ABNORMAL SECURITY INFORMATION SECURITY POLICY

During the Term of the Agreement, Abnormal will maintain an Information Security Program ("**Security Program**") in accordance with the requirements of this Information Security Policy ("**Security Policy**"). Terms not otherwise defined herein have the same meanings as set forth in the written subscription agreement under which Abnormal provides its Service as entered into by and between Customer and Abnormal ("**Agreement**"). In the event of a conflict between the terms of this Security Policy and the terms of the Agreement, the terms of this Security Policy will apply.

Elements of the Security Program.

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; unauthorized or unlawful access, use, disclosure, alteration, or destruction; and accidental loss or destruction or damage. The Security Program will maintain administrative, technical, and physical safeguards appropriate to: (a) the size, scope and type of Abnormal business; (b) the type of information that Abnormal stores; and (c) the need for security and confidentiality of such information.

1. Security Policies and Procedures. Abnormal will maintain and implement security policies and procedures designed to ensure that the Service and its employees and contractors process Customer Data in accordance with this Security Policy. Abnormal will implement and enforce disciplinary measures against employees and contractors for failure to abide by its security policies and procedures.

2. Intrusion Prevention. Abnormal will take 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 stringent firewall rules.

3. Physical Access Controls. Abnormal will establish limits on physical access to its information systems and facilities using physical controls (e.g., coded badge access) that provide reasonable assurance that access to data centers and other areas where Customer Data is stored is limited to authorized individuals. Data centers leverage camera or video surveillance systems at critical internal and external entry points.

4. Logical Access Controls.

Abnormal will take reasonable measures that are designed to ensure appropriate user authentication for all employees or contractors with access to Customer Data, including without limitation, by assigning each employee or contractor unique authentication credentials for accessing any system on which Customer Data is accessed and prohibiting employees or contractors from sharing their authentication credentials. Abnormal will restrict access to Customer Data to those employees or contractors who need access to Customer Data to perform Abnormal obligations under the Agreement.

Abnormal will take reasonable measures to implement and maintain logging and monitoring technologies designed to help prevent unauthorized access to, and to detect unauthorized attempts to access, its networks, servers, and applications. 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 will have policies in place that are designed to ensure that, upon termination of any employee or contractor, the terminated employee's or contractor's 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.

5. Environmental Access Controls. If Abnormal supplies data center services, Abnormal will 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. Disaster Recovery and Backup Controls. If Abnormal supplies data center services, Abnormal will: (a) back up its production file systems and databases according to a defined schedule; and (b) maintain a formal disaster recovery plan for the production data

center and conduct regular testing of the effectiveness of such plan.

7. Business Continuity and Incident Response Plans. If Abnormal processes, stores, or transmits Customer Data, then Abnormal will take reasonable measures to maintain business continuity plans and incident response plans to manage and minimize the effects of unplanned operational disruptions (cyber, physical or natural) ("**Incident Response Plans**"). These plans will include procedures to be followed in the event of an actual or suspected Security Breach or business interruption and have a stated goal of resumption of routine service within 48 hours of such an incident. The Incident Response Plans will require Abnormal to undertake a root cause analysis of any actual or suspected Security Breach and to document remediation measures.

8. Security Breach Notification. Abnormal will notify Customer of any unauthorized access to Customer Data in accordance with the terms and conditions of the Agreement. In the event no such terms are specified in the Agreement, the following terms will apply:

Abnormal will notify Customer of any unauthorized, unlawful or accidental access to, or disclosure, transfer, destruction, loss or alteration of, Customer Data (each, a "**Security Breach**") within two business days of Abnormal's knowledge of the Security Breach, regardless of whether the Security Breach triggers any applicable breach notification law. Abnormal will notify Customer of a Security Breach by email to Abnormal's primary contact within the Customer organization.

Notice to Customer will include: (a) a description of the nature of the Security Breach, including the categories and approximate number of 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 Breach; (d) a description of the measures taken or proposed to address the Security Breach; and (e) a description of measures to mitigate the adverse effects of the Security Breach.

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.

10. Secure Disposal.

Upon expiration or termination of the Agreement, Abnormal will return or delete Customer Data in accordance with the Agreement. If deletion is required, Customer Data will be securely deleted in accordance with industry leading methods (e.g., NIST SP 800-88), except that Customer Data stored electronically in Abnormal backup or email systems may be deleted over time in accordance with Abnormal records management practices.

If Abnormal stores Customer Data in Abnormal cloud computing services, Abnormal will retain Customer Data stored in its cloud computing services for the duration of any active the Subscription Term or until the expiration or termination of this Agreement. During a Subscription Term, Customer may export Customer Data from the Service (or Abnormal will otherwise make the Customer Data available to Customer) as described in the Documentation.

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 determine if existing controls, policies, and procedures are adequate.

12. Subcontractors. Prior to engaging new third-party service providers or adding new technologies to its Service that will access or process Customer Data (collectively, for the purposes of this Security Policy, "**Subcontractors**"), Abnormal will conduct a risk assessment of each Subcontractor's data security practices. Abnormal enters into written agreements with its Subcontractors with security obligations substantially similar to those contained in this Security Policy. Abnormal will be responsible for the acts or omissions of Subcontractors under the Agreement. This paragraph does not limit Abnormal's obligations regarding Sub-processors as set out in the DPA.

13. Change and Configuration Management. Abnormal will implement and maintain policies and procedures 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. Training and Background Checks. Abnormal will undertake the following measures that are designed to ensure that personnel who will have access to Customer Data are appropriately qualified.

14.1. Background Checks. Employees and contractors of Abnormal who will have access to Customer Data or systems that process Customer Data will undergo a civil and criminal background check, where permitted by applicable law, prior to accessing Customer Data or systems. Upon written request, not more than once per 12-month period, Abnormal will certify its compliance to Customer with this Section.

14.2. Information Security Awareness Training. Abnormal will provide new hire security awareness training, and refresher security awareness training at least once a year thereafter, to all personnel who process or may have access to Customer Data. Abnormal will make available to Customer documentation to validate compliance with this security awareness training requirement for the current year. Abnormal security awareness training is designed to meet industry standards and will include, at a minimum, education on safeguarding against data loss, misuse or breach through physical, logical and social engineering mechanisms.

14.3. Secure Code Training. Abnormal will provide annual training on secure coding principles and their application (Secure Code Training) to all personnel who develop or handle any Abnormal source code. Abnormal training will cover topics such as: (a) the Open Web Application Security Project (OWASP) 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.

15. Security Program Proof of Compliance.

Third Party Standards and Assessments. During the Term of the Agreement and at Abnormal's expense, Abnormal will undertake the following third-party assessments of the networks, servers, applications and operations where Customer Data is processed, stored or transmitted.

15.1. Third-Party Security Audit.

Abnormal engages an industry-recognized third party auditor to conduct a SOC 2 Type 2 security audit on at least an annual basis in order to demonstrate its compliance with the security requirements of the Security Program.

The Abnormal's SOC 2 Type 2 audit covers the Trust Services Criteria of Security, Availability and Confidentiality developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

Abnormal will make available to Customer copies of Abnormal's current SOC 2 report annually upon written request.

Where Abnormal is not permitted to audit the data processing facilities of its Subcontractors that store or process Customer Data (e.g., cloud data centers), Abnormal will seek assurances from such Subcontractors (e.g., in the form of an independent third party audit report such as the SOC 2 Type 2, ISO 27001, and vendor security evaluations).

15.2. Penetration Tests.

If Abnormal processes, stores, or transmits Customer Data, then at least once every year, Abnormal will undertake a network penetration test by an independent third party. Abnormal will remediate all critical and high vulnerabilities that the penetration test identifies within 30 days of the date they were first identified and will remediate all identified medium level vulnerabilities within a reasonable time period.

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, which will be deemed Confidential Information under the Agreement.

15.3. Audit and Vendor Risk Assessment.

From time to time, during regular business hours and upon reasonable notice, Customer, its regulators and/or designated third-party auditor(s) (that are not considered competitors of Abnormal) may perform, and Abnormal will reasonably assist with, a Vendor Risk Assessment (VRA). The VRA shall consist of a review of Abnormal's security related documentation regarding its compliance with this

Security Policy. Upon review of such materials, if Customer cannot find the assurances it considers necessary by review of such security documentation, then Customer may submit reasonable requests for information security and audit questionnaires that are necessary to confirm Abnormals's compliance with this Security Policy, provided that Customer shall not exercise this right more than once per year, and Abnormal will make its security personnel available to answer such questions related to Abnormal's compliance with this Security Policy and applicable regulations and laws. All reasonable costs and expenses actually incurred of such an audit shall be borne by the Customer. For the avoidance of doubt, Abnormal will pay all costs and expenses incurred in connection with Abnormal's own regulatory compliance and financial reporting requirements. In the event of a Security Breach that requires reporting a supervisory authority or other governmental authority, Customer may conduct an audit or VRA on no less than three days' notice, at Abnormal's expense.

In addition to Customer's audit rights, Abnormal agrees to reasonably cooperate and respond to Customer's annual security questionnaires. Any information exchanged with the activities described in this Section is deemed to be Abnormal Confidential Information.

16. Disclosure by Law.

In the event Abnormal is required by law, regulation, or legal process to disclose any Customer Data, Abnormal will (a) give Customer, to the extent possible, reasonable advance notice prior to disclosure so Customer may contest the disclosure or seek a protective order, and (b) reasonably limit the disclosure to the minimum amount that is legally required to be disclosed.

17. Updates.

As Abnormal releases new products, services, functionality, and features, Abnormal may update this Security Policy to account for such products, services, functionality, and features.