Virtana Security Policy

Virtana and Customer agree that this Security Policy is hereby incorporated into and made a part of their written agreement that references this policy (the “**Agreement**”) and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement, as applicable. In the event of any conflict between the terms of the Agreement and this Security Policy, this Security Policy shall govern.

Virtana utilizes infrastructure-as-a-service cloud providers as further described in the Agreement and/or Documentation (each, a "**Cloud Provider**") and provides the Service to Customer from a VPC/VNET hosted by the applicable Cloud Provider (the “**Cloud Environment**").

Virtana maintains a comprehensive documented security program based on NIST 800-53 (or industry recognized successor framework), under which Virtana implements and maintains physical, administrative, and technical safeguards designed to protect the confidentiality, integrity, availability, and security of the Service and Customer Data (the “**Security Program**”), including, but not limited to, as set forth below. Virtana regularly tests and evaluates its Security Program, and may review and update its Security Program as well as this Security Policy, provided, however, that such updates shall be designed to enhance and not materially diminish the Security Program.

1. Virtana's Audits & Certifications

1.1. The information security management system supporting the Service shall be assessed by one or more independent third-party auditors in accordance with standard audits and certifications ("**Third-Party Audits**"), which may include, if and when completed by Virtana (currently targeted for Q1 2022):

- SOC 2 Type II

1.2. Third-Party Audits are made available to Customer as described in Section 7.2.1.

1.3. To the extent Virtana discontinues a Third-Party Audit, Virtana will adopt or maintain an equivalent, industry-recognized framework.

2. Hosting Location of Customer Data

2.1. Hosting Location. The hosting location of Customer Data is the United States only.

3. Encryption

3.1. Encryption of Customer Data. Virtana encrypts back ups of Customer Data and leverages Transport Layer Security (TLS) 1.2 (or better) for Customer Data in-transit over untrusted networks.

3.2. Encryption Key Management. Virtana leverages AWS’ encryption key management system, which conforms to NIST 800-53 and involves annual rotation of encryption keys. Virtana logically separates encryption keys from Customer Data.

4. System & Network Security

4.1. Access Controls. All Virtana personnel access to the Cloud Environment is via a unique user ID and fully controlled access consistent with the principle of least privilege. All such access requires a VPN, with multi-factor authentication and passwords meeting or exceeding AWS’ policies pertaining to length and complexity requirements.

4.2. Endpoint Controls. For access to the Cloud Environment, Virtana personnel use Virtana-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) endpoint detection and response (EDR) tools to monitor and alert for suspicious activities and Malicious Code (as defined below), and (iii) vulnerability management in accordance with Section 4.7.3 (Vulnerability Management).

4.3. Separation of Environments. Virtana logically separates production environments from development and testing environments. The Cloud Environment is both logically and physically separate from Virtana's corporate offices and networks.

4.4. Firewalls / Security Groups. Virtana shall protect the Cloud Environment using industry standard firewall or security groups technology with deny-all default policies (except required ports) to prevent egress and ingress network traffic protocols other than those that are business-required.

4.5. Hardening. The Cloud Environment shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching as described in this Security Policy.

4.6. Monitoring & Logging.

4.6.1. Infrastructure Logs. Monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment. These logs are further monitored, analyzed for anomalies, and are securely stored to prevent tampering for at least one year.

4.6.2. User Logs. As further described in the Documentation, Virtana also captures logs of certain activities and changes within the Account and, at Customer's request, makes some, but not all, of those logs available to Customer for Customer's preservation and analysis.

4.7. Vulnerability Detection & Management.

4.7.1. Anti-Virus & Vulnerability Detection. The Cloud Environment leverages advanced threat detection tools used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code (collectively, "**Malicious Code**"). Virtana does not monitor Customer Data for Malicious Code.

4.7.2. Penetration Testing & Vulnerability Detection. Virtana conducts penetration tests on an ongoing basis throughout the year. Additionally Virtana engages to have independent penetration testing done annually by a third party independent auditor. Virtana also runs regular vulnerability scans for the Cloud Environment using updated vulnerability databases.

4.7.3. Vulnerability Management. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Service. Upon becoming aware of such vulnerabilities, Virtana will use commercially reasonable efforts to address private and public (e.g., U.S.-Cert announced) critical and high vulnerabilities within 30 days, and medium vulnerabilities within 90 days. To assess whether a vulnerability is 'critical', 'high', or 'medium', Virtana leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-Cert rating.

4.7.4. Open Source Components.Virtana will use commercially-available software tools (such as BlackDuck or similar) to identify open-source components and its licenses used as part of application software and make a list of open source components available on request by customers.

5. Administrative Controls

5.1. Personnel Security. Virtana requires criminal background screening on its personnel as part of its hiring process, to the extent permitted by applicable law.

5.2. Personnel Training. Virtana maintains a documented security awareness and training program for its personnel, including, but not limited to, onboarding and on-going training.

5.3. Personnel Agreements. Virtana personnel are required to sign confidentiality agreements. Virtana employee personnel are also required to sign/acknowledge their obligation to comply with Virtana's internal information security policies, which includes acknowledging responsibility for reporting security incidents involving Customer Data.

5.4. Personnel Access Reviews & Separation. Virtana reviews the access privileges of its personnel to the Cloud Environment at least quarterly, and removes access on a timely basis for all separated personnel.

5.5. Virtana Risk Management & Threat Assessment. Virtana's security committee meets regularly to review reports and material changes in the threat environment, and to identify potential control deficiencies in order to make recommendations for new or improved controls and threat mitigation strategies.

5.6. External Threat Intelligence Monitoring. Virtana reviews external threat intelligence, including US-Cert vulnerability announcements and other trusted sources of vulnerability reports. U.S.-Cert announced vulnerabilities rated as critical or high are prioritized for remediation in accordance with Section 4.7.3 (Vulnerability Management).

5.7. Vendor Risk Management. Virtana enters into terms and conditions with entities that process Customer Data designed to adequately protect Customer Data using security measures that enable Virtana to meet Virtana's obligations in this Security Policy.

6. Incident Detection & Response

6.1. Security Incident Reporting. If Virtana becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data (a "**Security Incident**"), Virtana shall notify Customer without undue delay, and in any case, where feasible, notify Customer within 72 hours after becoming aware.[1]

6.2. Investigation. In the event of a Security Incident as described above, Virtana shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident. Any logs determined to be relevant to a Security Incident, shall be preserved for at least one year.

6.3. Communication and Cooperation. Virtana shall provide Customer timely information about the Security Incident to the extent known to Virtana, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Virtana to mitigate or contain the Security Incident, the status of Virtana's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because Virtana personnel do not have visibility to the content of Customer Data, it will be unlikely that Virtana can provide information as to the particular nature of the Customer Data, or where applicable, the identities, number, or categories of affected data subjects. Virtana's communications with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Virtana of any fault or liability with respect to the Security Incident.

7. Customer Rights & Shared Security Responsibilities

7.1. Customer Audit Rights.

7.1.1. Where the Auditor is a third-party (or Customer is using a third-party to conduct an approved Pen Test under Section 7.1), such third party may be required to execute a separate confidentiality agreement with Virtana prior to any audit, Pen Test, or review of Audit Reports, and Virtana may object in writing to such third party if in Virtana's reasonable opinion the third party is not suitably qualified or is a direct competitor of Virtana. Any such objection by Virtana will require Customer to appoint another third party or conduct such audit, Pen Test, or review itself. Expenses incurred by Customer or the third party in connection with such audit, Pen Test, or review, shall be borne exclusively by Customer or the third party.

7.2. Shared Security Responsibilities. Without diminishing Virtana's commitments in this Security Policy, Customer agrees:

7.2.1. Virtana does not assess the content of Customer Data to identify information subject to any specific legal, regulatory or other requirement and Customer is responsible for making appropriate use of the Service to ensure a level of security appropriate to the particular content of Customer Data, including, where appropriate, implementation of encryption functionality, such as the "tri-secret secure" feature (as described in the Documentation), and the pseudonymization of Customer Data;

7.2.2. to be responsible for managing and protecting its User roles and credentials, including but not limited to (i) requiring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) reporting to Virtana any suspicious activities in the Account or if a user credential has been compromised, (iii) appropriately configuring User and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Data, and (iv) maintaining appropriate password uniqueness, length, complexity, and expiration;

7.2.3. to appropriately manage and protect any Customer-managed encryption keys to ensure the integrity, availability, and confidentiality of the key and Customer Data encrypted with such key.

[1] For clarity, where Customer's Agreement refers to the defined term "Security Breach", such reference shall be interpreted to refer to Security Incident, as defined herein.