ABNORMAL SECURITY CORPORATION INFORMATION SECURITY POLICY

This Information Security Policy ("**Policy**") is incorporated into the subscription agreement under which Abnormal Security Corporation ("Abnormal", "we", or "us") provides its Service ("**Agreement**") to the Party listed as Customer on the Agreement ("**Customer**") and describes Abnormal's Information Security Program ("**Security Program**") which Abnormal has implemented and will maintain in accordance with this Policy.

Abnormal may update this Policy from time to time, provided that any such update does not: (i) modify any provision of the Agreement except for this Policy; or (ii) materially diminish the overall security protections described herein during the Subscription Term. Any such updates will be posted to https://legal.abnormalsecurity.com/. Capitalized terms not otherwise defined in this Policy shall have the meanings given to them in the Agreement. Any ambiguity, conflict or inconsistency between this Policy, the Agreement, the DPA, or other document comprising this Agreement shall be resolved according to the following order of precedence: (1) DPA; (2) this Policy; (3) the Agreement; and (4) other supplementary documents incorporated into the Agreement.

Minimum Security Standards. The Security Program will use industry-standard controls designed to protect the confidentiality, integrity, and availability of Customer Data against anticipated or actual threats or hazards; accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or damage. The Security Program will use administrative, technical, and physical safeguards appropriate to: (a) the size, scope, and type of Abnormal's business; (b) the type of information that Abnormal processes on behalf of Customer (where such information is provided to Abnormal in accordance with the Agreement); and (c) the corresponding need for security and confidentiality of such information.

For more details on Abnormal's Security Program, please see the Security Hub at security.abnormalsecurity.com ("**Security Hub**")*.*

Service Infrastructure. The Service and Customer Data are hosted on infrastructure using industry-leading cloud hosting providers. No Customer Data is stored or processed in Abnormal office facilities.

Elements of the Security Program.

1. **Policies and Procedures**. Abnormal has implemented and will maintain security, privacy, confidentiality, availability, and code of conduct policies and procedures designed to ensure that the Service and Abnormal's employees and contractors ("**Personnel**") process Customer Data in accordance with this Policy and the Agreement. Abnormal has implemented and will enforce disciplinary measures against Personnel for failure to abide by the aforementioned policies and procedures.

2. **Logical Access Controls**. Abnormal will take reasonable measures that are designed to ensure appropriate user authentication for Personnel with access to Customer Data, including without limitation, by assigning each Personnel unique authentication credentials for accessing any system on which Customer Data is processed and prohibiting Personnel from sharing their authentication credentials. Abnormal will restrict access to Customer Data solely to those Personnel who need access to Customer Data to perform Abnormal's obligations under the Agreement.

   Further, Abnormal will take reasonable measures to implement and maintain logging and monitoring technologies designed to help detect and prevent unauthorized access to its networks, servers, and applications, including but not limited to those that process Customer Data. Abnormal will conduct periodic reviews of systems that process Customer Data to verify the identities of individuals who access and have privileged access to systems to help detect and prevent unauthorized access to its network, servers, and applications and verify that all changes to its authentication systems were authorized and correct. Abnormal has implemented and will maintain procedures and policies that are designed to ensure that, upon termination of any Personnel the terminated user access to any Customer Data on Abnormal systems will be promptly revoked, and in all cases, revocation will occur no later than twenty-four (24) hours following such termination.

3. **Intrusion Prevention**. Abnormal utilizes reasonable measures designed to ensure that its infrastructure protections are consistent with industry standards in preventing unauthorized access to Abnormal networks, servers, and applications.

Such measures include but are not limited to the implementation of intrusion prevention technologies, anti-malware services, and firewall rules.

4. **Physical Access**. Abnormal limits physical access to its office facilities using physical controls (e.g., coded badge access). Abnormal regularly assesses the cloud hosting provider's ability to provide reasonable assurance that access to their data centers and other areas where Customer Data is stored is limited to authorized individuals. Cloud hosting provider data centers and Abnormal office facilities leverage camera or video surveillance systems at critical internal and external entry points and are monitored by security Personnel.

5. **Environmental Protection**. Abnormal regularly assesses the cloud hosting provider's ability to provide reasonable assurance that cloud hosting provider data centers implement and maintain appropriate and reasonable environmental controls for its data centers and other areas where Customer Data is stored, such as air temperature and humidity controls, and protections against power failures.

6. **Backup**, **Disaster Recovery, and Business Continuity**. Abnormal will: (a) back up its production file systems and databases according to a defined schedule and conduct regular testing of backups; and (b) maintain a disaster recovery plan for the production data center and maintain business continuity plans designed to manage and minimize the effects of disaster events or unplanned operational disruptions with a stated goal of resuming routine service within forty-eight (48) hours; and (c) conduct regular testing of the effectiveness of such plans.

7. **Security Incident Response**. For purposes of this Policy, any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data is a "**Security Incident**". Abnormal will: (a) take reasonable measures to implement and maintain logging and monitoring technologies designed to identify, alert, and analyze security events; and (b) maintain plans and procedures to be followed in the event of an actual or suspected Security Incident ("**Incident Response Plans**"). The Incident Response Plans require Abnormal to undertake a root cause analysis of any actual or suspected Security Incident and to document remediation measures.

8. **Security Incident Notification**. Abnormal will implement and follow procedures that are designed to detect and respond to Security Incidents and will notify Customer of any Security Incident affecting its Customer Data within forty-eight (48) hours of Abnormal becoming aware of the Security Incident, regardless of whether the Security Incident triggers any applicable breach notification law. Such notification will be executed using the contact information provided by Customer under the Records and Validation section of the Agreement.

   Notice to a Customer will include: (a) a description of the nature of the Security Incident, including the categories and approximate number of Customer's data subjects and personal data records concerned; (b) the name of Abnormal's contact where more information can be obtained; (c) a description of the likely consequences of the Security Incident; (d) a description of the measures taken or proposed to address or mitigate the adverse effects of the Security Incident, to the extent within Abnormal's reasonable control.

9. **Storage and Transmission Security**. Abnormal will logically segregate Customer Data from all other Abnormal or third-party data. Abnormal will: (a) securely store Customer Data; (b) encrypt Customer Data during transmission using, at a minimum, Transport Layer Security (TLS) protocol version 1.2 or above; and (c) encrypt Customer Data at rest using, at a minimum, the Advanced Encryption Standard (AES) 256-bit encryption protocol. Abnormal will establish encryption key management processes that are designed to ensure the secure generation, storage, distribution, and destruction of encryption keys. Abnormal will not store Customer Data on any removable storage devices or other similar portable electronic media.

10. **Data Retention and Secure Disposal.** Abnormal will retain and securely dispose of Customer Data in accordance with the Agreement. During the Subscription Term, Customer may through the features of the Service access, return to itself or delete Customer Data. Following termination or expiration of the Agreement, Abnormal will delete all Customer Data from Abnormal's systems. Deletion will be in accordance with industry-standard secure deletion practices. Abnormal will issue a certificate of deletion upon Customer's written request. Notwithstanding the foregoing, Abnormal may retain Customer Data: (a) as required by applicable laws, or (b) in accordance with its standard backup or record retention policies, as

governed by the Agreement.

11. **Risk Identification and Assessment.** Abnormal will implement and maintain a risk assessment program to help identify foreseeable internal and external risks to Abnormal's information resources and to Customer Data, and determine if existing controls, policies, and procedures are adequate.

12. **Subprocessors.** Abnormal will authorize third-party service providers to access or process Customer Data ("**Subprocessors**") only in accordance with the requirements and procedures specified in the Agreement, and specifically in the DPA. Prior to authorizing Subprocessors, Abnormal security Personnel will conduct a risk assessment of each Subprocessor to seek assurances of its data security practices (e.g., in the form of an independent third-party audit report such as the SOC 2 Type 2, ISO 27001, or a vendor security and risk evaluation). Abnormal enters into written agreements with its Subprocessors with security and data processing obligations substantially the same as those contained in this Policy.

13. **Change and Configuration Management.** Abnormal has implemented and will maintain processes for managing changes and updates to production systems, applications, and databases, including without limitation, processes for documenting, testing, and approval of changes into production, security patching, and authentication.

14. **Release Management.** Abnormal follows a continuous release process versus a standard release schedule and does not require a maintenance downtime window for the Service when pushing a new release. No Customer interaction is required to upgrade to the new version; the release is automatically applied to all Customers. Releases follow Abnormal's change management procedures that are designed to ensure that releases are tested and approved prior to push to production. Abnormal communicates release information using the notification functionality within the Service.

15. **Training.** Abnormal will undertake the following measures that are designed to ensure that Personnel who will have access to Customer Data are appropriately qualified and trained to handle Customer Data:

    15.1. Information Security and Privacy Awareness Training. Upon hire and at minimum annually thereafter, Abnormal will require security and privacy awareness training to all Personnel who will process or have access to Customer Data. Abnormal security and privacy awareness training is designed to meet industry standards and will include, at a minimum, education on safeguarding against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, and social engineering mechanisms.

    15.2. Secure Code Training. Abnormal will require annual training on secure coding principles and their application at minimum annually to all Personnel who develop or handle any Abnormal source code. Abnormal secure code training will cover topics such as: (a) the Open Web Application Security Project list of the 10 most critical security risks to web-based applications (OWASP Top 10); and (b) appropriate techniques for the remediation of the listed security vulnerabilities.

16. **Background Checks**. Abnormal Personnel will undergo a civil and criminal background check, to the extent permitted by applicable law.

17. **Audit and Assessments.** Abnormal has implemented and will maintain a Compliance Audit Program including assessments performed by an independent third-party ("**Auditor**") and defined Customer audit rights in accordance with the Agreement.

    17.1 Independent Security Audit. Abnormal will engage an Auditor to certify compliance with the ISO 27001 standard, and conduct a SOC 2 Type 2 audit with a scoped audit period of a maximum 12 months to demonstrate its compliance with the security requirements of the Security Program. Abnormal's SOC 2 Type 2 audit covers the Trust Services Criteria of Security, Availability, Confidentiality, and Privacy. Abnormal will make available to Customer publicly available certificates and summary copies of its SOC 2 Type 2 audit report (each, an "**Audit Report**") on the Security Hub.

    17.2 Customer Audits. Abnormal will make available the information necessary to demonstrate its compliance with the Security Program to support Customer in obtaining the information necessary to complete Customer's audits, reviews, risk assessments, and security-related questions of Abnormal as Customer’s vendor. Please see the Security Hub for this information. For further details on Customer audit rights, please see your Data Processing Addendum (DPA).

17.3 Penetration Tests. At least once per twelve (12) month period, Abnormal will undertake a network penetration test by an independent third-party. Abnormal will make available to Customer an executive summary section of the penetration test report that pertains to the systems and operations that process, store, or transmit Customer Data. Abnormal will remediate all vulnerabilities that the penetration test identifies in accordance with the following remediation timelines:

Level	**Timeline**
Critical	15 days
High	30 days
Medium	60 days
Low	Reasonable timeframe based on nature and probability of exploitation

All information exchanged between the Parties in the course of the activities described in all Sections above are deemed to be Abnormal Confidential Information.