CYBERWALL.AI - Cybersecurity policies

Security requirements that CYBERDEFENSE.AI will maintain as part of the Service

Effective May 9, 2022

This Information Security Addendum ("Addendum") outlines the security requirements that CYBERDEFENSE.AI will maintain as part of the Service ("Security Requirements") and is incorporated into the Enterprise Subscription Terms of Service ("Agreement") by and between CYBERDEFENSE.AI and Customer. Capitalized terms used in this Addendum without a definition will have the meanings given to them in the Agreement.

1. General

1.1 CYBERDEFENSE.AI will (i) implement and maintain a comprehensive written information security program; (ii) update and review such program, as necessary, on a regular basis or upon a material change in the provision of the Service; and (iii) ensure such program (x) complies with applicable Laws, and applicable industry standards (including ISO/IEC 27001:2013, PCI DSS, SOC 2 Type II), (y) includes appropriate administrative, logical, technical, and physical safeguards that comply with this Addendum, and (z) is reasonably designed to achieve the following objectives:

(A) to ensure the security, confidentiality, integrity, and availability of Customer Data;

(B) to protect against any threats or hazards to the security and integrity of Customer Data; and

(C) to prevent unauthorized or accidental access, acquisition, destruction, loss, deletion, disclosure, alteration, or use of Customer Data.

1.2 The provisions of this Addendum will control in the event of a conflict between the Agreement (including any other attachments, exhibits, or schedules thereto) and this Addendum.

2. Policies; Awareness and Training

2.1 CYBERDEFENSE.AI will review policies addressing information security on at least an annual basis including, but not limited to: access and authentication management, asset management, change management, encryption, security, and privacy incident response, software development life cycle, and third-party risk management policy.

2.2 CYBERDEFENSE.AI will provide security awareness training to CYBERDEFENSE.AI employees at the time of hire and annually thereafter. Training will be regularly updated to include applicable information on security topics, including responsibilities for protecting data and systems and emerging threats and trends.

3. Access Management and Identification; Authentication

3.1 CYBERDEFENSE.AI will permit only those CYBERDEFENSE.AI Employees and third parties who are authorized pursuant to the Agreement (collectively, "Authorized Users") to access Customer Data. Authorized CYBERDEFENSE.AI personnel and authorized third parties will use Customer Data Customer solely as permitted under the Agreement and this Addendum.

3.2 CYBERDEFENSE.AI will follow industry standards to authenticate and authorize users.

3.3 Authorized Users will not use shared or generic identification credentials to access Customer Data.

3.4 CYBERDEFENSE.AI will require Authorized Users to use two-factor authentication to access systems where Customer Data resides.

3.5 CYBERDEFENSE.AI will maintain a centralized repository of all identification credentials used to access CYBERDEFENSE.AI's network where Customer Data resides.

3.6 CYBERDEFENSE.AI will revoke access from Authorized Users who no longer require access to Customer Data.

3.7 CYBERDEFENSE.AI will periodically review and revoke access rights of Authorized Users, as needed.

3.8 Authentication to CYBERDEFENSE.AI's network resources, platforms, devices, servers, workstations, applications, and devices will not be allowed with default passwords.

3.9 CYBERDEFENSE.AI will ensure that external network connections to CYBERDEFENSE.AI's network are secure.

3.10 CYBERDEFENSE.AI will change default server passwords prior to placing the device or system into production.

3.11 Workstations that have been inactive for a period of time will be automatically locked.

4. Secure Data Handling

4.1 CYBERDEFENSE.AI will encrypt Customer Data at rest, in transit, and in use via AES minimum 128-bit encryption and 1024-bit cipher key length.

4.2 CYBERDEFENSE.AI will apply and maintain full disk encryption of any Customer Data at rest on all CYBERDEFENSE.AI's systems that access, transmit, or store Customer Data.

4.3 Symmetric encryption keys and asymmetric private keys will be encrypted in transit, and storage, protected from unauthorized access, and secured. Cryptographic key management and rotation procedures will be documented. Access to encryption keys will be restricted to key custodians. CYBERDEFENSE.AI will follow industry standards to generate, store, and manage cryptographic keys used to encrypt Customer Data.

4.4 CYBERDEFENSE.AI will maintain secure data disposal procedures, including but not limited to using secure erase commands, degaussing, and "crypto shredding" as appropriate and in accordance with industry standards.

4.5 Customer Data will be logically separated from that of other CYBERDEFENSE.AI customers.

5. Infrastructure & Network Security

5.1 CYBERDEFENSE.AI will install, configure, and maintain perimeter and network security controls to prevent unauthorized access to Customer Data.

5.2 CYBERDEFENSE.AI will continuously monitor, log, and relevant alert for security events, including attempted and successful access, unauthorized changes on endpoints, network devices, and server systems containing Customer Data and other

indicators of compromise. All logs will be protected from unauthorized access or modification.

5.3 CYBERDEFENSE.AI will implement and maintain security, and hardening standards for network devices, based on industry best practices.

5.4 CYBERDEFENSE.AI will follow documented change management procedures.

6. Application Security

CYBERDEFENSE.AI will follow secure software development life cycle secure coding practices, such as those developed by the Open Web Application Security Project (OWASP) Top 10 (found at https://www.owasp.org/), to ensure harmful code is not delivered and best practices are followed. Coding practices will include (i) separate development, test, and production environments; (ii) regular security code reviews; (iii) scanning of all CYBERDEFENSE.AI software and/or applications storing, processing, or transmitting Customer Data; and (iv) use of only non-production, obfuscated, or de-identified data used in non-production environments (e.g., development or test).

7. Risk Management; Third Party/CYBERDEFENSE.AI Assurances

7.1 CYBERDEFENSE.AI will maintain a third-party risk management program which includes (i) maintenance of information security agreements to ensure that CYBERDEFENSE.AI's third parties with access to Customer Data are bound to data security requirements at least as restrictive as those set forth in this Addendum; and (ii) monitoring, and auditing the compliance of third parties with access to Customer Data with the requirements set forth in this Addendum.

7.2 Risk management will include remediation by CYBERDEFENSE.AI of any identified findings commensurate with risk and evidence of completion.

7.3 CYBERDEFENSE.AI will maintain a risk assessment program, which defines roles and responsibilities for performing risk assessment and responding to results. CYBERDEFENSE.AI will perform regular risk assessments to verify the design of controls that protect business operations and information technology.

8. Vulnerability & Patch Management

8.1 CYBERDEFENSE.AI will perform routine network and application-level scans for vulnerabilities and remediate them according to industry standards (e.g., PCI DSS).

8.2 At least once every year, CYBERDEFENSE.AI will engage an independent third-party security firm to perform a network and web application penetration test. Upon request, CYBERDEFENSE.AI will provide a summary of the results of the penetration tests.

8.3 CYBERDEFENSE.AI will apply security patches and system updates to CYBERDEFENSE.AI-managed software and applications, appliances, and operating systems according to industry standards (e.g., PCI DSS).

9. Business Continuity & Disaster Recovery

CYBERDEFENSE.AI will maintain a documented and operational business continuity and disaster recovery ("BC&DR") program. CYBERDEFENSE.AI will exercise and update its BC&DR program plans at least annually.

10. Security Breach Notification

10.1 CYBERDEFENSE.AI will maintain and annually update a documented data breach action and response plan.

10.2 If CYBERDEFENSE.AI discovers or is notified of a breach of security, which results in unauthorized access, acquisition, disclosure, or use relating to any Customer Data or Customer Systems or any violation of these Security Requirements ("Data Breach"), CYBERDEFENSE.AI will promptly at its expense: (i) notify Customer of the Data Breach without undue delay; (ii) investigate the Data Breach; (iii) mitigate the effects of the Data Breach;, and (iv) perform post-incident assessments, and report on the results of such assessment(s) to Customer.

11. Reporting & Audit

11.1 At least annually, CYBERDEFENSE.AI will engage with an independent assessor to (i) conduct a compliance assessment and provide a full attestation, review, or report under (A) Service Organization Control (SOC 2 Type II) or (B) other similar industry-recognized independent compliance assessment.

11.2 Upon request, CYBERDEFENSE.AI will provide a copy of the most recent SOC 2 Type II report.

11.3 CYBERDEFENSE.AI will cooperate with Customer in any reasonable investigations of possible fraudulent or unauthorized use of or access to Customer Data by CYBERDEFENSE.AI's employees or third parties. CYBERDEFENSE.AI agrees

to discuss applicable findings and any associated remediation plans with the Customer.

END