Cloud Services Security Program

Considering state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing Customer Data, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, ComputerTalk has implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk. ComputerTalk uses reasonable technical, organizational, and security measures designed to protect the Customer's personal data in possession of or otherwise processed by ComputerTalk against unauthorized access, alteration, disclosure, or destruction.

ComputerTalk has implemented and will maintain an information security program that follows generally accepted system security principles embodied in the PCI DSS and SOC 2 standards designed to protect the Customer Data as appropriate to the nature and scope of the ComputerTalk Cloud Services provided.

General Data Security Framework

a) Security Awareness and Training. ComputerTalk has developed and will maintain an information security and awareness program delivered to all employees at the time of hire and annually thereafter. The awareness program is delivered electronically and includes a testing aspect with minimum requirements to pass.

b) Policies and Procedures. ComputerTalk will maintain appropriate policies and procedures to support the information security program. Policies and procedures will be reviewed annually and updated as necessary.

c) Change Management. ComputerTalk will utilize a change management process based on industry standards to ensure that all changes to the Customer's environment are appropriately reviewed, tested, and approved.

d) Data Storage and Backup. ComputerTalk will create backups of critical Customer Data according to documented backup procedures. Backup data will not be stored on portable media. Customer Data stored on backup media will be protected from unauthorized access. Backup data for critical non-database production servers will be retained for approximately thirty (30) days. Backup data for critical production database servers and transactional data will be retained for a minimum of seven (7) days.

e) Anti-Virus and Anti-Malware Protection. ComputerTalk will utilize industry-standard anti-virus and anti-malware protection solutions to ensure that all servers in ComputerTalk's Cloud Service Environment are appropriately protected against malicious software such as trojan horses, viruses, and worms. ComputerTalk will use standard industry practice to ensure that the ComputerTalk Cloud Services as delivered to Customers do not include any program, routine, subroutine, or data (including malicious software or "malware," viruses, worms, and Trojan Horses) that are designed to disrupt the proper operation of the Services, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause the Customer Data or Services to be destroyed, damaged, or rendered inoperable. Customers acknowledge that the use of license keys will not breach this section.

f) Vulnerability and Patch Management. ComputerTalk will maintain a vulnerability management program based on industry-standard practices that routinely assess the Cloud Services Environment. Routine network and server scans will be scheduled and completed on at least a quarterly basis. The scan results will be analyzed to confirm identified vulnerabilities, and remediation will be scheduled within a timeframe commensurate with the relative risk. ComputerTalk will monitor various vulnerability advisory services to ensure that newly identified vulnerabilities are appropriately evaluated for possible impact on the Services. Critical and high-risk vulnerabilities will be promptly addressed following the patch management and change management processes.

g) Penetration Testing. ComputerTalk will perform internal, external, web application, and segmentation penetration tests on information assets and IT infrastructure at least annually and after any significant changes following applicable standards and regulatory requirements. Identified information risks and vulnerabilities will be appropriately addressed using risk management action plans to remediate such threats proactively.

h) Data Destruction. ComputerTalk will follow industry-standard processes for the secure destruction of Customer Data that becomes obsolete or is no longer required under the Agreement. Retired or decommissioned equipment that formerly held Customer Data and is scheduled for destruction will be securely destroyed using a qualified vendor who will provide a certificate of secure destruction.

Network Security

ComputerTalk will employ effective network security controls based on industry standards to ensure that Customer Data is segmented and isolated from other customer environments within the Cloud Services Environment. Controls include, but are not limited to:

a) Segregated Firewall Services. Customer environments are segmented using physical and contextual firewall instances. ComputerTalk employs advanced firewall technology with active threat detection to reduce the likelihood of a security threat impacting the Cloud Services Environment.

b) Intrusion Detection System. ComputerTalk has implemented intrusion detection systems across the ComputerTalk Cloud Service Environment.

c) No Wireless Networks. Wireless networks are not utilized within the Cloud Services Environment.

d) Data Connections between Customer and the ComputerTalk Cloud Service Environment. ComputerTalk uses SSL/TLS, VPN, and/or MPLS circuits to secure connections between browsers, client apps, and mobile apps to the ComputerTalk Cloud Service. Connections traversing an untrusted network (e.g., the Internet) will use SSL/TLS.

e) Data Connections between ComputerTalk Cloud Service Environment and Third Parties. Transmission or exchange of Customer Data with Customer and any third parties authorized by Customer to receive the Customer Data will be conducted using secure methods (e.g., SSL/TLS, HTTPS, SFTP).

f) Encrypted Recordings. ComputerTalk encrypts call recordings and chat sessions. The Customer is responsible for keeping sensitive data out of the recordings via the agent toolbar (iceBar), such as using the pause functionality.

g) Encryption Protection. ComputerTalk uses industry-standard methods to support encryption.

h) Logging and Monitoring. ComputerTalk will log security events from the operating perspective for all servers providing the ComputerTalk Cloud Service to Customers. ComputerTalk will monitor and investigate events that may indicate a security incident or problem. Event records will be retained for one year.

User Access Control

i) Access Control. ComputerTalk will implement appropriate access controls to ensure only authorized users have access to Customer Data within the ComputerTalk Cloud Service Environment.

j) Customer's User Access. The Customer is responsible for managing user access controls within the application. The Customer defines the usernames, roles, and password characteristics (length, complexity, and expiration timeframe) for its users. The Customer is entirely responsible for any failure by itself, its agents, contractors, or employees (including without limitation all its users) to maintain the security of all usernames, passwords, and other account information under its control. Except in a security lapse caused by ComputerTalk's gross negligence or willful action or inaction, the Customer is entirely responsible for all use of the ComputerTalk Cloud Service through its usernames and passwords, whether authorized by the Customer, and all charges resulting from such use. The Customer will immediately notify ComputerTalk if the Customer becomes aware of any unauthorized use of the ComputerTalk Cloud Service.

k) ComputerTalk User Access. ComputerTalk will create individual user accounts for each of its employees that have a business need to access Customer Data or Customer systems within the ComputerTalk Cloud Service Environment. The following guidelines will be followed regarding ComputerTalk user account management:

- User accounts are requested and authorized by ComputerTalk management.
- Strong password controls are systematically enforced.
- Connections are required to be made via secure industry-standard remote access technology using strong passwords that expire every ninety (90) days.
- Dormant or unused accounts are disabled after ninety (90) days of non-use.
- Session time-outs are systematically enforced.
- User accounts are promptly disabled upon employee termination or role transfer, eliminating a valid business need for access.

Business Continuity and Disaster Recovery

Disruption Protection. The ComputerTalk Cloud Service will be deployed and configured in a high-availability design. The Cloud Services environment is physically and logically separated from the ComputerTalk corporate network environment. A disruption event involving the corporate environment does not impact the availability of the ComputerTalk Cloud Service.

Business Continuity. ComputerTalk maintains a Business Continuity Management (BCM) process that identifies potential risks, threats, and vulnerabilities that could impact ComputerTalk's business operations. The overall objective is to ensure the business is more resilient to potential threats and enable the business to resume or continue operations under adverse or abnormal conditions.

Disaster Recovery. ComputerTalk offers various disaster recovery options to meet customer requirements. In general, most customers choose to run on a single data center high availability architecture. Off-site encrypted backup allows for rapid return to service in the same location or another ComputerTalk data center. Customer solutions that cannot tolerate any downtime are hosted out of physically diverse datacenters and are designed to run on one.

Security Incident Response

Security Incident Response Program. ComputerTalk will maintain a Security Incident response program based on industry standards designed to identify and respond to suspected and actual Security Incidents involving Customer Data. The program will be reviewed, tested, and, if necessary, updated on at least an annual basis. "Security Incident" means a confirmed event resulting in unauthorized use, deletion, modification, disclosure, or access to Customer Data.

Notification. In the event of a confirmed breach involving the unauthorized release or disclosure of Customer Data or other security event requiring notification under applicable law, ComputerTalk will notify the Customer within 72 hours and will reasonably cooperate so that Customer can make any required notifications relating to such event unless ComputerTalk is specifically requested by law enforcement or a court order not to do so.

Notification Details. ComputerTalk will provide the following details regarding the confirmed Security Incident to the Customer: (i) the date that the Security Incident was identified and confirmed; (ii) the nature and impact of the Security Incident; (iii) actions already taken by ComputerTalk; (iv) corrective measures to be taken; and (v) evaluation of alternatives and next steps.

Ongoing Communications. ComputerTalk will continue providing appropriate status reports to Customers regarding the resolution of the Security Incident and continually work in good faith to correct the Security Incident and prevent such Security Incidents in the future. ComputerTalk will cooperate, as reasonably requested by the Customer, to further investigate and resolve the Security Incident.

Cloud Services Environment Protection

Use of Colocation Datacenter Providers. ComputerTalk contracts with third-party providers for colocation space. Colocation providers and related services are reviewed annually to ensure that they continue to meet the needs of ComputerTalk and its Customers. Each colocation provider maintains certification based on their independent business models. Upon written request, security and compliance certifications and/or attestation reports for the colocation relevant to the Customer's Services will be provided. They may require additional non-disclosure agreements to be executed.

Physical Security. Each Cloud Services Environment is housed within a secure and hardened facility with the following minimum physical security requirements: (a) secured and monitored

points of entry; (b) surveillance cameras in the facility; (c) on-site access validation with identity check; (d) access only to persons on an access list approved by ComputerTalk; (e) on-site network operations center staffed 24x7x365.

Environmental Controls. Each Cloud Services Environment is equipped to provide redundant external electrical power sources, redundant uninterruptible power supplies, backup generator power, and redundant temperature and humidity controls.