.

- 44. **Notification Loss** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to:

- a. provide any legally required notification services to those natural persons whose **Protected Personal Information** was wrongfully disclosed, accessed, acquired, or otherwise compromised or impacted as a result of the applicable **Information Privacy Event**;
- b. complete mailing or other communications duties to notify those natural persons whose **Protected Personal Information** was wrongfully disclosed, accessed, acquired, or otherwise compromised or impacted as a result of the applicable **Information Privacy Event**;
- c. provide information on the availability of any related services or resources to those natural persons whose **Protected Personal Information** was wrongfully disclosed, accessed, acquired, or otherwise compromised or impacted as a result of the applicable **Information Privacy Event**; and
- d. retain the services of a **Cyber Response Firm** to provide consultative and professional services related to **Notification Loss** described in paragraphs V.44.a.-V.44.c. above.

**Notification Loss** includes costs and expenses incurred in order to comply with applicable **Privacy Regulations** and shall follow the law of the applicable jurisdiction which most favors coverage for such costs and expenses. Those voluntary costs and expenses not required to comply with any applicable **Privacy Regulations** require our prior consent.

- 45. **PCI Data Security Standards** means generally accepted and published rules, regulations, standards, or guidelines which relate to data security and the safeguarding, disclosure, and handling of **Protected Personal Information** and which are adopted or required by the Payment Card Industry Data Security Standards Council or any payment provider whose payment method is accepted for processing.

- 46. **PCI-DSS Claim** means any **Claim**, brought by or on behalf of a Payment Card Association or entity processing or providing payment card transactions, based upon an **Insured Organization's** actual, alleged, or potential non-compliance with **PCI Data Security Standards**, including but not limited to:

- a. failure to properly protect, handle, manage, store, destroy, or control payment account or payment card data, including applicable **Protected Personal Information**; or
- b. non-compliance with EMV specifications or mobile payment security requirements.

**PCI-DSS Claim** includes an investigation into a potential violation of **PCI Data Security Standards**, which may reasonably be expected to give rise to a **PCI-DSS Claim**.

47. **PCI-DSS Penalties** means monetary assessments, fines, penalties, chargebacks, reimbursements, and fraud recoveries, including card reissuance costs, the **Insured Organization** is legally obligated to pay due to a **PCI-DSS Claim** and its non-compliance under a payment card processing agreement or merchant services agreement pertaining to **PCI Data Security Standards**.
48. **PCI-DSS Response Expenses** means reasonable and necessary costs and expenses to retain the services of:
- a. a third party forensic firm that is a qualified Payment Card Industry Forensic Investigator, to determine the cause and scope of the **Information Privacy Event** which led to a **PCI-DSS Claim**; and
  - b. a Qualified Security Assessor (QSA) to validate an **Insured Organization's** adherence to **PCI Data Security Standards** following a **PCI-DSS Claim**.
49. **Period of Restoration** means the continuous period of time that:
- a. begins with the earliest date a **System Disruption** first occurred; and
  - b. ends on the date when **Insured Computer Systems** or **External Computer Systems** are, or could have been, repaired or restored with reasonable speed to the same functionality and level of service which existed prior to the **System Disruption**.
- A **Period of Restoration** shall not exceed one hundred eighty (180) days from the date the applicable **System Disruption** first occurred; provided, however, that the end of the **Policy Period** shall not cut short the **Period of Restoration**.
50. **Policy** means, collectively, the Declarations, **Application**, each included Insuring Agreement, and all forms and endorsements, stated in ITEM 8 of the Declarations, which are attached to and form part of this **Policy**.
51. **Policy Period** means the period of time from the Effective Date to the Expiration Date, as set forth in ITEM 2 of the Declarations, or the effective date of termination of this **Policy**, whichever is earlier.
52. **Pollution** means any liquid, gaseous, solid or thermal irritant or contaminant, including vapor, smoke, fumes, acids, chemicals and material to be recycled, reconditioned or reclaimed.
53. **Privacy Policy** means an **Insured Organization's** written or electronic policies which govern the collection, dissemination, confidentiality, integrity, accuracy, disclosure, sale, access, or availability of **Protected Personal Information**.
54. **Privacy Regulations** means any local, state, federal, or foreign identity theft or privacy protection laws, statutes, legislation, or regulations which require commercial entities which collect, process, or maintain **Protected Personal Information** to post privacy policies, adopt specific privacy or security controls, or notify individuals in the event that **Protected Personal Information** has potentially or actually been compromised, accessed, or acquired without their authorization.
- Privacy Regulations** explicitly include, but are not limited to, the Gramm-Leach Bliley Act of 1999, Health Insurance Portability and Accountability Act of 1996, California Database Breach Act, Minnesota Plastic Card Security Act, and General Data Protection Regulation Standard, and regulations issued pursuant to such Acts or Standards, as amended if applicable.
55. **Property Damage** means damage to, loss of use of, or destruction of any tangible property other than electronic or non-electronic data or **Protected Personal Information**.

56. **Protected Personal Information** means any of the following information or data, regardless of whether such data or information is in electronic, non-electronic, or any other format:
- a. any natural person's social security number, name, e-mail address, driver's license or state identification number, address, and telephone number;
  - b. any natural person's personally identifiable pictures or videos, internet browsing history, security access codes, or passwords, and account histories;
  - c. any natural person's medical or healthcare data, biometric records, or any other protected health information ("PHI");
  - d. any natural person's credit card or debit card number, account number, or any other protected financial information; or
  - e. any other non-public personal information or data of a natural person as specified in any **Privacy Regulations**.

**Protected Personal Information** does not include **Corporate Information**.

57. **Public Relations Loss** means reasonable and necessary public relations related costs and expenses incurred or paid by an **Insured Organization** to:
- a. protect or restore the **Insured Organization's** reputation;
  - b. mitigate financial harm to the **Insured Organization's** business; and
  - c. retain the services of a **Cyber Response Firm** to provide public relations or crisis communications consultative and professional services related to **Public Relations Loss** described in paragraphs V.57.a. and V.57.b. above.

58. **Regulatory Assessments and Expenses** means reasonable and necessary costs and expenses an **Insured** becomes legally obligated to pay on account and as a direct result of a **Regulatory Claim** to retain the services of a **Cyber Response Firm** to perform a legally required audit or assessment, including related consultative and professional services, of the **Insured Organization's** privacy practices or **Computer Systems**.

**Regulatory Assessments and Expenses** includes costs and expenses incurred in order to comply with applicable **Privacy Regulations** and shall follow the law of the applicable jurisdiction which most favors coverage for such costs and expenses. Those costs and expenses not required to comply with any applicable **Privacy Regulations** require our prior consent.

59. **Regulatory Claim** means any **Claim** brought by, or on behalf of, the Federal Trade Commission, the Federal Communications Commission, any supervisory authority enforcing the General Data Protection Regulation Standard, or any state attorney general, government licensing entity, regulatory authority, or any federal, state, local, or foreign governmental entity in such entity's official capacity.

**Regulatory Claim** includes an investigation into a potential violation of **Privacy Regulations**, which may reasonably be expected to give rise to a **Regulatory Claim**.

60. **Regulatory Penalties** means civil fines or penalties resulting from a **Regulatory Claim**, including **GDPR Penalties**, imposed against an **Insured** by the Federal Trade Commission, the Federal Communications Commission, any supervisory authority enforcing the General Data Protection Regulation Standard, or any state attorney general, government licensing entity, regulatory authority, or any federal, state, local, or foreign governmental entity in such entity's official capacity.

61. **Related Incident** means all **Wrongful Acts** and **Cyber Events** which share as a common nexus any act, fact, circumstance, situation, event, transaction, cause, or series of related acts, facts, circumstances, situations, events, transactions, or causes, and all:
- a. **Cyber Events** arising out of any **Related Incident** shall be considered one single **Cyber Event**, and such **Cyber Event** shall be considered first discovered on the date the earliest of such **Cyber Events** is first discovered, regardless of whether such date is before or during the **Policy Period**; and
  - b. **Claims** arising out of all **Related Incidents** shall be considered one single **Claim**, and such **Claim** shall be considered first made on the date the earliest of such **Claims** is first made, regardless of whether such date is before or during the **Policy Period**.
62. **Retention** means the amounts stated as **Retention** in ITEM 6 of the Declarations with respect to the Insuring Agreement to which each such stated **Retention** amount applies.
63. **Reward Expense Loss** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to an informant for information not otherwise available which leads to the arrest and conviction of a natural person or an entity responsible for the **Cyber Event** which resulted in a covered **Loss** under this **Policy**.
- Reward Expense Loss** requires our prior consent.
64. **Subsidiary** means:
- a. any corporation, partnership, limited liability company or other entity in which the **Named Insured** owns, directly or indirectly through one or more **Subsidiaries**, more than fifty percent (50%) of such entity's outstanding securities or voting rights representing the present right to elect, appoint or exercise a majority control over such entity's board of directors, board of trustees, board of managers, natural person general partners, or functional equivalent;
  - b. any entity operated as a joint venture in which the **Named Insured** owns, directly or indirectly through one or more **Subsidiaries**, exactly fifty percent (50%) of the issued and outstanding voting stock and whose management and operation an **Insured Organization** solely controls, pursuant to a written agreement with the owner(s) of the remaining issued and outstanding voting stock; or
  - c. any non-profit entity over which the **Named Insured**, directly or indirectly through one or more **Subsidiaries**, exercises management control.
65. **System Disruption** means the measurable interruption, suspension, degradation, or failure in the service of:
- a. with respect to Insuring Agreement I.C.1., **Insured Computer Systems**; or
  - b. with respect to Insuring Agreement I.C.2., **External Computer Systems**;
- directly caused by a **Network Security Event** or **Information Privacy Event**.

66. **System Restoration Loss** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to:
- a. restore **Computer Systems**, including replacing or reinstalling software programs contained therein, to their level of functionality immediately prior to the applicable **Network Security Event**;
  - b. remove any **Malicious Code** from **Computer Systems** resulting from the applicable **Network Security Event**;
  - c. restore the configuration of **Computer Systems** to an adequacy at or higher to that which was present immediately prior to the applicable **Network Security Event**; and
  - d. retain the services of a **Cyber Response Firm** to provide consultative and professional services related to **System Restoration Loss** described in paragraphs V.66.a.–V.66.c. above.
67. **Technical Response Loss** means reasonable and necessary costs and expenses incurred or paid by an **Insured Organization** to:
- a. investigate and determine the cause of the applicable **Information Privacy Event** or **Network Security Event**;
  - b. mitigate or contain an ongoing **Information Privacy Event** or **Network Security Event**;
  - c. identify and catalog natural persons whose **Protected Personal Information** was wrongfully disclosed, accessed, acquired, or otherwise compromised or impacted as a result of an applicable **Information Privacy Event**;
  - d. identify and catalog organizations whose **Corporate Information** was wrongfully disclosed, accessed, acquired, or otherwise compromised or impacted as a result of an applicable **Network Security Event**; and
  - e. retain the services of a **Cyber Response Firm** to provide consultative and professional services related to **Technical Response Loss** described in paragraphs V.67.a.–V.67.d. above.
68. **Third Party Coverage** means Insuring Agreement(s) I.A.1., I.A.2., I.A.4., I.B.1., and I.F.1.
69. **Wrongful Act** means any **Information Privacy Wrongful Act**, **Network Security Wrongful Act**, or **Media Wrongful Act**.

## VI. Exclusions

### A. EXCLUSIONS APPLICABLE TO ALL INSURING AGREEMENTS

This **Policy** shall not apply to any **Loss**, **Damages**, or **Claim Expenses** on account of any **Wrongful Act**, any **Cyber Event**, or any **Claim**:

1. Conduct

based upon, arising out of, or attributable to any **Insured's**:

- a. fraudulent, criminal, or malicious error, act or omission;
- b. intentional or deliberate violation of the law; or
- c. gaining of any profit, remuneration, or advantage to which such **Insured** was not legally entitled.

However, this exclusion shall not apply to:

- d. **Claim Expenses** or our duty to defend any such **Claim**; or
- e. **Damages** unless a final, non-appealable, adjudication establishes that such **Insured** committed such conduct, act, or violation.

Provided that:

- f. no such conduct pertaining to any **Insured Person** shall be imputed to any other **Insured Person**;
- g. any such conduct pertaining to past, present, or future members of the **Control Group** shall be imputed to the **Insured Organization**; provided, however, if such member of the **Control Group** acted deliberately outside his or her capacity as such then such conduct shall not be imputed to the **Insured Organization**; and
- h. for **First Party Coverage** only, this exclusion shall not apply to an intentionally dishonest or fraudulent act or omission, willful violation of any statute, rule of law, or gaining any profit, remuneration, or advantage by an **Employee**.

2. Contract

for breach of any express, implied, actual or constructive contract, warranty, or guarantee.

However, this exclusion shall not apply to:

- a. liability assumed by an **Insured**, but only to the extent that such assumed liability would have attached to the **Insured** in the absence of such contract, warranty, or guarantee;
- b. an **Insured's** contractual obligation to maintain the confidentiality or security of **Protected Personal Information**;
- c. an **Insured's** obligation under an implied or statutory standard of care obligation to prevent an **Information Privacy Event** or **Network Security Event**;
- d. with respect to Insuring Agreement I.A.1., an unintentional violation by an **Insured** to comply with an **Insured Organization's Privacy Policy**

- e. solely with respect to Insuring Agreement I.A.4., a **PCI-DSS Claim**;
- f. solely with respect to Insuring Agreement I.F.1., any actual or alleged misappropriation of idea under implied contract; or
- g. solely with respect to Insuring Agreement I.A.1., an **Insured's** unintentional breach of contract or agreement with a business associate, as defined in the U.S. Health Insurance Portability and Accountability Act (HIPAA), as amended, or the Health Information Technology for Economic and Clinical Health Act (HITECH), as amended.

3. Bodily Injury

for any actual or alleged **Bodily Injury**.

However, this exclusion shall not apply to:

- a. solely with respect to Insuring Agreement I.F.1., emotional distress, mental anguish, humiliation, or loss of reputation resulting from a **Media Wrongful Act**; or
- b. solely with respect to Insuring Agreement I.A.1., emotional distress, mental anguish, or mental injury resulting from an **Information Privacy Wrongful Act**.

4. Property Damage

alleging, based upon, arising out of, or attributable to **Property Damage**.

5. Prior Notice

alleging, based upon, arising out of, or attributable to any fact, circumstance, situation, event, **Cyber Event**, or **Wrongful Act** which was the subject of any notice of claim or potential claim given by or on behalf of any **Insured** under any policy of insurance of which this **Policy** is a direct or indirect renewal or replacement, or which it succeeds in time.

6. Prior Knowledge

alleging, based upon, arising out of, or attributable to any fact, circumstance, situation, event, **Cyber Event**, or **Wrongful Act** that is, or reasonably would be regarded as, the basis for a **Claim** or **Cyber Event** about which any member of the **Control Group** had knowledge prior to the Continuity Date set forth in ITEM 7 of the Declarations.

7. Pending or Prior Proceedings

alleging, based upon, arising out of, or attributable to any fact, circumstance, situation, event, **Cyber Event**, or **Wrongful Act** underlying or alleged in any prior or pending civil, criminal, administrative or regulatory proceeding or litigation against an **Insured** as of, or prior to, the Prior and Pending Litigation Date set forth in ITEM 7 of the Declarations.

8. Pollution

alleging, based upon, arising out of, or attributable to:

- a. the actual, alleged or threatened discharge, release, seepage, migration, or disposal of **Pollution**;
- b. any request that any **Insured** test for, monitor, clean up, remove, contain, treat, detoxify, or neutralize **Pollution**, including any voluntary decision to do so; or
- c. any request or requirement brought by or on behalf of any governmental authority relating to testing, monitoring, cleaning, removing, containing, treating, neutralizing, or in any way responding to or assessing the effects of **Pollution**.

9. War

alleging, based upon, arising out of, or attributable to war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, civil commotion assuming the proportions of or amounting to an uprising, or military or usurped power.

10. Nuclear, Biological, and Chemical Contamination

alleging, based upon, arising out of, or attributable to any planning, construction, maintenance, or use of any nuclear reactor, nuclear storage, disposal, waste or radiation site, or any other nuclear facility or site, the transportation of nuclear material, or any nuclear reaction or radiation, or radioactive, biological or chemical contamination, regardless of its cause.

11. Natural Disaster

alleging, based upon, arising out of, or attributable to fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, act of God, nature or any other related physical event.

12. Intellectual Property

alleging, based upon, arising out of, or attributable to any infringement, violation, or misappropriation of, or assertion of any right to, or interest in, any patent, copyright, trademark, trade dress or any other intellectual property right.

However, this exclusion shall not apply to:

- a. solely with respect to Insuring Agreement I.F.1., an otherwise covered **Claim** for a **Media Wrongful Act**, except to the extent such **Claim** alleges that **Media Content** consisted of computer software or software technology which infringed upon copyrighted software;
- b. solely with respect to Insuring Agreement I.A.1., any **Claim** arising out of any actual, alleged, or reasonably suspected failure by an **Insured** to properly disclose, handle, manage, store, destroy, protect, use or otherwise control **Protected Personal Information** resulting from an **Information Privacy Event**; or
- c. solely with respect to Insuring Agreement I.B.1., any **Claim** arising out of the actual or alleged disclosure of **Corporate Information** resulting from a **Network Security Event**.

13. Fees or Chargebacks

alleging, based upon, arising out of, or attributable to any fees, expenses, or costs paid to or charged by an **Insured**, including chargebacks, transfer fees, transaction fees, merchant service fees, or prospective service fees.

However, this exclusion shall not apply to:

- a. Solely with respect to Insuring Agreement I.A.4., any **PCI-DSS Claim**.

14. Unsolicited Communications

alleging, based upon, arising out of, or attributable to any violation of the Telephone Consumer Protection Act of 1991, as amended, or any similar federal, state, common, or foreign law relating to the unsolicited electronic dissemination of faxes, e-mails or other communications, or a natural person's or entity's right of seclusion.

However, this exclusion shall not apply to:

- a. solely with respect to Insuring Agreements I.A.1. and I.A.2., a **Claim** resulting from any **Insured's** actual, alleged or reasonably suspected violation of any **Privacy Regulation**; or
- b. solely with respect to Insuring Agreements I.A.1. and I.A.2., a **Claim** resulting from any **Insured's** actual or alleged failure to adequately protect **Computer Systems** resulting in the release of **Protected Personal Information**.

15. Consumer Protection Laws

alleging, based upon, arising out of, or attributable to any **Insured's** violation of the Truth in Lending Act, Fair Debt Collection Practices Act, Fair Credit Reporting Act, or the Fair and Accurate Credit Transactions Act or any amendments thereto or any rules or regulations promulgated thereunder, or any similar federal, state, common, or foreign law.

However, this exclusion shall not apply to:

- a. solely with respect to Insuring Agreement I.A.1., any **Claim** arising out of the actual or alleged disclosure or theft of **Protected Personal Information** resulting from an **Information Privacy Event**.

16. Infrastructure

alleging, based upon, arising out of, or attributable to any electrical or mechanical failures of infrastructure, including an interruption, electrical disturbance, surge, spike, brownout, blackout, or outages to electricity, gas, water, or Internet access service and Domain Name System (DNS) service provided by the service provider that hosts an **Insured Organization's** website, telecommunications, or other infrastructure.

However, this exclusion shall not apply to failures, interruptions, disturbances or outages of telephone, cable or telecommunications systems, networks or infrastructure:

- a. under an **Insured's** direct operational control; or
- b. solely with respect to Insuring Agreement(s) I.A.1. and I.B.1., which are the result of an actual or alleged **Information Privacy Wrongful Act** or **Network Security Wrongful Act**.

## B. EXCLUSIONS APPLICABLE TO PARTICULAR INSURING AGREEMENTS

This **Policy** shall not apply to any **Loss, Damages, or Claim Expenses** on account of any **Wrongful Act**, any **Cyber Event**, or any **Claim**:

### 1. Prior Acts

Exclusively with respect to **Third Party Coverage**, alleging, based upon, arising out of, or attributable to any **Wrongful Act**:

- a. taking place, in whole or in part, prior to the Retroactive Date as stated in ITEM 7 of the Declarations; or
- b. by a **Subsidiary** or any of its **Insured Persons**, occurring at any time during which such entity was not a **Subsidiary**.

### 2. Insured vs. Insured

Exclusively with respect to **Third Party Coverage**, brought by or on behalf of any:

- a. **Insured**:
- b. entity, if ten percent (10%) or more of its equity is owned, controlled, operated or managed, directly or indirectly, by any **Insured** at the time the **Wrongful Act** is committed or **Claim** is made; or
- c. successor or assignee of any **Insured**.

However, this exclusion shall not apply to any **Claim**:

- d. brought by or on behalf of an **Insured Person** for a **Wrongful Act**, but only to the extent such **Insured Person** did not commit or contribute to such **Wrongful Act** or to such extent such **Insured Person** is alleging an **Insured Organization** failed to comply or act in accordance with a **Privacy Regulation**;
- e. brought by or on behalf of an **Employee** alleging employee-related invasion of privacy or employee-related wrongful infliction of emotional distress, but only to the extent that such **Claim** arises out of the loss of **Protected Personal Information** resulting from an **Information Privacy Wrongful Act**; or
- f. brought by or on behalf of any **Insured** which is a third party entity as described in paragraph VII.A.2.a..

### 3. Securities

Exclusively with respect to **Third Party Coverage**, alleging, based upon, arising out of, or attributable to any **Insured's**:

- a. purchase, sale, or offer, or solicitation of an offer, to purchase or sell securities; or
- b. violation of the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940, the Investment Advisors Act, the Organized Crime Control Act of 1970, or any other federal, state or local securities law, and any amendments thereto or any rules or regulations circulated thereunder, or any similar federal, state or common law.

However, paragraph VI.B.3.b. of this exclusion shall not apply to:

- c. solely with respect to Insuring Agreement(s) I.A.1., I.A.2., and I.A.4., any **Claim** alleging a failure to disclose an actual, reasonably suspected or potential **Information Privacy Event** if such disclosure is required by any **Privacy Regulations**.

4. Governmental Seizure

Exclusively with respect to **First Party Coverage**, alleging, based upon, arising out of, or attributable to any confiscation, nationalization, seizure, or destruction of a **Computer System** or electronic data held or processed by an **Insured** or by order of any governmental or public authority.

5. Employment Practices or Discrimination

Exclusively with respect to **Third Party Coverage**, alleging, based upon, arising out of, or attributable to any employment practices or illegal discrimination of any kind, or any employment relationship, or the nature, terms or conditions of employment, including claims for workplace torts, wrongful termination, dismissal or discharge, or any discrimination, harassment, or breach of employment contract.

However, this exclusion shall not apply to:

- a. solely with respect to Insuring Agreement(s) I.A.1., I.A.2., and I.A.4., that portion of any **Claim** alleging **Employee** related invasion of privacy or wrongful infliction of emotional distress, provided that such **Claim** arises out of the actual or alleged disclosure or theft of **Protected Personal Information** resulting from an **Information Privacy Wrongful Act**.

6. Antitrust

Exclusively with respect to **Third Party Coverage**, alleging, based upon, arising out of, or attributable to any unfair competition or restraint of trade, including violations of any local, state, federal, or foreign laws governing the foregoing, whether brought by or on behalf any individuals, entities, the Federal Trade Commission, or any other federal, state, local, or foreign government agency.

However, this exclusion shall not apply to:

- a. solely with respect to Insuring Agreement I.A.2., a **Regulatory Claim** resulting directly from a violation of **Privacy Regulations**;
- b. solely with respect to Insuring Agreement I.F.1., a **Claim** for a **Media Wrongful Act** as defined in paragraph V.40.g..

7. Advertising & Representations

Exclusively with respect to Insuring Agreement(s) I.F.1. and I.F.2, alleging, based upon, arising out of, or attributable to any inaccurate, inadequate, or incomplete description of the price of goods, products or services, cost guarantees, cost representations, or contract price estimates, the authenticity of any goods, products or services, or the failure of any goods or services to conform with any represented quality of performance.

8. Licensing

Exclusively with respect to Insuring Agreement(s) I.F.1. and I.F.2., alleging, based upon, arising out of, or attributable to any action brought by or on behalf of the Federal Trade Commission, the Federal Communications Commission, or any other federal, state, or local government agency or ASCAP, SESAC, BMI or other licensing or rights entities in such entity's regulatory, quasi-regulatory, or official capacity, function or duty.

9. Contest or Game of Chance

Exclusively with respect to Insuring Agreement(s) I.F.1. and I.F.2., alleging, based upon, arising out of, or attributable to any gambling, contest, game of chance, lottery, or promotional game, including the redemption of coupons or tickets related thereto.

C. EXCLUSIONS APPLICABLE TO FINANCIAL FRAUD INSURING AGREEMENTS

Exclusively with respect to Insuring Agreement(s) I.E.1. and I.E.2., this **Policy** shall not apply to any **Computer Crimes Loss, Fraudulent Inducement Loss, or Reward Expense Loss** on account of any **Computer Crimes** or any **Fraudulent Inducement Instructions**:

1. Financial Fraud of Intellectual Property

for the loss of confidential information, including trade secrets, formulas, patents, customer information, negatives, drawings, manuscripts, prints, and other records of a similar nature, or other confidential information, intellectual property of any kind, data or computer programs.

2. Interest Income

for or applicable to any potential income, including interest and dividends, not realized by the **Insured Organization** or a customer of the **Insured Organization**.

3. Forged or Altered Instruments

resulting directly from forged, altered, or fraudulent negotiable instruments, securities, documents or written instructions or instructions used as source documentation to enter electronic data or send instructions.

## VII. Conditions

### A. INSURED EXTENSIONS

**Third Party Coverage** shall extend to apply as follows:

1. Spousal, Domestic Partner, Estates, and Legal Representatives
  - a. In the event of an **Insured Person's** death, incapacity, or bankruptcy, any **Claim** made against such **Insured Person's** estate, heirs, executors, administrators, assigns, and legal representatives shall be considered to be a **Claim** made against such **Insured Person**, but only to the extent such **Insured Person** would otherwise be covered under this **Policy**; and
  - b. In the event of a **Claim** made against an **Insured Person's** lawful spouse or domestic partner, such **Claim** shall be considered to be a **Claim** made against such **Insured Person**, but only for a **Wrongful Act** actually or allegedly committed by such **Insured Person** other than such spouse or domestic partner.
2. Additional Insureds
  - a. If an **Insured Organization** is required by contract, or has explicitly agreed in writing, to add any third party entity as an **Insured** under this **Policy**, then such third party entity shall be considered an **Insured** under this **Policy** but only for **Wrongful Acts** actually or allegedly committed or attempted by an **Insured Organization** other than such third party entity.

### B. SUBSIDIARIES

1. Coverage for Subsidiaries

With respect to any **Insured Organization** which is a **Subsidiary**, coverage afforded under this **Policy** for such **Subsidiary**, and its **Insured Persons**, shall only apply to:

- a. **Loss** resulting from **Cyber Events** which occurred after the effective date that such entity became a **Subsidiary** and prior to the date that such entity ceased to be a **Subsidiary**; and
- b. **Claims** for **Wrongful Acts** which actually or allegedly occurred after the effective date that such entity became a **Subsidiary** and prior to the date that such entity ceased to be a **Subsidiary**.

Any entity which ceases to be a **Subsidiary** during the **Policy Period** shall be afforded coverage through the expiration date of the current **Policy Period** but only with respect to **Wrongful Acts** and **Cyber Events** which occurred before the date it ceased to be a **Subsidiary**.

2. **Subsidiary Acquisition or Creation**

If, during the **Policy Period**, an **Insured Organization** acquires or creates another entity whose gross revenues exceed twenty five percent (25%) of the consolidated gross revenues of the **Insured Organization**, as of the most recent fiscal year prior to the effective date of this **Policy**, and such that the acquired or created entity becomes a **Subsidiary**, then such **Subsidiary** shall only be considered an **Insured Organization** for a period of ninety (90) days following its acquisition or formation unless:

- a. the **Named Insured** provides us written notice within sixty (60) days of the full particulars of such entity and agrees to any additional premium and amendments to this **Policy** relating to such entity; and
- b. we have ratified our acceptance of such entity as a **Subsidiary** by endorsement to this **Policy**.

## C. CHANGE OF CONTROL & AUTOMATIC RUN-OFF

If a **Change of Control** occurs during the **Policy Period**, then:

1. **Third Party Coverage** under this **Policy** shall:
  - a. continue in full force and effect until the expiration date of the current **Policy Period** with respect to **Claims** for **Wrongful Acts** committed before such **Change of Control**; and
  - b. cease with respect to **Claims** for **Wrongful Acts** committed after such **Change of Control**;
2. **First Party Coverage** under this **Policy** shall:
  - a. continue in full force and effect until the expiration date of the current **Policy Period** with respect to **Loss** for **Cyber Events** which occurred before such **Change of Control**; and
  - b. cease with respect to **Loss** for **Cyber Events** which occurred after such **Change of Control**;
3. The **Named Insured** shall have the right to give us notice that it desires to purchase an Extended Reporting Period, in accordance to the conditions set forth in section VII.D.2., Extended Reporting Period, of this **Policy**; and
4. This **Policy** may not be canceled by the **Named Insured**, and the entire premium shall be deemed fully earned.

## D. EXTENDED REPORTING PERIOD

1. **Automatic Discovery Reporting Period**

If this **Policy** does not renew or otherwise terminates for a reason other than failure to pay premium, then following the effective date of such event the **Named Insured** shall have the right, for a period of sixty (60) days following such event, to give us written notice of **Claims** made against any **Insured** during such sixty (60) day period for any **Wrongful Acts** committed prior to the effective date of such **Policy** termination or end of the **Policy Period**, whichever is applicable.

## 2. Extended Reporting Period

An “Extended Reporting Period,” if purchased, means the period of time in which the **Named Insured** may give us written notice of **Claims** first made against any **Insured** under this **Policy**, and shall be extended to apply to **Claims** first made during such Extended Reporting Period but only with respect to;

- a. **Claims** for **Wrongful Acts** which occurred prior to the effective date of **Policy** termination, the end of the **Policy Period**, or effective date of **Change of Control** (whichever is applicable); and
- b. **Claims** for **Wrongful Acts** made against persons or entities which were **Insureds** as of the effective date of **Policy** termination, the end of the **Policy Period**, or effective date of **Change of Control** (whichever is applicable).

If this **Policy** does not renew or otherwise terminates for a reason other than for failure to pay premium, or upon the occurrence of a **Change of Control**, then upon the effective date of such event:

- c. the **Named Insured** shall have the right to give us notice that it desires to purchase an Extended Reporting Period for **Third Party Coverage** at any of the following additional periods and associated premium amounts, which are represented as a percentage of the annualized premium of the **Policy** to which the Extended Reporting Period applies:
  - i. one (1) year for seventy five percent (75%); or
  - ii. two (2) years for one hundred twenty five percent (125%);
- d. the **Named Insured**, or a party acting on its behalf, may send us a request for the purchase of an Extended Reporting Period outside the additional periods and amounts indicated in VII.D.2.c. above, and we may, at our discretion, subsequently provide a quote for such request;
- e. any **Claim** made during a purchased Extended Reporting Period shall be deemed to have been made during the **Policy Period** immediately preceding the Extended Reporting Period;
- f. the **Aggregate Limit of Insurance** and Sub-Limits of Insurance available for any purchased Extended Reporting Period shall not be increased or renewed, unless we expressly provide such amendment via an endorsement to this **Policy**;
- g. the **Named Insured's** right to purchase an Extended Reporting Period shall lapse unless we receive written notice from the **Named Insured**, or a party acting on its behalf, of the election to purchase such Extended Reporting Period within sixty (60) days after this **Policy's** termination or expiration date or, if applicable, the effective date of any **Change of Control**; and
- h. the entire premium charged for any purchased Extended Reporting Period is due at the time of purchase and shall be considered fully earned as of the effective date of such Extended Reporting Period.

## E. NOTICE

### 1. Notice of Claims and Cyber Events

An **Insured** shall, as a condition precedent to our obligations under this **Policy**, give us written notice as soon as practicable after any member of the **Control Group**:

- a. first becomes aware of any **Claim** made against an **Insured**; or
- b. discovers any **Cyber Event**;

Provided further, and notwithstanding VII.E.1.a. and VII.E.1.b. above:

- c. all such notice of **Claims** made or **Cyber Events** discovered must be noticed to us no later than ninety (90) days after the end of the **Policy Period** or termination of this **Policy**, whichever is earlier; and
- d. if an Extended Reporting Period is purchased pursuant to section VII.D.2., all **Claims** made during such Extended Reporting Period must be reported to us no later than the end of the Extended Reporting Period;

All such notices described in this clause VII.E.1. must include the following details related to the applicable **Cyber Event** or **Claim**:

- e. all pertinent facts, particulars, and dates, including the nature of such **Cyber Event** and its potential consequences and **Damages**;
- f. the identities of those persons allegedly involved or affected; and
- g. with respect to notices related to **First Party Coverage**, the business operations, **Computer Systems**, or other assets affected.

### 2. Notice of Circumstances

If, during the **Policy Period**, any member of the **Control Group** first becomes aware of any circumstances which may reasonably give rise to a **Claim** under this **Policy**, then any **Claim** which arises out of such circumstances shall be deemed to have been first made at the time such written notice was received by us, but only to the extent that such written notice includes the following details and is received by us during the **Policy Period**:

- a. details on why the **Insured** believes a **Claim** may be forthcoming;
- b. all pertinent facts, particulars, and dates, including the nature of such circumstances, why the **Insured** believes a **Claim** may reasonably be forthcoming, and its potential consequences and **Damages**; and
- c. the identities of those persons allegedly involved or affected.

### 3. Notice Delivery

All notices described within this condition VII.E., Notice, shall be given to us in writing, either electronically or non-electronically, at the address set forth in ITEM 5 of the Declarations. All such notices shall be effective on the date we receive such notice. If such notice is mailed or transmitted by electronic mail, the date of such mailing or transmission shall constitute the date that such notice was given to us, and proof of mailing or transmission shall be sufficient proof of notice.

## F. OBLIGATIONS

In connection with all **Claims** and **Cyber Events** under this **Policy**, the **Insured** agrees to the following:

1. The **Insured** shall cooperate with and assist us in the effort to defend and settle any **Claim**, including:
  - a. attending hearings and trials, assisting in securing and giving evidence, obtaining the attendance of witnesses, and enforcing the **Insured's** rights of contribution or indemnity against any person or entity which may be liable to such **Insured** because of an act or omission covered under any **Third Party Coverage**; and
  - b. delivering to us copies of all demands, legal papers, other related legal documents and invoices the **Insured** receive, as soon as practicable.
2. The **Insured** shall not settle any **Claim**, incur any **Claim Expenses**, or otherwise assume any contractual obligation or admit any liability with respect to any **Claim** without our written consent, which shall not be unreasonably withheld. We shall not be liable for any settlement, **Claim Expenses**, assumed obligation, or admission to which we have not provided such consent.

## G. POLICY TERMINATION

1. We may only cancel this **Policy** prior to the expiration date of the **Policy Period** if the **Named Insured** fails to pay premium prior to its due date. If such cancellation is being considered, we shall deliver a written notice of pending cancellation. Such notice shall be delivered at least twenty (20) days prior to the date that such cancellation is proposed to become effective. If the full premium due is remitted to us prior to the proposed cancellation effective date, then such cancellation shall not go into effect.
2. The **Named Insured** may cancel this **Policy** at any time and for any reason by delivering such instructions to us by mail or electronic mail. Such instructions may be delivered directly by the **Named Insured** or through any person or entity contracted to act on the **Named Insured's** behalf for the placement of this **Policy**.
3. If this **Policy** is canceled for any reason prior to the end of the **Policy Period**, we shall refund the unearned premium computed pro rata. Such premium adjustment shall be made as soon as practicable upon termination of the **Policy**, but payment or tender of any unearned premium by us shall not be a condition precedent to the effectiveness of such termination.
4. We are not required to renew or offer to renew this **Policy** upon the expiry of its **Policy Period**.

## H. LOSS CALCULATIONS FOR BUSINESS INTERRUPTION AND PUBLIC RELATIONS

1. In determining and calculating the amount of **Public Relations Loss** covered under this **Policy**, we shall give due consideration to the prior experience of the **Insured Organization's** public and market perception before the beginning of the applicable **Cyber Event** or **Media Wrongful Act**, and we shall make this assessment at our sole discretion, in good faith, and as we deem reasonable and necessary.
2. In determining and calculating the amount of **Contingent Business Interruption Loss**, **Business Interruption Loss**, and **Extra Expense** covered under this **Policy**, we shall give due consideration to the prior experience of the **Insured Organization's** business before the beginning of the applicable **System Disruption** and to the probable business such **Insured Organization** could have performed had no **System Disruption** occurred.

## I. REPRESENTATIONS & SEVERABILITY

We have relied upon the representations and statements in the **Application** in granting this **Policy** to the **Insured**, with such representations and statements forming the basis of coverage under this **Policy**. With respect to such representations and statements contained in the **Application**:

1. no knowledge possessed by an **Insured Person** shall be imputed to any other **Insured Person**, and the **Application** shall be considered to be separate for each **Insured Person**;
2. in the event the **Application** contains misrepresentations made with the actual intent to deceive or contains misrepresentations which materially affect either the acceptance of the risk or the hazard assumed by us under this **Policy**, then no coverage shall be afforded under this **Policy** based upon, arising from, or in any way attributable to any such misrepresentations with respect to:
  - a. any **Insured Person** who knew of such misrepresentations, regardless of if such **Insured Person** knew such **Application** contained such misrepresentations; and
  - b. an **Insured Organization** if any past or present member of the **Control Group** knew of such misrepresentations, regardless of if such member of the **Control Group** knew such **Application** contained such misrepresentations.
3. we shall not be entitled under any circumstances to void or rescind this **Policy** with respect to any **Insured**.

## J. OTHER INSURANCE

1. If any **Loss, Damages, or Claim Expenses** or other amounts covered under this **Policy** are covered under any other valid and collectible insurance, then this **Policy** shall apply only to the extent that the amount of such **Loss, Damages, or Claim Expenses** are in excess of the amount of such other insurance whether such other insurance is specified as primary, contributory, excess, contingent or otherwise.

However, paragraph VII.J.1. above shall not apply if such other insurance is written explicitly to serve as excess insurance over the **Aggregate Limit of Insurance** or Sub-Limits of Insurance provided by this **Policy**.

2. The conditions set forth in VII.D.1., Automatic Discovery Reporting Period, and VII.E.2., Notice of Circumstances, shall not apply to **Claims** that are covered under any subsequent insurance purchased by an **Insured** or for an **Insured's** benefit, or that would be covered by any subsequent insurance but for the exhaustion of the amount of insurance limits applicable and available under such subsequently placed insurance.

## K. SUBROGATION

1. In the event of any payment by us of **Loss, Damages, or Claim Expenses** or other amounts under this **Policy**, we are subrogated to the **Insured's** rights of recovery against any person or organization, and the **Insureds** shall execute and deliver instruments, papers, and whatever else is necessary to secure such rights and enable us to effectively bring suit or otherwise pursue subrogation rights in the name of the **Insureds** under this **Policy**.
2. However, we shall not subrogate as described in paragraph VII.K.1. above:
  - a. against any **Insured Person**, unless such **Insured Person** was in violation of paragraph VI. A.1.; or
  - b. if an **Insured** agreed in writing to waive such **Insured's** right of recovery or subrogation against any person or entity prior to the **Cyber Event** or **Wrongful Act** which gave rise to the **Claim** or **Loss** connected with such subrogation.

## L. RECOVERIES

All recoveries from third parties for payments of **Loss, Damages, or Claim Expenses** shall be applied in the following order of priority after first deducting the costs and expenses incurred in obtaining such recovery:

1. to us, to reimburse us for any **Retention** we paid on an **Insured's** behalf and for any **Damages, Loss, or Claims Expenses** we paid under this **Policy**; and
2. to the **Insured**, to reimburse the **Insured** for any **Retention** such **Insured** paid and for any other amounts not covered under this **Policy**.

Provided, that such recoveries shall not include any recovery from insurance, reinsurance, security, or indemnity taken for our benefit, or any portion of a **Retention** we waived.

#### M. AUTHORIZATION

The **Named Insured** has the authority to act on behalf of all **Insureds** and is responsible for the payment of premiums and receiving of notices of cancellation, nonrenewal, or any change to coverage provided under this **Policy**. All **Insureds** agree to this authority and have delegated, individually and collectively, all such authority exclusively to the **Named Insured**.

Provided, however, that nothing within this condition, VII.M. Authorization, shall relieve any **Insured** from giving any notice to us that is required under this **Policy**.

#### N. ASSIGNMENT

This **Policy**, including any rights or duties herein, may not be transferred or assigned to another party unless we have provided our prior written consent to such transfer or assignment.

#### O. ACTION AGAINST US

No action shall lie against us unless, as a condition precedent thereto, the **Insured** has been in full compliance with all terms of this **Policy**. No person or entity shall have any rights under this **Policy** to join us as a party to any action against any **Insured** to determine such **Insured's** liability, nor shall we be impleaded by such **Insured** or the legal representatives of such **Insured**.

#### P. DISPUTES & RESOLUTIONS

This condition, VII.P. Disputes & Resolutions, provides the terms and conditions applicable to disputes which may arise between us and any **Insured** or amongst various **Insureds**. If any limitation in this section is deemed to be inconsistent with applicable law, such limitation is amended so as to equal the minimum period of limitation provided by such law.

1. If any dispute persists between us and any **Insured** as it relates to this **Policy**, or any term or condition herein, we and such **Insureds** agree to make a determined effort to solve such dispute via alternative dispute mediation or through a third-party mediator. The costs to procure such mediation shall be paid by us, if applicable, but our payments of such costs shall not persist past a single alternative dispute mediation effort.
2. In the event of a disagreement between or amongst any **Insureds**, the **Named Insured** shall have exclusive authority to act on behalf of all other **Insureds** with respect to negotiation of settlements and the decision to appeal or not to appeal any judgment.

#### Q. BANKRUPTCY

Bankruptcy or insolvency of any **Insured**, including any **Insured Person's** estate, does not relieve us of any of our obligations, rights or defenses under this **Policy**.

#### R. STATE AMENDATORY INCONSISTENCY

If there is an inconsistency between any term or condition of this **Policy**, those terms and conditions which are more favorable to the **Insured's** coverage shall apply to the extent permitted by law.

Provided, however, that with respect to any time period relating to notice of cancellation provided under this **Policy**, we shall apply the applicable state law.

#### S. TERRITORY

Coverage provided under this **Policy** shall extend to **Cyber Events** and **Wrongful Acts** occurring or discovered, **Claims** made, and **Losses** incurred anywhere in the world.

#### T. HEADINGS

The titles, headings, and subheadings of certain paragraphs, sections, conditions, or provisions of this **Policy**, and any endorsements attached thereto, are intended solely for convenience and reference and form no part of the terms and conditions of coverage under this **Policy**.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

## Service of Process Endorsement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

This **Policy** is subject to the following:

- 1) The following provision applies to Alaska, Arizona, Florida, Idaho, Missouri, Nevada, New Mexico, North Carolina, South Dakota, Tennessee, Texas, Washington, and Wyoming only:

We designate the Superintendent of Insurance, Insurance Commissioner, Director of Insurance, or other officer specified by law, pursuant to the laws of the State where this **Policy** is delivered, as our true and lawful attorney upon whom may be served any lawful process in any action, suit or proceeding instituted in the State in which this **Policy** is delivered, by, or on behalf of, the **Named Insured** or any beneficiary hereunder arising out of this **Policy**. We designate the Corporate Secretary of At-Bay Specialty Insurance Company, 1209 Orange Street Wilmington, DE 19001 as the person whom the said officer is authorized to mail such process or true copy thereof.

- 2) The following provision applies to Alabama, Colorado, Georgia, Hawaii and Mississippi only:

We designate the Superintendent of Insurance, Insurance Commissioner, Director of Insurance, or other officer specified by law, pursuant to the laws of the State where this **Policy** is delivered, and the Resident Agent denoted below, as our true and lawful attorney upon whom may be served any lawful process in any action, suit or proceeding instituted in the State in which this **Policy** is delivered, by, or on behalf of, the Named Insured or any beneficiary hereunder arising out of this **Policy**. We designate the Corporate Secretary of At-Bay Specialty Insurance Company, 1209 Orange Street Wilmington, DE 19001 as the person whom the said officer and/or Registered Agent is authorized to mail such process or true copy thereof.

Alabama	Commissioner of Insurance and Resident Agent  C T Corporation System 2 North Jackson Street, Suite 605, Montgomery, Alabama 36104	Hawaii	Insurance Commissioner and Resident Agent  C T Corporation System 900 Fort Street, Suite 1680, Honolulu, Hawaii 96813
Colorado	Commissioner of Insurance or	Mississippi	Commissioner of Insurance and

	Resident Agent  C T Corporation System 7700 E Arapahoe Rd, STE 220, Centennial, CO 80112-1268		Resident Agent  C T Corporation System 645 Lakeland East Drive, Suite 101, Flowood, MS 39232
Georgia	Commissioner of Insurance and Safety Fire and Resident Agent  C T Corporation System 289 S Culver St Lawrenceville, GA 30046		

- 3) The following provision applies to Arkansas, Kentucky, Oregon, and West Virginia only:

We designate the following individual as our true and lawful attorney upon whom may be served any lawful process in any action, suit or proceeding instituted in the State in which this **Policy** is delivered, by, or on behalf of, the **Named Insured** or any beneficiary hereunder arising out of this **Policy**. We designate the Corporate Secretary of At-Bay Specialty Insurance Company, 1209 Orange Street Wilmington, DE 19001 as the person whom the said individual is authorized to mail such process or true copy thereof.

Arkansas	Resident Agent  C T Corporation System 124 West Capitol Avenue, Suite 1900, Little Rock, AR 72201	Oregon	Resident Agent  C T Corporation System 780 Commercial Street SE, STE 100, Salem, OR 97301
Kentucky	Secretary of State  700 Capital Avenue Suite 152 Frankfort, KY 40601	West Virginia	Secretary of State  1900 Kanawha Boulevard East State Capitol Complex Bldg. 1, Ste. 157-K Charleston, WV 25305

- 4) The following provision applies to California only:

A surplus lines insurer shall be sued, upon any cause of action arising in the State under any contract issued by it as a surplus lines contract pursuant to the laws the state of California. A surplus lines insurer issuing such **Policy** is deemed to have authorized service of process against it in the manner and to the effect as provided in the laws of the state of California. Service of legal process against the insurer may be made in any such action by service upon the designated agent. The designated agent for service of process is: Registered Agent, C T Corporation System, 30 N Brand Blvd, STE 700, Glendale, CA 91203.

- 5) The following provision applies to Illinois only:

We designate the Director of the Illinois Department of Insurance and his successor or successors in office, at 320 West Washington Street, Bicentennial Building, Springfield, IL 62727, as our true and lawful attorney upon whom may be served any lawful process in any action, suit or proceeding instituted by, or on behalf of, the **Insured** or any beneficiary hereunder arising out of this contract of insurance. We designate the Corporate Secretary of At-Bay Specialty Insurance Company, 1209 Orange Street Wilmington, DE 19001 as the person to whom the said officer is authorized to mail such process or true copy thereof.

- 6) The following provision applies to Iowa only:

An eligible surplus lines insurer may be sued upon a cause of action arising in Iowa under a surplus lines insurance **Policy** or contract placed by the insurer or upon evidence of insurance placed by the insurer and issued or delivered in Iowa by a surplus lines insurance producer. We designate the Commissioner of Insurance, 1963 Bell Avenue, Suite 100, Des Moines, IA 50315 as the person upon whom service of process can be made.

- 7) The following provision applies to Maine only:

An unauthorized insurer shall be sued, upon any cause of action arising in the State under any contract issued by it as a surplus lines contract pursuant to the laws of the state of Maine. An unauthorized insurer issuing such **Policy** is deemed to have authorized service of process against it in the manner and to the effect as provided in the laws of the state of Maine. Service of legal process against the insurer may be made in any such action by service of two copies upon the designated agent. The designated agent for service of process is: Registered Agent, C T Corporation System, 128 State Street #3, Augusta, Maine 04330.

- 8) The following provision applies to New York only:

The Superintendent of the New York State Department of Financial Services and his/her successors is appointed by the excess lines insurer issuing this **Policy** to be its true and lawful attorney upon whom may be served all lawful process in any proceeding instituted by or on behalf of an Insured or beneficiary arising out of this insurance **Policy** and the excess lines insurer signifies its agreement that service of process in such manner is of the same legal force and validity as personal service of process in New York State upon the insurer.

- 9) The following provision applies to Pennsylvania only:

It is agreed that in the event we fail to pay any amount claimed to be due under this **Policy** we will submit, at the **Insured's** request, to the jurisdiction of any court of competent jurisdiction within the United States of America and will comply with all requirements necessary to give such court jurisdiction. All matters arising hereunder shall be determined in accordance with the law and practice of such court. It is further agreed that in any such action instituted against any **Insured** under this contract, we will abide by the final decision of such court or of any appellate court in the event of an appeal.

Service of process shall be made pursuant to the procedures provided by 42 Pa. C.S. Chapter 53 Subchapter B (relating to interstate and international procedure). When making service of process by mail, such process shall be mailed to the Corporate Secretary of At-Bay Specialty Insurance Company, 1209 Orange Street Wilmington, DE 19001. The above named is authorized and directed to accept service of process on our behalf for any action or upon any request of the **Insured** to give a written undertaking to the **Insured** that they will enter a general appearance for us in the event such an action shall be instituted.



Further, pursuant to any statute of any state, territory or district of the United States of America, which makes provisions therefore, we hereby designate the Secretary of State, 401 North Street, Harrisburg, PA 17120, as the true and lawful attorney upon whom any lawful process may be served in any action, suit or proceeding instituted by, or on behalf of, the Insured or any beneficiary hereunder arising out of this contract of insurance, and hereby designate the above named as the person on whom such process or a true copy thereof shall be served.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

## Reputational Harm Insuring Agreement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to ITEM 6 of the Declarations:

Insuring Agreement:	Inclusion:	Sub-Limit of Insurance:	Retention:
G. Reputational Harm			
G.1. Reputational Harm	Included	\$1,000,000.	\$2,500.

- 2) The following is added to the Declarations:

**Reputational Harm Indemnity Period:** 180 days.

- 3) The following is added to section I. Insuring Agreements:

### G. REPUTATIONAL HARM

#### 1. Reputational Harm

We shall pay the **Insured Organization** for **Reputational Harm Loss** and **Public Relations Loss** incurred by the **Insured Organization** as a direct result of a **Reputational Harm Event** which first occurs during the **Policy Period**.

- 4) The following are added to section V. Definitions:

- a) **Adverse Publication** means a publication, report, communication, opinion, or media of any other form which:
- i) disseminates any previously non-public information:
  - ii) specifically states or references an **Insured Organization** or **Covered Brand**; and
  - iii) is disseminated or publicized to the general public via any electronic or non-electronic medium or media channel including, but not limited to, television, print media, radio or electronic networks, the internet, or electronic mail.

- b) **Covered Brand** means any brand owned exclusively by, or licensed exclusively to, an **Insured Organization**.
- c) **Reputational Harm Event** means the first appearance of a publicly available **Adverse Publication** which:
  - i) directly states or alleges that an **Insured Organization** has experienced an **Information Privacy Event** or **Network Security Event**, regardless of the factual accuracy of any statement(s) contained therein;
  - ii) is reasonably expected to cause, or has already caused, material damage, harm, or tarnish to the public perception and reputation of an **Insured Organization**, including, but not limited to, damage to such **Insured Organization's** goodwill amongst its customers, suppliers, or community with whom such **Insured Organization** habitually deals with in the course of its business; and
  - iii) is reasonably expected to lead, or has already led, to an **Insured Organization's** provable loss of income.
- d) **Reputational Harm Indemnity Period** means the continuous period of time that:
  - i) begins with the date the **Reputational Harm Event** first occurred; and
  - ii) ends on the date when the number of days stated in the Declarations as the **Reputational Harm Indemnity Period** have elapsed.

The **Reputational Harm Indemnity Period** shall not be cut short or reduced by the intervening expiration of the **Policy Period**, if applicable.

- e) **Reputational Harm Loss** means the following amounts incurred by an **Insured Organization** during the **Reputational Harm Indemnity Period**:
  - i) net profit before income taxes that would have been earned had no **Reputational Harm Event** occurred;
  - ii) net loss before income taxes that would have been avoided had no **Reputational Harm Event** occurred; and
  - iii) costs to retain the services of a third party forensic accounting firm to determine the amounts of **Reputational Harm Loss** described in paragraphs 4)e)i) and 4)e)ii) above, subject to our prior consent.

The amount of **Reputational Harm Loss** will be determined and calculated in accordance with section VII. Conditions, Loss Calculation for Reputational Harm Loss, as detailed in item 10) of this endorsement.

- 5) The following is added to section V. Definitions, 15. **Cyber Event**:

**Cyber Event** also means a **Reputational Harm Event**.

- 6) The following is added to section V. Definitions, 24. **First Party Coverage**:

**First Party Coverage** also means Insuring Agreement I.G.1., Reputational Harm.

- 7) The following is added to section V. Definitions, 37. **Loss**:

**Loss** also means **Reputational Harm Loss**.

For the purposes of this endorsement and solely with respect to Insuring Agreement I.G.1., Reputational Harm, **Loss** shall not include:

- a) variable costs, including the cost of raw materials and other costs, that would have been incurred by the **Insured Organization** during the applicable **Reputational Harm Indemnity Period** but were saved as a result of the **Reputational Harm Event**.
- 8) Section V. Definitions, 37. **Loss**, paragraph c., is deleted and replaced with the following:
  - c. an **Insured Organization's** internal operating costs, expenses, or fees, except to the extent covered under Insuring Agreement(s) I.C.1., I.C.2., and I.G.1.;

- 9) The following is added to section VI. Exclusions, B., Exclusions Applicable to Particular Insuring Agreements:

Exclusively with respect to Insuring Agreement I.G.1., Reputational Harm:

based upon or resulting from an **Adverse Publication** which:

- a) does not specifically state or refer to an **Insured Organization** or a **Covered Brand**;
  - b) does not specifically state or refer to an alleged or actual **Information Privacy Event** or **Network Security Event** experienced by an **Insured Organization**; or
  - c) is disseminated and directed to an **Insured** and is not available to the general public.
- 10) The following is added to section VII. Conditions:

#### LOSS CALCULATION FOR REPUTATIONAL HARM LOSS

In determining and calculating the amount of **Reputational Harm Loss** covered under this **Policy**, we shall use reasonable projections and give due consideration to:

- 1. the experience of the **Insured Organization's** business prior to the first occurrence of the **Reputational Harm Event**;
- 2. the public and market perception of the **Insured Organization** prior to the first occurrence of the **Reputational Harm Event**; and
- 3. the **Insured Organization's** net profit or net loss during the twelve (12) months immediately preceding the date of the **Reputational Harm Event's** first occurrence; and
- 4. market and industry trends, variations, and circumstances, including, but not limited to, seasonable influences and economic conditions, which would have affected the **Insured Organization's** business and operations regardless of the occurrence of the **Reputational Harm Event**.

We shall determine and calculate the amount of **Reputational Harm Loss** at our sole discretion, in good faith, and as we deem reasonable and necessary. Any disputes between us and the **Insured** over such determination and calculation shall be subject to the terms set forth in section VII., P., Disputes & Resolutions.

11) The following is added to section VII. Conditions, E. Notice, 1.:

Solely with respect to a **Reputational Harm Event**, and notwithstanding all other terms set forth in section VII.E.1., an **Insured** shall:

- a) give us written notice of any discovered **Reputational Harm Event** during the applicable **Reputational Harm Indemnity Period** following the first occurrence of such **Reputational Harm Event**.

Any notice of a **Reputational Harm Event** described in paragraph 11)a) above must include details and clear evidence that:

- b) such **Reputational Harm Event** is reasonably expected to lead, or already has led, to **Reputational Harm Loss**; and
- c) such **Reputational Harm Loss** is directly attributable to such **Reputational Harm Event**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## War & Cyber Terrorism Enhancement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section V. Definitions:

For the purposes of this endorsement and subject to the conditions, limitations, and other terms contained herein:

- a) **Cyber Terrorism** means the premeditated use of disruptive activities, or the threat to use disruptive activities, against a **Computer System**, including any associated network and data stored thereon, with the intention to cause harm, to further social, ideological, religious, political, or similar objectives, or to intimidate any person in furtherance of such objectives.

Provided further, however, that such activities set forth in item 1)a) directly above shall not be considered **Cyber Terrorism** when such activities are committed by, or at the express direction of, a government simultaneously engaged in an active conflict involving physical combat by one or more military forces of, or operating at the direction of, nation states or factions in the case of a civil war.

- 2) Section VI. Exclusions, A. Exclusions Applicable to All Insuring Agreements, item 9. War, is deleted and replaced with the following:

9. War

alleging, based upon, arising out of, or attributable to war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), strike, lock-out, riot, civil war, rebellion, revolution, insurrection, or civil commotion assuming the proportions of, or amounting to, an uprising, or military or usurped power.

However, this exclusion shall not apply to **Cyber Terrorism**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## California Consumer Privacy Act Enhancement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section V. Definitions:

**CCPA Penalties** means **Regulatory Penalties** an **Insured** becomes legally obligated to pay as a result of a **Regulatory Claim** for such **Insured's** actual, alleged or reasonably suspected non-compliance with the California Consumer Privacy Act, as amended.

- 2) The following is added to section V. Definitions, 17. **Damages**:

**Damages** include **CCPA Penalties** to the same extent that **Damages** include **Regulatory Penalties**, but solely with respect to, subject to, and notwithstanding the terms and conditions set forth in paragraph V.17.f..

- 3) The following is added to section V. Definitions, 30. **Information Privacy Event**:

**Information Privacy Event**, paragraph V.30.c., also includes, but is not limited to, any violation of the California Consumer Privacy Act, as amended, including any violation of requirements therein which govern the **Insured Organization's** use, sale, processing, profiling, acquisition, sharing, maintenance, and retention of **Protected Personal Information**.

- 4) The following is added to section V. Definitions, 54. **Privacy Regulations**:

**Privacy Regulations** include the California Consumer Privacy Act, as amended.

- 5) The following is added to section V. Definitions, 59. **Regulatory Claim**:

**Regulatory Claim** includes any **Claim** brought by, or on behalf of, any supervisory authority enforcing the California Consumer Privacy Act, as amended.

- 6) The following is added to section V. Definitions, 60. **Regulatory Penalties**:

**Regulatory Penalties** includes **CCPA Penalties**, but only to the extent such **CCPA Penalties** are civil fines or penalties imposed against an **Insured**:

- a) by any supervisory authority enforcing the California Consumer Privacy Act, as amended; and
- b) as a direct result of an otherwise covered **Regulatory Claim**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Law Enforcement Cooperation Enhancement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section VII. Conditions, E. Notice:

Notwithstanding anything in section VII.E.2., Notice of Circumstances, to the contrary:

- a) In the event an **Insured** receives a request from a law enforcement authority to keep confidential certain information about an actual, possible, or reasonably suspected **Cyber Event** or **Wrongful Act**, then the notice of such **Cyber Event** or **Wrongful Act**, including any **Claim** relating to or arising out of such **Cyber Event** or **Wrongful Act**, shall be considered timely under this **Policy**, provided the **Insured**:
  - i) requests permission from such law enforcement authority to share such information with us as soon as practicable following the receipt of such a request;
  - ii) only withholds from us that portion of the information that the law enforcement authority has instructed such **Insured** not share with us; and
  - iii) provides us with a full notice of such **Cyber Event**, **Wrongful Act**, or **Claim** as soon as legally possible after the law enforcement authority permits such **Insured** to share with us the full notice.
- b) Furthermore, with respect to any failure or delay by the **Insured** in providing information to us following receipt of a law enforcement authority request as set forth in part 1)a) of this endorsement:
  - i) the **Insured's** failure to provide documentation to us, or otherwise cooperate with us, will not be the basis for a denial of coverage for any **Cyber Event** or **Claim** under this **Policy**, but only to the extent the procedure set forth in part 1)a) of this endorsement is followed in connection with such authorized law enforcement request.

Notwithstanding the above, no coverage shall be afforded for any **Cyber Event** or **Claim** if the information withheld relating to such **Cyber Event** or **Claim** is subject to exclusion under section VI.A.6., Prior Knowledge, section VI.A.7., Pending or Prior Proceedings, or any other limitation in this **Policy** relating to any misrepresentations provided in the **Application**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Voluntary & Preventative Shutdown Coverage

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section V. Definitions, 65. **System Disruption**:

Subject to our prior consent, which will not be unreasonably withheld, **System Disruption** includes a measurable interruption, suspension, degradation, or failure in the service of:

- a) with respect to Insuring Agreement I.C.1. Direct Business Interruption, **Insured Computer Systems**; and
- b) with respect to Insuring Agreement I.C.2. Contingent Business Interruption, **External Computer Systems**:

directly caused by a **Voluntary Shutdown**.

- 2) The following is added to section V. Definitions:

**Voluntary Shutdown** means an **Insured's** voluntary, intentional, and reasonably necessary shutdown of:

- a) with respect to Insuring Agreement I.C.1. Direct Business Interruption, **Insured Computer Systems** in response to a credible or actual threat of an **Information Privacy Event**, a **Network Security Event**, or, if attached as an endorsement to this **Policy**, a **System Failure** expressly directed against such **Insured Computer Systems**, but only to the extent that:
  - i) a **System Disruption** may reasonably be expected in the absence of such shutdown; and
  - ii) such shutdown serves to mitigate, reduce, or avoid **Business Interruption Loss**; and
- b) with respect to Insuring Agreement I.C.2. Contingent Business Interruption, the **Insured's** connectivity or access to **External Computer Systems** in response to an actual **Information Privacy Event**, **Network Security Event**, or, if attached as an endorsement to this **Policy**, **System Failure** against such **External Computer Systems**, but only to the extent that:
  - i) a **System Disruption** may reasonably be expected in the absence of such shutdown; and
  - ii) such shutdown serves to mitigate, reduce, or avoid **Contingent Business Interruption Loss**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy** number: AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Financial Fraud Funds or Securities Endorsement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section V. Definitions, 27. **Funds or Securities**:

**Funds or Securities** also means any tangible, physical, or other assets which maintain a fungible, market, or transferrable monetary value.

**Funds or Securities** includes **Funds or Securities** that are owned by, or under the care, custody or control of, the **Insured Organization**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Social Engineering Forged Instruments Carveback

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section VI. Exclusions, C. Exclusions Applicable to Financial Fraud Insuring Agreements, item 3. Forged or Altered Instruments:

However, this exclusion shall not apply with respect to Insuring Agreement I.E.1., Social Engineering.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Explicit Bricking Coverage Endorsement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section V. Definitions, 38. **Malicious Code**:

**Malicious Code** includes **Bricking** that is functionally equivalent to **Malicious Code** described in paragraphs V.38.a. and V.38.b..

- 2) Section V. Definitions, 66. **System Restoration Loss**, paragraph a., is deleted and replaced with the following:

- a. restore **Computer Systems** to their level of functionality immediately prior to the applicable **Network Security Event**, including:

- i. replacing or reinstalling software programs contained therein; and
- ii. replacing or reinstalling computer hardware contained therein; provided, however, that this paragraph V.66.a.ii. is subject to:

- (a) section V. Definitions, 37. **Loss**, paragraph f. ii.; and
- (b) our determination that the replacement or reinstallation of computer hardware is essential to or will reduce the cost of the restoration effort of **Computer Systems** described in paragraph V.66.a. above;

- 3) The following is added to section V. Definitions:

**Bricking** means any software or computer program which is purposefully designed to adversely affect and render any computer hardware or "IoT" device, including any critical computer hardware, components, or software program contained therein, as useless, inaccessible, damaged, or non-functional to an extent which is beyond reasonable repair or restoration.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy** number: AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Affirmative Pay-On-Behalf Intent (1<sup>st</sup> Party)

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) Section I. Insuring Agreements, A. Information Privacy, item 3. Event Response and Management, is deleted and replaced with the following:

3. Event Response and Management

We shall pay the **Insured Organization** for, or pay on behalf of the **Insured Organization**, all **Technical Response Loss, Legal Services Loss, Public Relations Loss, Notification Loss, Reward Expense Loss, and Credit Monitoring Loss** incurred by the **Insured Organization** as a result of an **Information Privacy Event** first discovered during the **Policy Period**.

- 2) Section I. Insuring Agreements, B. Network Security, item 2. Event Response and Recovery, is deleted and replaced with the following:

2. Event Response and Recovery

We shall pay the **Insured Organization** for, or pay on behalf of the **Insured Organization**, all **Technical Response Loss, Public Relations Loss, Data Recovery Loss, Reward Expense Loss, and System Restoration Loss** incurred by the **Insured Organization** as a result of a **Network Security Event** first discovered during the **Policy Period**.

- 3) Section I. Insuring Agreements, D. Cyber Extortion, item 1. Cyber Extortion, is deleted and replaced with the following:

1. Cyber Extortion

We shall pay the **Insured Organization** for, or pay on behalf of the **Insured Organization**, all **Extortion Loss, Reward Expense Loss, and Public Relations Loss** incurred by the **Insured Organization** as a direct result of an **Extortion Threat** first discovered during the **Policy Period**.

- 4) Section I. Insuring Agreements, F. Media Content, item 2. Media Event Response, is deleted and replaced with the following:

2. Media Event Response

We shall pay the **Insured Organization** for, or pay on behalf of the **Insured Organization**, all **Public Relations Loss and Reward Expense Loss** incurred by the **Insured Organization** as a result of a **Media Wrongful Act** first discovered during the **Policy Period**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## HIPAA/HITECH Betterment Coverage (\$25,000)

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section V. Definitions:

**HIPAA/HITECH Betterment Expenses** means reasonable and necessary costs and expenses the **Insured Organization** becomes legally obligated to pay as a direct result of, and as part of, a final settlement or adjudication of a **Regulatory Claim** to:

- a) create, iterate or improve the **Insured Organization's** internal policies or practices in order to establish or re-establish the **Insured Organization's** compliance with the following **Privacy Regulations**;
  - i) the U.S. Health Insurance Portability and Accountability Act (HIPAA), as amended; and/or
  - ii) the Health Information Technology for Economic and Clinical Health Act (HITECH), as amended.

**HIPAA/HITECH Betterment Expenses** are part of and not in addition to **Regulatory Assessments and Expenses**.

- 2) The following is added to section V. Definitions, 58. **Regulatory Assessments and Expenses**:

**Regulatory Assessments and Expenses** includes **HIPAA/HITECH Betterment Expenses**, if applicable; provided, however, that:

- a) our maximum liability under this **Policy** and the most we shall pay for **HIPAA/HITECH Betterment Expenses** shall be \$25,000;
- b) the amount set forth in paragraph V.58.a) above is part of and not in addition to:
  - i) the **Aggregate Limit of Insurance**; and
  - ii) the amount stated as the Sub-Limit of Insurance for Insuring Agreement I.A.2. in ITEM 6. of the Declarations; and
- c) **HIPAA/HITECH Betterment Expenses** shall only be considered **Damages** covered under this **Policy** to the extent such **HIPAA/HITECH Betterment Expenses** are deemed insurable under the applicable laws of any jurisdiction which most favors coverage and which has a substantial relationship to an **Insured**, us, this **Policy** or the **Regulatory Claim** which gave rise to such **HIPAA/HITECH Betterment Expenses**.

- 3) Section V. Definitions, 17. **Damages**, paragraph f., is deleted and replaced with the following:
- f. with respect to a **Regulatory Claim** under Insuring Agreement I.A.2., any:
    - i) **Regulatory Penalties**;
    - ii) **GDPR Penalties**; and
    - iii) **Regulatory Assessments and Expenses**, including any **HIPAA/HITECH Betterment Expenses**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## PCI-DSS Betterment Coverage (\$25,000)

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

1) Section V. Definitions, 48. **PCI-DSS Response Expenses**, is deleted and replaced with the following:

48. **PCI-DSS Response Expenses** means reasonable and necessary costs and expenses to retain the services of:

- a. a third party forensic firm that is a qualified Payment Card Industry Forensic Investigator, to determine the cause and scope of the **Information Privacy Event** which led to a **PCI-DSS Claim**;
- b. a Qualified Security Assessor (QSA) to validate an **Insured Organization's** adherence to **PCI Data Security Standards** following a **PCI-DSS Claim**; and
- c. a **Cyber Response Firm** to improve the **Insured Organization's** computer systems or network security in order to establish or re-establish the **Insured Organization's** adherence to **PCI Data Security Standards** following a **PCI-DSS Claim**.

Our maximum liability under this **Policy** and the most we shall pay for costs and expenses described in paragraph V.48.c. above shall be \$25,000.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy** number: AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Enhanced Settlement Provision (90/10)

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) Section IV. Defense & Settlement of Claims, B. Settlement, item 1.b., is deleted and replaced with the following:
  - b. we shall pay and maintain responsibility for ninety percent (90%) of all **Claim Expenses** and **Damages** that are in excess of the amount referenced in paragraph IV.B.1.a. above.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy** number: AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Affirmative Voluntary Notification Costs (\$100,000)

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) Section V. Definitions, 44. **Notification Loss**, the last paragraph, is deleted and replaced with the following:

**Notification Loss** includes costs and expenses incurred in order to comply with applicable **Privacy Regulations** and shall follow the law of the applicable jurisdiction which most favors coverage for such costs and expenses. Those voluntary costs and expenses not required to comply with any applicable **Privacy Regulations** shall be subject to, and require, our prior consent if the total amount of such costs and expenses exceeds \$100,000.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Contingent Bodily Injury Coverage [Sub-Limit]

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section II. Limits of Insurance :

Solely with respect to the coverage afforded under part 2) of this endorsement, the most we shall pay, and our maximum liability, for all **Damages** and **Claims Expenses** resulting from any **Claim** alleging, based upon, arising out of, or attributable to **Bodily Injury** shall be:

- a) \$250,000.

Furthermore, the amount set forth directly above, in item 1)a) of this endorsement, will in no way serve to increase our liability under this **Policy** and shall be part of, and not in addition to, the Sub-Limit of Insurance for Insuring Agreement I.B.1. and the **Aggregate Limit of Insurance**.

- 2) The following is added to section VI. Exclusions, A. Exclusions Applicable to All Insuring Agreements, item 3. Bodily Injury:

However, this exclusion shall not apply to:

- a) solely with respect to Insuring Agreement I.B.1., any **Claim** for **Bodily Injury** directly caused by, or directly resulting from, an otherwise covered **Network Security Wrongful Act**.

- 3) The following is added to section VII. Conditions, J. Other Insurance:

As a condition precedent to the coverage provided under this endorsement, it is understood and agreed that:

- a) the **Insured** must maintain a valid and collectible commercial general liability insurance policy, effective throughout the **Policy Period** of this **Policy**, for its business activities and operations; and  
b) the coverage provided under this endorsement shall only apply to the extent no similar coverage is provided under any other insurance policy available to the **Insured** or, if applicable, any Additional Insureds for which coverage applies pursuant to section VII.A.2. Additional Insureds.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy** number: AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Invoice Manipulation Coverage

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section II. Limits of Insurance:

The following provisions shall apply solely with respect to coverage provided under Insuring Agreement I.E.2., Computer Fraud, in addition and subject to the provisions of section II. Limits of Insurance, and notwithstanding anything in the **Policy** to the contrary.

- a) Solely with respect to coverage provided and applied under Insuring Agreement I.E.2., Computer Fraud, as a direct result of **Computer Crimes** caused by **Invoice Manipulation**:
- i) our maximum liability under this **Policy** and the most we shall pay for any resulting **Computer Crimes Loss** incurred by the **Insured Organization** shall be the amount stated as the Sub-Limit of Insurance for Insuring Agreement I.E.2., Computer Fraud, in ITEM 6. of the Declarations; and
  - ii) the applicable amount of covered **Computer Crimes Loss**, pursuant to paragraph 1)a)i) above, shall be part of and not in addition to:
    - (1) the **Aggregate Limit of Insurance**; and
    - (2) the amount stated as the Sub-Limit of Insurance stated for Insuring Agreements I.E.2., Computer Fraud, in ITEM 6. of the Declarations.

- 2) Section V. Definitions, 8. **Computer Crimes**, is deleted and replaced with the following:

8. **Computer Crimes** means intentional, fraudulent, or unauthorized input, destruction, or modification of electronic data or computer instructions into **Computer Systems** by any entity which is not an **Insured Organization** or person who is not an **Insured Person**, provided that such **Computer Crimes** cause:
- a. **Funds or Securities** to be transferred, paid, or delivered;
  - b. an account of the **Insured Organization**, or of its customer, to be added, deleted, debited, or credited; or
  - c. **Invoice Manipulation**.

- 3) Section V. Definitions, 9. **Computer Crimes Loss**, is deleted and replaced with the following:

9. **Computer Crimes Loss** means:
- a. with respect to **Computer Crimes** which did not cause **Invoice Manipulation**, the **Insured Organization's** loss of **Funds or Securities**; or

- b. with respect to **Computer Crimes** which cause **Invoice Manipulation**, any **Invoice Costs** incurred by the **Insured Organization**.
- 4) The following are added to section V. Definitions:
  - a) **Invoice Manipulation** means the release or distribution of any fraudulent invoice or payment instruction to a third party which results in an **Uncollectable Invoice**.
  - b) **Uncollectable Invoice** means the **Insured Organization's** inability to collect payment of **Funds or Securities** from a third party, for goods, products or services that it has transferred or provided to such third party, as a result of the intentional, fraudulent, or unauthorized input, destruction, or modification of electronic data or computer instructions into **Computer Systems** by any entity which is not an **Insured Organization** or person who is not an **Insured Person**.
  - c) **Invoice Costs** means the direct net cost incurred by the **Insured Organization** to provide or transfer goods, products or services to a third party.

**Invoice Costs** shall not include any profit the **Insured Organization** expected to realize, as a result of transferring or providing such goods, products or services to such third party, had there been no **Computer Crimes** causing **Invoice Manipulation**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Funds Transfer Fraud Coverage

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) Section I. Insuring Agreements, E. Financial Fraud, 1. Social Engineering, is deleted and replaced with the following:

1. Social Engineering

We shall pay the **Insured Organization** for **Fraudulent Inducement Loss** and **Reward Expense Loss** incurred by the **Insured Organization** as a direct result of:

- a. **Fraudulent Inducement Instructions** it receives and accepts, and which are first discovered, during the **Policy Period**; or
- b. **Fraudulent Inducement Instructions** a **Financial Institution** receives and accepts, and which are first discovered, during the **Policy Period**.

- 2) The following is added to section V. Definitions, 25. **Fraudulent Inducement Instructions**:

Solely with respect to Insuring Agreement I.E.1., Social Engineering, part b., **Fraudulent Inducement Instructions** means a fraudulent electronic, telegraphic, cable, teletype, facsimile, telephone, or written instruction issued to a **Financial Institution**, without any **Insured's** knowledge, participation, or consent, which:

- a) directs such **Financial Institution** to transfer, pay, or deliver **Funds or Securities** from a **Bank Account**;
- b) directly causes **Funds or Securities** to be transferred, paid, or delivered from a **Bank Account**;
- c) is purportedly issued to such **Financial Institution** by an **Insured**; and
- d) is issued to such **Financial Institution** by any entity which is not an **Insured Organization** or by any person who is not an **Insured Person**.

**Fraudulent Inducement Instructions** covered under Insuring Agreement I.E.1., Social Engineering, part b., does not mean or include **Computer Fraud** otherwise covered under Insuring Agreement I.E.2., Computer Fraud.

- 3) The following is added to section V. Definitions, 37. **Loss**:

Solely with respect to Insuring Agreement I.E.1., Social Engineering, part b., **Loss** shall not include any:

- a) amounts for which a **Financial Institution** has agreed to indemnify or reimburse the **Insured Organization** following such **Financial Institution's** receipt and acceptance of **Fraudulent Inducement Instructions**;
  - b) amounts of income lost or not realized by the **Insured Organization** or by any third party whose **Funds or Securities** are under the care, custody, or control of the **Insured Organization**;-
  - c) amounts lost as a result of any actual or alleged use of credit, debit, charge, access, convenience, or other cards or the information or data contained within, or on, such cards;
  - d) amounts lost as a result of the extension of any loan, credit, or similar promise to pay; or
  - e) amounts incurred by any **Insured** to prove or establish the existence of **Fraudulent Inducement Instructions**.
- 4) The following is added to section V. Definitions:

**Bank Account** means any account:

- a) that is maintained by an **Insured Organization** at a **Financial Institution**; and
  - b) from which the **Insured Organization** can initiate the transfer, payment, or delivery of **Funds or Securities**.
- 5) The following is added to section V. Definitions:

**Financial Institution** means any financial or banking institution at which the **Insured Organization** maintains **Funds or Securities** in a **Bank Account**.

**Financial Institution** does not include any organization, entity, or institution which is an **Insured Organization**.

- 6) The following is added to section VII. Conditions, J. Other Insurance:

Solely with respect to Insuring Agreement I.E.1., Social Engineering:

If any **Insured** or any other party at interest in any **Fraudulent Inducement Loss** covered under this **Policy** has any other crime insurance, including but not limited to any other crime or fidelity bond, indemnity, or similar insurance, which would cover amounts of such loss in whole or in part in the absence of this **Policy**, then this **Policy** shall be null and void to the extent of the amount received or recoverable under such other crime insurance; provided further, however, that this **Policy** shall cover any otherwise covered **Fraudulent Inducement Loss** to the extent the amount of such **Fraudulent Inducement Loss** is in excess of the amount recoverable or received under the other crime insurance.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## CryptoJacking & Utility Coverage [Full Limits]

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section I. Insuring Agreements, B. Network Security, item 2. Event Response and Recovery:

Solely with respect to the coverage provided under this endorsement, Insuring Agreement I.B.2., Event Response and Recovery, also includes the following:

We shall pay the **Insured Organization** for, or pay on behalf of the **Insured Organization**, all **Utility Loss** incurred by the **Insured Organization** as a result of a **Network Security Event** first discovered during the **Policy Period**.

- 2) The following is added to section V. Definitions:

**Crypto-Currency** means a digital currency or asset which is electronically stored and transferred, is operated independently of any central bank or other central authority, and requires cryptographic techniques to verify and regulate its transfer and generation.

- 3) The following is added to section V. Definitions:

**CryptoJacking** means the gaining of access to, or use of, an **Insured Computer System** by:

- a) an unauthorized person; or
- b) an authorized person for purposes not authorized by an **Insured Organization**;

to mine for **Crypto-Currency**.

- 4) The following is added to section V. Definitions:

**Telephone Fraud** means the gaining of access to, or use of, an **Insured Computer System** by:

- a) an unauthorized person; or
- b) an authorized person for purposes not authorized by an **Insured Organization**;

to fraudulently infiltrate and manipulate telecommunications or telephone system(s) from a remote location.

- 5) The following is added to section V. Definitions:

**Utility Loss** means additional amounts incurred by the **Insured Organization** for its use of, or access to, any of the following utility services or resources:

- a) electricity, natural gas, oil, water, or sewage;
- b) television or internet; or
- c) telecommunication or telephone toll, line, or long distance communication.

Provided further, however, that such **Utility Loss** includes only those additional amounts which:

- d) are charged to the **Insured Organization** by the provider of the respective utility resource or service:
  - i) in a periodic billing statement due for payment during the **Policy Period**;
  - ii) pursuant to a written contract between the **Insured Organization** and such utility resource or service provider that was executed before the **CryptoJacking** or **Telephone Fraud** first occurred; and
  - iii) in excess of any amount(s) which the **Insured Organization** would have incurred had no **CryptoJacking** or **Telephone Fraud** occurred;
- e) are not charged to the **Insured Organization** at a flat fee that does not scale with the rate or use of the respective utility resource or service.

- 6) The following is added to section V. Definitions, 37. **Loss**:

Solely with respect to Insuring Agreement I.B.2., Event Response and Recovery:

**Loss** also means **Utility Loss**, but solely to the extent such **Utility Loss** is incurred by the **Insured Organization** as a direct result of **CryptoJacking** or **Telephone Fraud**.

- 7) The following is added to section V. Definitions, 42. **Network Security Event**.

Solely with respect to Insuring Agreement I.B.2., Event Response and Recovery:

**Network Security Event** also means any actual or reasonably suspected **CryptoJacking** or **Telephone Fraud**, but solely to the extent such **CryptoJacking** or **Telephone Fraud** results directly in **Utility Loss** incurred by the **Insured Organization**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

## Breach Costs Outside [Additional Limit]

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to the **Policy**:

	Value
<b>Additional Breach Costs Limit:</b>	\$1,000,000.

Provided further, however, that if the amount stated in ITEM 6 of the Declarations as the Sub-Limit of Insurance applicable to Insuring Agreement I.A.3. is less than \$1,000,000, then the amount of **Additional Breach Costs Limit** provided under this endorsement shall not be \$1,000,000 but instead shall be an amount equal to the Sub-Limit of Insurance applicable to Insuring Agreement I.A.3..

- 2) The following is added to section II. Limits of Insurance:

### C. BREACH COSTS OUTSIDE [ADDITIONAL LIMIT]

The conditions, limitations, and other terms of this section II.C. shall apply solely with respect to coverage provided under Insuring Agreement I.A.3., Event Response and Management.

- (1) **Loss** incurred by the **Insured Organization** as a result of an **Information Privacy Event** first discovered during the **Policy Period** under Insuring Agreement I.A.3. shall first apply to, and reduce, the **Additional Breach Costs Limit**.
- (2) The **Additional Breach Costs Limit** shall be:
  - a) one single additional limit of insurance applicable solely to **Loss** incurred under, and pursuant to, Insuring Agreement I.A.3., regardless of the number of **Information Privacy Events** discovered during the **Policy Period**; and
  - b) in addition to, and not part of, the Sub-Limit of Insurance applicable to Insuring Agreement I.A.3. and the **Aggregate Limit of Insurance**.
- (3) Payment of the **Additional Breach Costs Limit** by us shall reduce, and may exhaust, the **Additional Breach Costs Limit**. If the **Additional Breach Costs Limit** is exhausted by our payment of **Loss**, we shall have no further obligations with respect to the **Additional Breach Costs Limit** coverage provided under this endorsement.

- (4) Upon exhaustion of the **Additional Breach Costs Limit**, any further payment by us of **Loss** incurred by the **Insured Organization** as a result of an **Information Privacy Event** first discovered during the **Policy Period** under Insuring Agreement I.A.3. shall:
- a) be part of, and not in addition to, the Sub-Limit of Insurance applicable to Insuring Agreement I.A.3. and the **Aggregate Limit of Insurance**; and
  - b) reduce, and may exhaust, the Sub-Limit of Insurance applicable to Insuring Agreement I.A.3. and the **Aggregate Limit of Insurance**.
- 3) The following is added to section II. Limits of Insurance, A. Aggregate Limit of Insurance:
- This section II.A., Aggregate Limit of Insurance, shall apply subject to section II.C., which is set forth in part 2) of this endorsement.
- 4) The following is added to section II. Limits of Insurance, B. Sub-Limits of Insurance:
- This section II.B., Sub-Limits of Insurance, shall apply subject to section II.C., which is set forth in part 2) of this endorsement.
- 5) The following is added to section V. Definitions:
- Additional Breach Costs Limit** means the amount set forth in part 1) of this endorsement.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy** number: AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## OFAC Exclusion Endorsement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section VI. Exclusions, A. Exclusions Applicable to All Insuring Agreements:

alleging, based upon, arising out of, or attributable to the violation of, or the exposure of any **Insured** or us to, any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws, regulations of the United States Treasury Department's Office of Foreign Assets Control ("OFAC").

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Government Action & Licensing Exclusion

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) Section VI. Exclusions, B. Exclusions Applicable to Particular Insuring Agreements, item 8. Licensing is deleted in its entirety.
- 2) The following is added to section VI. Exclusions, A. Exclusions Applicable to All Insuring Agreements:

alleging, based upon, arising out of, or attributable to any governmental investigation or enforcement of any federal, state, or local regulation or any action brought by or on behalf of the Federal Trade Commission, the Federal Communications Commission, or any other federal, state, or local government agency, or ASCAP, SESAC, BMI or other licensing or rights entities in such entity's regulatory, quasi-regulatory, or official capacity, function or duty.

However, this exclusion shall not apply to:

- a. an otherwise covered **Regulatory Claim** under Insuring Agreement I.A.2. of this **Policy**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Amendment to Pollution and Nuclear, Biological, and Chemical Contamination Exclusions Endorsement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) Section V. Definitions, 52. **Pollution**, is deleted and replaced with the following:
  52. **Pollution** means any liquid, gaseous, solid or thermal irritant or contaminant, including vapor, smoke, fumes, acids, chemicals, microorganisms, mold, mildew, fungus, spores, bacteria, disease, virus, and materials to be recycled, reconditioned or reclaimed.
- 2) Section VI. Exclusions, A. Exclusions Applicable to All Insuring Agreements, item 8. Pollution, is deleted and replaced with the following:
  8. Pollution  
alleging, based upon, arising out of, or attributable to:
    - a. the presence or actual, alleged or threatened discharge, release, seepage, migration, or disposal of **Pollution**;
    - b. any request that any **Insured** test for, monitor, clean up, remove, contain, treat, detoxify, or neutralize **Pollution**, including any voluntary decision to do so; or
    - c. any request or requirement brought by or on behalf of any governmental authority relating to testing, monitoring, cleaning, removing, containing, treating, neutralizing, or in any way responding to or assessing the effects of **Pollution**.
- 3) Section VI. Exclusions, A. Exclusions Applicable to All Insuring Agreements: 10. Nuclear, Biological, and Chemical Contamination is deleted and replaced with the following:

10. Nuclear, Biological, and Chemical Contamination:

alleging, based upon, arising out of, or attributable to any planning, construction, maintenance, or use of any nuclear reactor, nuclear storage, disposal, waste or radiation site, or any other nuclear facility or site, the transportation of nuclear material, or any nuclear reaction or radiation, or radioactive, biological, including, but not limited to, mold, mildew, fungus, spores, disease, virus or microorganism of any type, nature or description, or chemical contamination, regardless of its cause.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Biometric Privacy Violation Exclusion (Data Breach Carveback)

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to section VI. Exclusions, A. Exclusions Applicable to All Insuring Agreements:

### Biometric Privacy Violation

alleging, based upon, arising out of, or attributable to any violation of the Biometric Information Privacy Act (BIPA) or any similar federal, state, common, or foreign law.

However, this exclusion shall not apply to:

- a. solely with respect to Insuring Agreements I.A.1. and I.A.2., an otherwise covered **Claim** for an **Information Privacy Wrongful Act** based upon or resulting from any actual or reasonably suspected failure to prevent unauthorized access to **Protected Personal Information**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

## Business Interruption Waiting Period Endorsement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to the **Policy**:

The applicable and respective value of **Business Interruption Waiting Period** is stated in the following table:

	Value
<b>Business Interruption Waiting Period:</b>	8 hours.

- 2) The following is added to Section III. Retention:

In addition and subject to all other provisions of Section III. Retention and solely with respect to coverage provided under Insuring Agreements I.C.1. and I.C.2., if a **System Disruption** of **Computer Systems** directly results from a **Network Security Event** or **Information Privacy Event** then:

- a) for each such **System Disruption**:
  - i) our liability shall apply only after the **Business Interruption Waiting Period** has elapsed; and
  - ii) only to that portion of **Loss** incurred by the **Insured Organization** after such **Business Interruption Waiting Period** has elapsed; and
- b) if the applicable **System Disruption** is covered under both Insuring Agreements I.C.1. and I.C.2.:
  - i) the sum of the **Business Interruption Waiting Periods** shall not exceed the largest applicable **Business Interruption Waiting Period**; and
- c) the **Retention** amount in ITEM 6 of the Declarations will not apply.

- 3) Section V. Definitions, 49. **Period of Restoration**, is deleted and replaced with the following:

49. **Period of Restoration** means the continuous period of time that:

- a. begins with the expiration of the **Business Interruption Waiting Period**; and
- b. ends on the date when **Insured Computer Systems** or **External Computer Systems** are, or could have been, repaired or restored with reasonable speed to the same functionality and level of service which existed prior to the **System Disruption**.

A **Period of Restoration** shall not exceed one hundred eighty (180) days from the date the applicable **System Disruption** first occurred; provided, however, that the end of the **Policy Period** shall not cut short the **Period of Restoration**.

4) The following are added to section V. Definitions:

- a) **Business Interruption Waiting Period** means the number of hours stated as the value of **Business Interruption Waiting Period** within the table under part 1) of this endorsement.

The **Business Interruption Waiting Period** begins at the date and time the actual **System Disruption** starts, and ends after the number of **Business Interruption Waiting Period** hours have elapsed.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

## Contingent and Direct System Failure (for use with Business Interruption Waiting Period Endorsement)

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to the **Policy**:

The applicable and respective values of **Direct System Failure Limit**, **Contingent System Failure Limit**, and **System Failure Waiting Period** are stated in the following table.

	Value
<b>Direct System Failure Limit:</b>	\$1,000,000.
<b>Contingent System Failure Limit:</b>	\$1,000,000.
<b>System Failure Waiting Period:</b>	8 hours.

- 2) The following is added to section II. Limits of Insurance:

The following provisions shall apply solely with respect to coverage provided under Insuring Agreements I.C.1. and I.C.2., in addition and subject to the provisions of section II. Limits of Insurance, and notwithstanding anything in the **Policy** to the contrary.

- a) With respect to coverage provided and applied under Insuring Agreements I.C.1., the **Direct System Failure Limit** is:
- i) part of and not in addition to the **Aggregate Limit of Insurance** and the applicable Sub-Limit of Insurance stated in ITEM 6 of the Declarations for Insuring Agreements I.C.1..
- b) With respect to coverage provided and applied under Insuring Agreements I.C.2., the **Contingent System Failure Limit** is:
- i) part of and not in addition to the **Aggregate Limit of Insurance** and the applicable Sub-Limit of Insurance stated in ITEM 6 of the Declarations for Insuring Agreements I.C.2..

- 3) The following is added to the section III. Retention:

In addition and subject to all other provisions of Section III. Retention and solely with respect to coverage provided under Insuring Agreements I.C.1. and I.C.2., if a **System Disruption** of **Computer Systems** directly results from a **System Failure** then:

- a) for each such **System Disruption**:
    - i) our liability shall apply only after the **System Failure Waiting Period** has elapsed; and
    - ii) only to that portion of **Loss** incurred by the **Insured Organization** after such **System Failure Waiting Period** has elapsed; and
  - b) if the applicable **System Disruption** is covered under both Insuring Agreements I.C.1. and I.C.2.:
    - i) the sum of the **System Failure Waiting Periods** shall not exceed the largest applicable **System Failure Waiting Period**; and
  - c) if such **System Disruption** is also the direct result of a **Network Security Event** or **Information Privacy Event**:
    - i) the **System Failure Waiting Period** shall apply only to that portion of the **System Disruption** which is a direct result of a **System Failure**; and
  - d) the **Retention** amount in ITEM 6 of the Declarations will not apply.
- 4) Section V. Definitions, 49. **Period of Restoration**, is deleted and replaced with the following:
49. **Period of Restoration** means the continuous period of time that:
- a. begins:
    - i. with respect to a **System Disruption** that is directly caused by a **Network Security Event** or **Information Privacy Event**, with the expiration of the **Business Interruption Waiting Period**; or
    - ii. with respect to a **System Disruption** that is directly caused by a **System Failure**, with the expiration of the **System Failure Waiting Period**; and
  - b. ends on the date when **Insured Computer Systems** or **External Computer Systems** are, or could have been, repaired or restored with reasonable speed to the same functionality and level of service which existed prior to the **System Disruption**.

A **Period of Restoration** shall not exceed one hundred eighty (180) days from the date the applicable **System Disruption** first occurred; provided, however, that the end of the **Policy Period** shall not cut short the **Period of Restoration**.

- 5) Section V. Definitions, 65. **System Disruption**, is deleted and replaced with the following:
65. **System Disruption** means the measurable interruption, suspension, degradation, or failure in the service of:
- a. with respect to Insuring Agreement I.C.1., **Insured Computer Systems**; and

b. with respect to Insuring Agreement I.C.2., **External Computer Systems**;

directly caused by a **Network Security Event**, **Information Privacy Event**, or **System Failure**.

6) The following are added to section V. Definitions:

a) **Contingent System Failure Limit** means, solely with respect to coverage provided under Insuring Agreements I.C.2., the amount stated as the value of **Contingent System Failure Limit** within the table under part 1) of this endorsement.

The **Contingent System Failure Limit** is the most we shall pay, and represents our maximum liability, for all **Contingent Business Interruption Loss**, **Extra Expense**, **Public Relations Loss**, and **Reward Expense Loss**, combined, resulting from a **System Disruption** of **External Computer Systems** directly caused by a **System Failure**.

b) **Direct System Failure Limit** means, solely with respect to coverage provided under Insuring Agreements I.C.1., the amount stated as the value of **Direct System Failure Limit** within the table under part 1) of this endorsement.

The **Direct System Failure Limit** is the most we shall pay, and represents our maximum liability, for all **Business Interruption Loss**, **Extra Expense**, **Public Relations Loss**, and **Reward Expense Loss**, combined, resulting from a **System Disruption** of **Insured Computer Systems** directly caused by a **System Failure**.

c) **Human Error or Omission** means an operating error or omission by:

- i) an **Employee**; or
- ii) an entity which is not an **Insured Organization**, or a person who is not an **Insured Person**, in their provision, fulfillment or delivery of services to an **Insured Organization**.

**Human Error or Omission** includes, but is not limited to, errors or omissions in the selection, utilization, choice, or incorrect or inappropriate intervention of computer programs, software and parameters.

d) **Infrastructure Power Failure** means a failure, surge or capacity reduction of an electrical system, network or infrastructure under the direct operational control of the **Insured Organization**.

e) **Programming Error** means an error that occurs during the programming, development or encoding of any computer software, program, application, firmware, or operating system that results in an interruption of the **Insured Organization's** operations or the malfunction or inoperability of **Computer Systems**.

f) **System Failure** means any unplanned and measurable interruption, suspension, degradation, or failure in the service of **Computer Systems** which is not directly caused by a **Network Security Event** or **Information Privacy Event**.

**System Failure** includes, but is not limited to, an unplanned:

- i) **Human Error or Omission**;
- ii) **Programming Error**; or
- iii) **Infrastructure Power Failure**.

- g) **System Failure Waiting Period** means the number of hours stated as the value of **System Failure Waiting Period** within the table under part 1) of this endorsement.

The **System Failure Waiting Period** begins at the date and time the actual **System Disruption** starts, and ends after the number of **System Failure Waiting Period** hours have elapsed.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

## Contingent Non-IT Provider System Disruption (for use with Contingent and Direct System Failure Endorsement)

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of the premium charged, it is agreed that the **Policy** is amended as follows:

- 1) The following is added to the **Policy**:

The applicable and respective value of the **Contingent Non-IT Provider Business Interruption Limit** and **Contingent Non-IT Provider System Failure Limit** is stated in the following table:

	Value
<b>Contingent Non-IT Provider Business Interruption Limit:</b>	\$1,000,000.
<b>Contingent Non-IT Provider System Failure Limit:</b>	\$1,000,000.

- 2) The following is added to section II. Limits of Insurance:

The following provisions shall apply solely with respect to coverage provided under Insuring Agreements I.C.2., in addition and subject to the provisions of section II. Limits of Insurance, and notwithstanding anything in the **Policy** to the contrary.

- a) With respect to coverage provided and applied under Insuring Agreements I.C.2., the **Contingent Non-IT Provider Business Interruption Limit** and **Contingent Non-IT Provider System Failure Limit** is:

- i) part of and not in addition to the **Aggregate Limit of Insurance** and the applicable Sub-Limit of Insurance stated in ITEM 6 of the Declarations for Insuring Agreements I.C.2..

- 3) The follow is added to Section V. Definitions, 10. **Computer Systems**:

Solely with respect to Insuring Agreement I.C.2. Contingent Business Interruption, **Computer Systems** also means **Non-IT Provider Computer Systems**.

- 4) Section V. Definitions, 11. **Contingent Business Interruption Loss** is deleted and replaced as follows:

11. **Contingent Business Interruption Loss** means the following amounts incurred by an **Insured Organization** during the **Period of Restoration**:

- a. net profit before income taxes that would have been earned had no **System Disruption** of **External Computer Systems** or **Non-IT Provider Computer Systems** occurred;
- b. net loss before income taxes that would have been avoided had no **System Disruption** of **External Computer Systems** or **Non-IT Provider Computer Systems** occurred;
- c. the **Insured Organization's** continuing normal operating and payroll expenses; and
- d. costs to retain the services of a third party forensic accounting firm to determine the amounts of **Contingent Business Interruption Loss** described in paragraphs V.11.a.–V.11.c. above, subject to our prior consent.

5) Section V. Definitions, 49. **Period of Restoration**, is deleted and replaced with the following:

49. **Period of Restoration** means the continuous period of time that:

- a. begins:
  - i. with respect to a **System Disruption** that is directly caused by a **Network Security Event** or **Information Privacy Event**, with the expiration of the **Business Interruption Waiting Period**; or
  - ii. with respect to a **System Disruption** that is directly caused by a **System Failure**, with the expiration of the **System Failure Waiting Period**; and
- b. ends on the date when **Insured Computer Systems**, **External Computer Systems**, or **Non-IT Provider Computer Systems** are, or could have been, repaired or restored with reasonable speed to the same functionality and level of service which existed prior to the **System Disruption**.

A **Period of Restoration** shall not exceed one hundred eighty (180) days from the date the applicable **System Disruption** first occurred; provided, however, that the end of the **Policy Period** shall not cut short the **Period of Restoration**.

6) The following is added to section V. Definitions, 65. **System Disruption**:

Subject to our prior consent, which will not be unreasonably withheld, **System Disruption** includes a measurable interruption, suspension, degradation, or failure in the service of:

- a) with respect to Insuring Agreement I.C.1. Direct Business Interruption, **Insured Computer Systems**; and
- b) with respect to Insuring Agreement I.C.2. Contingent Business Interruption, **External Computer Systems** or **Non-IT Provider Computer Systems**.

directly caused by a **Network Security Event**, **Information Privacy Event**, or **System Failure**.

7) The following is added to Section V. Definitions:

- a) **Contingent Non-IT Provider Business Interruption Limit** means, solely with respect to coverage provided under Insuring Agreements I.C.2., the amount stated as the value of **Contingent Non-IT Provider Business Interruption Limit** within the table under paragraph 1) of this endorsement.

The **Contingent Non-IT Provider Business Interruption Limit** is the most we shall pay, and represents our maximum liability, for all **Contingent Business Interruption Loss, Extra Expense, Public Relations Loss, and Reward Expense Loss**, combined, resulting from a **System Disruption of Non-IT Provider Computer Systems** directly caused by a **Network Security Event** or **Information Privacy Event**.

- b) **Contingent Non-IT Provider System Failure Limit** means, solely with respect to coverage provided under Insuring Agreements I.C.2., the amount stated as the value of **Contingent Non-IT Provider System Failure Limit** within the table under paragraph 1) of this endorsement.

The **Contingent Non-IT Provider System Failure Limit** is the most we shall pay, and represents our maximum liability, for all **Contingent Business Interruption Loss, Extra Expense, Public Relations Loss, and Reward Expense Loss**, combined, resulting from a **System Disruption of Non-IT Provider Computer Systems** directly caused by a **System Failure**.

- c) **Non-IT Provider** means any entity that is not owned, operated, or controlled by an **Insured** that provides products or services to an **Insured Organization** pursuant to a written contract with the **Insured Organization** for the provision of such products or services.

- d) **Non-IT Provider Computer Systems** means any computer hardware, software, firmware, wireless device, voice based telecommunication system, operating system, virtual machine, as well as any data stored thereon, and:

- i) associated input, output, processing, data storage, and mobile devices, networks, operating systems, application software, networking equipment, storage area networks, and other electronic data storage or backup facilities; and
- ii) includes, but is not limited to, associated telephone systems (including "PBX", "CBX," "Merlin," or "VoIP"), remote access systems (including "DISA"), peripheral communication equipment and systems, industrial control systems (including "SCADA"), Internet of things (commonly referred to as "IoT"), media libraries, extranets, and offline electronic data storage facilities;

which are rented, leased, owned, or operated by a **Non-IT Provider**.

**Non-IT Provider Computer Systems** does not mean **Insured Computer Systems** or **External Computer Systems**.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.



This endorsement is attached to, forms part of, and modifies:

**Policy number:** AB-6617380-04  
**Named Insured:** Caissa Public Strategy, LLC

---

## Embedded Security Endorsement

Insurance coverage underwritten by At-Bay Specialty Insurance Company | 1209 Orange Street | Wilmington, DE 19801

In consideration of **Embedded Security** fee identified in ITEM 3 of the Declarations, it is agreed that this **Policy** is amended as follows:

- 1) During the **Policy Period**, **Embedded Security** is available to the **Named Insured**.
- 2) The following is added to Section V. Definitions:

**Embedded Security** means the cybersecurity loss control and risk management tools, included as part of At-Bay's cybersecurity risk management solution. **Embedded Security** offerings include:

- At-Bay Stance™ Exposure Manager. A purpose-built platform that provides regular scans to identify your IT assets, scans for vulnerabilities, prioritizes actions based on threat intelligence, and showcases a unified risk dashboard.
- At-Bay Stance™ Managed Security. Managed Security may include, but is not limited to, the following: risk advisory services; preferred pricing and select subsidized offerings on third-party risk management tools, solutions, and services; mitigation and implementation services; and other cyber loss control and risk management tools and resources.

Eligibility, rules, and limitations will vary based on your risk profile and security requirements. For details and instructions on how to activate your Exposure Manager account and for a current list of the **Embedded Security** offerings that may be available to you please visit: [at-bay.com/embedded-security](https://at-bay.com/embedded-security).

**Embedded Security** offerings may be provided by At-Bay Insurance Services, LLC, its affiliates, or other third parties and may require the **Named Insured** to enter into a separate agreement with the relevant company. For the avoidance of doubt, it is the sole discretion of the **Named Insured** to engage with any of the **Policy's Embedded Security** offerings and such engagement has no impact on the premium or fees charged under this **Policy**.

From time to time At-Bay may enter into agreements with third parties to make available the loss control services or products referenced above. At-Bay's agreement with any third party does not eliminate any **Insured's** obligations under this **Policy** or change any terms of this **Policy**. At-Bay's agreement with any third party and any related program may be terminated at any time.

- 3) Section VII. Conditions, G. Policy Termination, is modified to the extent necessary to provide the following:

If this **Policy** is canceled by the **Named Insured** prior to the end of the **Policy Period**, we shall refund the **Embedded Security** fee identified in ITEM 3 of the Declarations computed pro rata.



Such adjustment shall be made as soon as practical upon termination of the **Policy**, but payment or tender of any such fee by us shall not be a condition precedent to the effectiveness of such termination.

All other terms, conditions, and exclusions of the **Policy** shall remain unchanged.

## Notice to Policyholders

Includes copyrighted material of Insurance Services Office, Inc., with its permission

In accordance with TRIA requirements, this Notice is being provided to our Policyholders:

### DISCLOSURE PURSUANT TO TERRORISM RISK INSURANCE ACT

THIS NOTICE IS ATTACHED TO AND MADE PART OF YOUR POLICY IN RESPONSE TO THE DISCLOSURE REQUIREMENTS OF THE TERRORISM RISKINSURANCE ACT. THIS NOTICE DOES NOT GRANT ANY COVERAGE OR CHANGE THE TERMS AND CONDITIONS OF ANY COVERAGE UNDER THE POLICY.

SCHEDULE – PART I
<p>Terrorism Premium (Certified Acts): \$0</p> <p>This premium is the total Certified Acts premium attributable to the following Coverage Part(s), Coverage Form(s) and/or Policy(ies):</p> <p><i>Cyber Insurance Policy</i></p>
SCHEDULE – PART II
<p>Federal Share of Terrorism Losses: 80% (refer to Paragraph B. below)</p> <p>Information required to complete this Schedule, if not shown above, will be shown in the Declarations.</p>

#### A. Disclosure of Premium

In accordance with the federal Terrorism Risk Insurance Act, we are required to provide you with a notice disclosing the portion of your premium, if any, attributable to coverage for terrorist acts certified under the Terrorism Risk Insurance Act. The portion of your premium attributable to such coverage is shown in the Schedule of this notice or in the policy Declarations.

#### B. Disclosure of Federal Participation in Payment of Terrorism Losses

The United States Government, Department of the Treasury, will pay a share of terrorism losses insured under the federal program. The federal share equals a percentage (as shown in Part II of the Schedule of this notice or in the policy Declarations) of that portion of the amount of such insured losses that exceeds the applicable insurer retention. However, if aggregate insured losses attributable to terrorist acts certified under the Terrorism Risk Insurance Act exceed \$100 billion in a calendar year, the Treasury shall not make any payment for any portion of the amount of such losses that exceeds \$100 billion.

#### C. Cap on Insurer Participation in Payment of Terrorism Losses

If aggregate insured losses attributable to terrorist acts certified under the Terrorism Risk Insurance Act exceed \$100 billion in a calendar year and we have met our insurer deductible under the Terrorism Risk Insurance Act, we shall not be liable for the payment of any portion of the amount of such losses that exceeds \$100 billion, and in such case insured losses up to that amount are subject to pro rata allocation in accordance with procedures established by the Secretary of the Treasury.