**Data Security Exhibit**

This Data Security is made a part of the **Master Services Agreement** between Client and Everbridge. The Agreement, including without limitation this Data Security exhibit, reflect the parties' agreement with regard to the security and safeguarding of Client Data. Unless otherwise stated, capitalized terms in this Data Security exhibit shall have the meanings set forth in the Agreement.

**1. Security Framework**

1.1 Everbridge's security framework is based on the comprehensive set of security requirements and controls within US National Institute of Standards and Technology ("NIST") Special Publication 800-53 – Security and Privacy Controls for Information Systems and Organizations, the ISO 27001 framework, and the General Data Protection Regulation ("GDPR") for privacy compliance.

1.2 Annually, Everbridge achieves certification and accreditation from an independent third-party assessment organization ("3PAO") approved under the Federal Risk and Authorization Management Program (FedRAMP).

**2. Globally Applicable Certifications**.

2.1 **SSAE-18 SOC 3.** Annually, Everbridge publishes a Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a publicly available summary of the Everbridge SOC 2 Type II report.

2.2 **ISO/IEC 27001 Certification**. The Everbridge suite of products that are ISO-certified include Mass Notification, Safety Connection™, Crisis Management, Visual Command Center®, IT Alerting, SMARTweather and ThreatView, and Everbridge's mobile apps, both in the United States and Europe.

2.3 **US Government Certifications.**

(a) **FedRAMP Authorization**. Everbridge Suite has achieved the Federal Risk and Authorization Management Program, or FedRAMP, compliance and authorization. FedRAMP is a United States government-wide program that provides a standardized approach (based on NIST SP 800-53 revision 4) to security assessment, authorization, and continuous monitoring for cloud products and services.

(b) **Telecommunication Service Priority (TSP) Level 3 Certified.** Everbridge maintains a certification as a Level 3 Telecommunication Service Priority (TSP) System by the Department of Homeland Security (DHS).

(c) **SAFETY Act.** The United States Department of Homeland Security (DHS) has designated and certified Everbridge under the SAFETY Act (Support Anti-terrorism by Fostering Effective Technology). Pursuant to the SAFETY Act, the designation provides legal liability protections to both Everbridge and its customers in the result of technology failures during a DHS declared terrorist attack. Applications on the Everbridge critical communications platform are now on the DHS SAFETY Act's "Approved Technologies List."

2.4 **EU Privacy & Security Compliance.**

(a) **Data Regulations and Frameworks**. Everbridge maintains compliance with General Data Protection Regulation (GDRP) and current EU legislation, including the Data Protection Directive 95/46/EC, the UK Data Protection Act, and the German Federal Data Protection Act (Bundesdatenschutgesetz) and is certified under the EU-US Privacy Shield. Everbridge participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework.

(b) **BSI Cloud Computing Compliance Control Catalog (C5).** The Everbridge Critical Event Management platform has undergone a third-party audit to ensure it complies with security requirements defined by C5.

2.5 **UK Government Listings**

(a) **G-Cloud.** The Everbridge Critical Event Management platform is a listed vendor within the G-Cloud framework. G-Cloud is the UK government's latest framework that is designed to simplify and accelerate adoption of cloud-based services within the public sector.

(b) **UK ICO.** Everbridge is registered by the Information Commissioner's Office. This UK-based governmental office upholds information rights in the public interest, promoting openness by public bodies and data privacy.

**3. Physical Security.**

3.1 **Corporate Office Locations**

(a) Multiple levels of access control are used at Everbridge company location including secured elevator access, secure corporate office space, and use of employee access cards.

(i) **Employees**: All employees are issued picture ID badges and encoded access cards that allow admission to the elevators, stairwells, and the company suite. The issuance of access cards is controlled by a designated company employee and all requests for access cards must be approved by a senior company executive and must be presented to building security.

(ii) **Non-Employees**. Non-employees (vendors, visitors, and customers) must sign in at the lobby desk. Building security must enable an elevator to take the non-employee to the proper building floor. Non-employees must request access to the company's suite via an intercom that is positioned just outside the main suite doors. All visitors and vendors are always escorted by an Everbridge employee inside the company suite.

(b) Both building and corporate office spaces are covered by 24x7x365 CCTV and recordings are maintained for 90 days unless otherwise required.

3.2 **Hosting Facilities**

(a) All hosting facilities are SOC2 or ISO27001 compliant and undergo annual audits. Physical security controls at the facilities include 24/7 on-site security staff, photo ID required for entry into the data centers, card key and biometrics scans required for collocation space, computerized access control system, video surveillance at all entrances and on every aisle, locked racks and cabinets, and visitors are not permitted.

(b) Everbridge maintains active service agreements with all providers that include security compliance, SLAs, and confidentiality. At no time is any third party provider granted access to the Everbridge solution or the client data therein.

**4. Personnel Security.**

(a) **Employment Verification & Background Checks.**

(i) **Background Check**. Everbridge performs or has previously performed a rigorous background check on all Everbridge employees who have access to technology infrastructure or Client Data. We use an industry-leading third-party for these checks, which include Social Security Number Trace/Address Verification, Consumer Credit Report*, County Criminal, Federal District Criminal, Driving Record*, Education Verification*, Employment Verification, Nationwide Criminal Search with Alias, Nationwide Registered Sex Offender Search, Office of Foreign Assets Control (OFAC) Check.

(ii) **E-verify**. Everbridge also participates in the E-verify program to confirm all company employees are authorized to work in the United States, and all personnel must review and sign its employment and confidentiality agreements prior to starting work.

*Specific background element conducted based on position and position requirements.

(b) **Security Awareness & Privacy Training**. Everbridge's annual security awareness and privacy training is mandatory for all Everbridge personnel. The level of training is based on job role and responsibilities, is tracked for completion by its Security and its Human Resource Teams.

## 5. Platform & Technical Support.

5.1 **Dedicated Network Operations Center (NOC) Team**.

(a) To monitor the solution in real-time and ensure delivery of its services, Everbridge employs a dedicated operations team that manages its 24x7x365 Network Operations Centers (NOCs) from geographically separate Everbridge office locations: Pasadena, CA and Burlington, MA.

(b) In the event an anomaly is detected by one of its monitoring solutions, immediate text alerts are issued to responsible NOC personnel for investigation and remediation (if needed).

5.2 **Client Technical Support**

(a) Clients are able to interface with highly trained Technical Support Team to submit a new support case, manage an existing support case, search its knowledge base articles, and access Everbridge University for on-demand training and certifications.

(b) Everbridge's team is available 24x7x365 (via telephone, email, and through its Support Center online) in accordance with its most recently published Support Services Guide.

5.3 **Live Operator Service**

(a) A top-priority phone queue to the Emergency Live Operator service is provided to help the client send emergency notifications if the Client cannot access the Everbridge interface directly, and emergency live operator messages are available per year without any additional cost.

(b) User authentication using its Live Operator service is conducted through the Users' defined security challenge question and associated response. Once authenticated successfully, the Everbridge Live Operator will immediately be able to assist the Client caller with their request.

5.4 **Service Advisories.** Everbridge communicates maintenance activities, service impacting events, and system status alerts via Service Advisories posted on the Everbridge Support Center and emailed to client defined personnel. Service advisories are available for thirty (30) days beyond the conclusion of the maintenance or event.

## 6. Encryption.

6.1 Everbridge's implemented encryption technologies align to FIPS 140-2, NIST 800-53 controls, and FedRAMP compliance. HTTPS TLS 1.2 and SFTP using SSH are used for secure communication with the platform.

6.2 Client Data is encrypted at rest using AES 256-Bit encryption. All encryption keys are managed internally by Everbridge using a digital key management solution.

**7. Access Control Policy**. Everbridge's access control Policy is governed by the NIST 800-37/53, Controls for Moderate Risk systems, AC-1 through AC-25 and we maintain controls for two main access types (defined below).

## 8. Everbridge Corporate Policies

8.1 **Access Policy**. When privileges are assigned for Everbridge personnel, the "least privilege" model is used and privileges are assigned based solely on job function. Access requests include a formal request from Human Resources, review, and a management approval process. All granted access for any Everbridge employee is fully logged, tracked, and reviewed quarterly. Access to any production systems requires a need from a job responsibility perspective and requires Executive Management approval. Any change in job status or responsibility also triggers immediate access controls reviews. Access requires the use of multi-factor authentication (username, complex alpha-numeric password, multi-factor authentication numeric PIN).

8.2 **Production Platform Policy**. During the initial implementation, the Everbridge implementation specialist will work with the client to define and assign the appropriate initial administrators and security roles for use with the Everbridge system. However, long term, client administrators are responsible for provisioning access and assigning security roles for their administrators or users.

## 9. Authentication.

9.1 **Everbridge Corporate Policy**.

(a) Everbridge leverages Single Sign On throughout its organization.

(b) All Everbridge personnel are required to login with:

(i) a unique and valid username,

(ii) complex alpha-numeric password, and

(iii) a multi-factor authentication PIN for access to any Everbridge corporate computing asset.

(c) **Passwords**

(i) must be a minimum of 12 characters in length, use a minimum of 3 different character categories, (alpha (lower caps, upper caps), numbers, and special characters);

(ii) must be changed every 90 days, and

(iii) personnel may not leverage their last 24 passwords.

(iv) After 5 unsuccessful login attempts, accounts are locked out until unlocked by an authorized administrator.

9.2 **Production Platform Policy.**

(a) Everbridge, by default, requires all users to login using a valid unique username and complex alpha-numeric password.

(b) Passwords must be:

(i) between 8 and 64 characters in length (Client configurable to require at least 12 characters), use a minimum of 3 different character categories (alpha (lower caps, upper caps), numbers, and special characters),

(ii) changed every 90 days (client configurable – 90 days; 180 days; 365 days; off), and

(iii) users may not leverage their last 3 passwords (client configurable to the last 24 passwords). After 5 unsuccessful login attempts (client configurable to 3 unsuccessful logins), accounts are locked out until unlocked by an authorized client administrator.

(c) Everbridge also offers clients the ability to use Single Sign On (SSO) functionality with a SAML 2.0 compliant authentication as an option. This allows clients to leverage their existing authentication solution to manage user accounts, password complexity, and expiration settings directly.

**10. Session Management.**

10.1 **Everbridge Corporate Policy**. Everbridge maintains a concurrent session restriction for its users accessing corporate computing resources and sessions expire after fifteen (15 minutes) of inactivity.

10.2 **Production Platform Policy**. For its client users accessing Everbridge's production platform, Everbridge maintains a concurrent session restriction for all users and session expiration timeframes are configurable by clients between fifteen (15) minutes and twelve (12) hours.

**11. Business Continuity & Disaster Recovery.**

11.1 Everbridge's Business Continuity – Disaster Recovery (BCDR) plan is tested once per year. Recovery efforts strive to resume all business activities as soon as possible and many recovery tasks will be conducted in tandem. However, in the event that prioritization is necessary, Everbridge has established a recovery order for all business areas of the company. Everbridge has recovery plans for different types of disruptions: natural disasters, accidents or failures, technical disasters, malicious activities and pandemics.

11.2 All support and technical operations are conducted from within the Everbridge corporate office locations in California and Massachusetts, United States, Colchester, United Kingdom and Bengaluru, India. Everbridge maintains up-to-date BCDR plans which include "rolling" support services throughout the globe should a catastrophic event strike one or more of its corporate office locations.

11.3 Everbridge employs multiple hosting facilities for all its test and production systems in a fully redundant, geographically dispersed configuration. Client Data is continuously replicated among sites, and each site can provide the full range of Everbridge services. If service is disrupted at any site, all traffic is dynamically rerouted to another site so that Everbridge's systems remain constantly available. Every system in the infrastructure is individually fault tolerant, with redundant power, network, and disc, wherever possible.

11.4 Should a catastrophic event occur, and the recovery of systems is required, the maximum:

(a) Recovery Time Objective (RTO) is 15 minutes (or less), and

(b) Recovery Point Objective is (RPO) is 24 hours (or less).

11.5 Everbridge is able to share its latest BCDR Plan Table of Contents and its latest Continuity Plan Test Results as secure documentation upon request.

**12. Redundancy & Backup.**

12.1 **System Redundancy**.

(a) Everbridge employs multiple hosting facilities for all of its test and production systems in a fully redundant, geographically dispersed configuration.

(b) Data is continuously replicated among the various sites, and each site can provide the full range of Everbridge services. If service is disrupted at any site, all traffic is dynamically rerouted to another site so that Everbridge's systems remain constantly available. This transition is invisible to the client, who experiences no downtime as a result. Every system and tier within the Everbridge infrastructure is individually fault tolerant, with redundant power, networking, and hardware, telephony, and data communication wherever possible.

12.2 **Platform Backup**.

(a) Non-disruptive backup services. Everbridge maintain a Storage Area Network (SAN) in each hosting facility which is utilized for backup purposes.

(b) Everbridge executes incremental backups daily and full platform backups are executed weekly. Backups are encrypted and available for one (1) year. In the event restoration is required, Everbridge is able to conduct a partial or full restore as needed. There are no backup requirements for our clients at any time and all backups are conducted and managed solely by Everbridge.

**13. Risk Management Framework.** Everbridge's Risk Management Framework is governed by NIST 800-53 and in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37. Risk management is handled by Everbridge's Security & Compliance Team internally, is reviewed and updated annually (unless otherwise required) and is approved by Executive Management.

**14. Incident Response.** Everbridge follows the Incident Response procedures outlined in NIST 800-61 and are included in NIST 800-53. Everbridge's compliance to NIST 800-53 is audited annually by a 3PAO as required. Everbridge is able to share its latest Incident Response plan as secure documentation for review upon request.

**15. Data Segregation**

15.1 Everbridge Platform is a fully hosted multi-tenant SaaS solution.

(a) Everbridge hosts multiple clients on a load-balanced farm of identical application instances.

(b) Each client's data is partitioned within the production database.

15.2 Data is logically segregated

(a) while the data for all clients resides in the same secured database, no client has access to another client's data.

15.3 To address the privacy and segregation of each Everbridge client's data, Everbridge employs a unique Account ID, ORG ID, and query validations for all operations to ensure one client does not gain access to another's data.

**16. Monitoring & Logging.**

16.1 Everbridge fully hosts and manages all aspects of the solution and we apply active monitoring against all processes within all tiers of its infrastructure from multiple monitoring points around the globe.

16.2 Logs are centrally stored, encrypted, and maintained for one year.

16.3 Everbridge's audit and logging procedures are governed by NIST 800-37/53, Controls for Moderate Risk systems, and details can be found in controls AU-1 through AU-16.

16.4 In the event an anomaly is detected, Everbridge's monitoring solutions issue immediate text alerts to 24x7x365 Everbridge NOC personnel for investigation and remediation (if needed).

**17. System Hardening.**

17.1 All Everbridge systems and infrastructure are "hardened" and extraneous or unneeded services, applications, and user accounts are removed or completely disabled.

17.2 Everbridge's firewalls are locked down to allow access only via HTTPS, SFTP (secure data transmission), SMTP (for mail) and DNS (Everbridge's name servers).

17.3 Traffic among the tiers of Everbridge's infrastructure is tightly controlled using ACLs and a series of VLANs. All other traffic/applications are prohibited.

**18. Intrusion Detection, Malware Protection, and Data Loss Prevention (DLP)**

18.1 Everbridge monitors all aspects of its platform and its corporate computing environments in real time.

18.2 Everbridge's secure web gateway employs URL filtering, malware detection, and application control technology to protect its enterprise and enforce internet policy compliance.

18.3 Everbridge systems are configured to use a proxy setting to allow inbound and outbound web traffic inspection by the web security appliance to ensure that security policies are being followed. The proxy system enforces URL, Webmail, Instant Messaging, Social Network/Blogs, Streaming Media/File Share, Business Usages/Productivity, and Enterprise Social/Collaboration policies.

18.4 All corporate computing systems leverage an anti-virus solution that continuously monitors and scans the system for malicious code, such as viruses, worms, etc.

18.5 Everbridge's production platform runs on highly customized Linux implementations which minimizes virus/malware threats since Linux does not run processes without having administrative approval.

18.6 The Everbridge Acceptable Use of Internet, Electronic Mail & Social Media Policy documents outline additional requirements and policy guidance that Everbridge follows to protect against malicious code attacks.

**19. Penetration Testing.** Everbridge conducts internal weekly scans against all systems, pre-release scanning against all code before use, and Everbridge engage with an industry-leading 3PAO for annual security vulnerability and penetration testing. All findings are documented and remediation plans developed and added to an ongoing Plan of Action and Milestones document (PoAM). Everbridge can share its latest Penetration Test Report as a secure document upon request.

**20. Vulnerability Management.**

20.1 Everbridge has implemented an Information Security Vulnerability Management Framework which is governed by NIST 800-53 controls to identify and manage vulnerabilities that may affect the confidentiality, integrity and availability of Everbridge Information and Information Systems. This Framework include the following key tenants:

(a) defined roles,

(b) responsibilities and implementation processes for vulnerability management;

(c) creation and maintenance of an asset inventory;

(d) process and security requirements for vulnerability monitoring,

(e) security patching timelines,

(f) vulnerability scanning,

(g) penetration testing,

(h) severity assessment,

(i) mitigation and remediation, and

(j) reporting and compliance.

20.2 Remediation of all vulnerabilities is conducted based on criticality, applicability, and endpoint;

20.3 Patches are evaluated against the industry standard CVSS scoring system;

20.4 Timelines for deployment of patches are:

(a) Seven (7) days for Critical,

(b) Thirty (30) days for High,

(c) Ninety (90) days for Medium; and

(d) One hundred and eighty (180) days for Low impact vulnerabilities.

**21. Threat Information Awareness.**

21.1 Everbridge leverages notification and threat intelligence services from U.S. CERT and applicable vendors to determine possible threats and vulnerabilities in the solution.

21.2 Everbridge's security staff is also member of InfraGard, a partnership between the FBI and members of the private sector.

**22. Endpoint Protection Policy**

22.1 Everbridge leverages systems management technologies for all corporate owned systems.

22.2 Everbridge's systems are built from a baseline approved configuration and only the required applications are installed to perform the assigned job duties.

22.3 All systems have:

(a) anti-virus software installed,

(b) configured for automatic daily checks (and updates) of new definitions, and

(c) tamper protection is enabled to prevent disabling the software.

22.4 Corporate users do not have administrative access and the use of peripheral devices (USB, CD/DVD media) is restricted and enforced through group policy.

**23. Vendor Management Policy**

23.1 Everbridge maintains a Vendor Management Policy within its Supply Chain Risk Management (SCRM) which is a part of its security risk management. This policy includes:

(a) procedures for entering into third party relationships,

(b) managing third party relationships,

(c) monitoring third party service levels,

(d) terminating third party relationships (if required), and

(e) coordinating information protection activities related to entering, managing, monitoring, and terminating third party relationships.

23.2 Everbridge's policies are and procedures are reviewed and updated annually.

23.3 At no time is any third party granted access to the Everbridge platform or the Client Data therein.

**24. Data Retention Policies.**

24.1 **Product system reporting data.** Product system reporting data is available for all client campaigns in the web-based console and product suite for 18 months. At any time, clients may download and archive reports available in Everbridge in various formats (HTML, CSV, PDF) and store these internally within their organization.

24.2 **Client Data**. Data that clients store for notification purposes within the Everbridge system is not purged or managed by Everbridge, in any way, throughout the life of an active services agreement. However, when an organization's contract expires, the organization's account will be deactivated and listed for deletion. Thirty (30) days from the contract expiration date, the organization's data will be flagged for purging and all of the organization's data will be removed from the active system. Everbridge retains the organization's data for one (1) month in the event the organization wishes to extend its subscription.

24.3 **Business records**. Business records are kept by Everbridge for seven (7) years and/or as required by law.

**25. Data and Media Sanitization & Destruction**. We contract with an industry-leading document and hardware destruction and sanitization organization. The company provides NAID Certified (National Association for Information) destruction services and specializes in the destruction of both paper documentation as well as various types of technical media (hard drives, CDs, DVDs, magnetic media, non-magnetic media, memory sticks, etc.) as per DoD 5220.22M. Everbridge is able to provide clients with a Certificate of Destruction upon request.

**26. Everbridge Mobile Apps** Everbridge's apps are developed internally, are natively designed for the operating systems to which they apply (iOS and Android), leverage secure transmission (HTTPS TLS 1.2), and secure storage (inherent device encryption). It is important to note that Client Data is not stored or processed in our mobile apps and our apps are included in our secure development, vulnerability management, and security vulnerability and penetration testing processes.