Cloud Services Security Program

ComputerTalk's contact center cloud services for customers in the North American region are provided from wholly-owned data centers in colocation facilities in Toronto and Markham (Canada) and Chicago (United States). ComputerTalk maintains PCI DSS, SOC 2 Type 2, and ISO 27001:2013 (annual third-party) compliance for these data center locations, effectively minimizing the cybersecurity risks associated with cloud services. ComputerTalk works diligently to ensure we offer our customers a secure, resilient, and highly available cloud service for their business-critical operations.

General Data Security Framework

a) **Formal control framework:** To ensure that cybersecurity and data privacy risks are minimized, ComputerTalk has implemented a comprehensive security control program that includes formal policies, operational processes, risk management, and senior governance structures. Policies and procedures are available to all employees and are subject to annual review and third-party validation.

b) **Security awareness and training:** All ComputerTalk employees must complete information security and awareness training at the time of hire and annually after that. The program includes online cybersecurity training, a review of information security policies and operational process documentation, and a formal attestation of adherence. All employees involved with software development, including those engaged with quality assurance, receive secure coding training on an annual basis based upon the OWASP Top 10.

c) **Secure software development:** ComputerTalk ice platform development follows a secure software development lifecycle policy that includes third-party component vulnerability scanning, code reviews, and multi-stage OWASP Top 10 vulnerability testing. Web-facing applications developed for customer-specific business requirements are subject to a formalized security standard incorporating OWASP Top 10 scanning at the development stage and vulnerability scanning before production deployment.

d) **Separation of production, development, and corporate environments:** Production environments are logically separate from development and test environments and ComputerTalk's corporate network. Change approval must be obtained, and all test data must be removed before the software is promoted to production. Testing in production environments is limited to pre-production quality assurance validation, vulnerability scanning, and customer acceptance testing.

e) **Change management:** Before implementation, all hardware, software, or configuration changes to the cloud service production environment are subject to formal review and

authorization. Identification of risk factors, risk mitigation plans, consistency with established practice, security considerations, and testing methodology are central to the review/approval process.

f) **Data backup and restoration:** ComputerTalk uses a third-party service to perform backups that allow a data restoration point of less than 24 hours. Backup data is encrypted both in transit and at rest, and ComputerTalk regularly validates that the service fully maintains security certifications that meet our requirements. All customer data is encrypted, retained for 90 days, and backed up daily. Backup restoration integrity for critical data and servers is tested on a planned basis throughout the year.

g) **Security threat mitigation:** A formal vulnerability management program, automated patching tools, and formal operational practices are used to ensure timely security updates and rapid response to new critical and high security vulnerabilities. Routine internal and external vulnerability scans are executed on at least a quarterly basis and following significant changes to the environment. Scan results are analyzed to identify critical and high vulnerabilities, allowing for timely remediation. In addition, ComputerTalk monitors various industry advisory services to proactively identify new and emerging vulnerabilities and threats that, combined with vulnerability scanning, allow for comprehensive risk-based planning decisions. New critical and high vulnerabilities are promptly targeted for remediation consistent with established vulnerability and patch management procedures with the objective of remediation wherever feasible within 30 days of identification.

h) **Third-party penetration testing:** Third-party penetration tests are performed on information assets and IT infrastructure at least annually, including internal, external, web application, and segmentation tests. Remediation of critical and high vulnerabilities is validated as a requirement of our third-party security controls certification program.

i) **Data destruction:** ComputerTalk follows formal processes to ensure the secure destruction of customer data (a) that is aged beyond scheduled retention periods, (b) within 30 days following service termination, or (c) otherwise at the direction of the customer. ComputerTalk uses a qualified vendor for the secure destruction of retired or decommissioned equipment used for data storage.

Network Security

ComputerTalk employs comprehensive network controls to protect customer data from internal and external threats. Controls include, but are not limited to:

a) **Segmented firewall-protected architecture:** Web-facing infrastructure elements are situated on a separate subnet (DMZ) behind web application firewalls that provide active threat detection. Firewalls handling internal network traffic to and from the DMZ are fully hardened, limiting connections to documented, secure, trusted endpoints.

b) **Remote access:** Access to the ComputerTalk cloud environment is limited to authorized staff using remote access technology, including audit trail logging. Any unusual access patterns trigger alerts for senior technical investigation.

c) **Antivirus and antimalware protection:** ComputerTalk deploys advanced antivirus tools with file integrity monitoring to ensure that the services are protected from any malware threats that could disrupt the proper operation of the services or may cause the customer data or services to be breached, damaged, or rendered inoperable.

d) **Infrastructure hardening:** ComputerTalk uses configuration guides and group policies to ensure that all infrastructure components are hardened effectively and consistently, that services not required are disabled, and that data encryption is limited to trusted and secure protocols.

e) **Intrusion detection system:** ComputerTalk has implemented intrusion detection systems across the Cloud Services Environment. Wireless access is not permitted. Real-time scanning and alerting are deployed to identify any rogue wireless connection attempts.

f) **Data in transit encryption:** Data traffic within ComputerTalk's Cloud Services Environment and transmission or exchange of data with the customer and any third parties, as authorized by the customer, use secure encryption methods (e.g., SSL/TLS, HTTPS, SFTP).

g) **Data at rest encryption:** Customer data at rest is encrypted. Customers are responsible for keeping sensitive data out of audio recordings via the agent toolbar (iceBar) using the pause functionality.

h) **Logging, monitoring, and alerting:** Internal platform monitoring and alerting are performed continuously to detect system health and performance issues, component failure, and potential security-related issues early. A security incident event manager (SIEM) analyzes and correlates every login, logoff, file access, database query, or potentially malicious event. Using an alert management framework, we ensure that the response to an alert matches the degree of alert urgency.

User Access Control

a) **Access control:** ComputerTalk has implemented appropriate access controls to ensure only authorized users can access customer data within the ComputerTalk Cloud Services Environment.

b) **Customer's user access:** The customer manages user access controls within the application. The customer defines its users' roles and password characteristics (length, complexity, and expiration timeframe). 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 for a security lapse resulting from ComputerTalk's gross negligence, willful action, or inaction, the customer is entirely responsible for all

use of the service by managing usernames and passwords
and any impacts resulting from such use. The customer is to immediately notify ComputerTalk if they become aware of any unauthorized use of the services.

c) **ComputerTalk privileged access:** ComputerTalk creates role-based privileged accounts for employees who have a business need to access the ComputerTalk Cloud Services Environment. The following guidelines are followed regarding ComputerTalk user account management:
   i. User accounts are requested and authorized by ComputerTalk management.
   ii. Strong password controls are systematically enforced.
   iii. Connections are made via secure remote access technology using strong passwords that expire every 90 days.
   iv. Dormant or unused accounts are disabled after 90 days of non-use.
   v. Session time-outs are systematically enforced.
   vi. User accounts are promptly disabled upon employee termination or role transfer, eliminating a valid business need for access.

Business Continuity and Disaster Recovery

a) **Disruption protection:** The ComputerTalk cloud service platform is configured using a high-availability architecture and is logically separate from the ComputerTalk corporate network environment. Should a security event disrupt an aspect of the corporate environment, there would be no impact on the security or availability of the cloud service.
b) **Business continuity:** ComputerTalk maintains and tests on an annual basis a business continuity management (BCM) process that identifies potential risks, threats, and vulnerabilities that could impact ComputerTalk's business operations. The objective is to ensure the business is resilient to potential threats and enable the business to resume or continue operations under adverse or abnormal conditions quickly.
c) **Disaster recovery:** ComputerTalk offers various disaster recovery options to meet customer requirements. Customers generally choose a single data center option with our standard high-availability architecture. Off-site encrypted backup allows for rapid return to service with a restoration objective of fewer than 24 hours. Customer solutions that cannot tolerate downtime can be hosted out of physically diverse data centers and designed to run on one.

Security Incident Response

a) **Security incident response program:** ComputerTalk maintains a security incident response program designed to identify and respond to suspected and actual security incidents involving customer data. The program is reviewed, tested, and 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.
b) **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 the customer can make any required notifications relating to such an event unless ComputerTalk is specifically requested by law enforcement or a court order not to do so.

c) **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.

d) **Ongoing communications:** ComputerTalk will continue providing appropriate status reports to customers regarding security incident resolution and continually work in good faith to correct and prevent such incidents in the future. ComputerTalk will cooperate, as reasonably requested by the customer, to investigate and resolve the security incident.

Third-Party Service Providers

a) **Third-party security validation:** ComputerTalk contracts with selected third-party providers for colocation data center space, data backup services, and certain third-party cloud services with whom, under the direction of the customer, customer data is shared as a core requirement of the service offered by the third party. ComputerTalk ensures that each third-party provider has security certifications that meet security control requirements. ComputerTalk performs an annual review of each service partner to ensure that they continue to meet the security needs of ComputerTalk and its customers. All third parties requiring access to ComputerTalk's information systems, whether suppliers, customers, or otherwise, must be apprised and agree to follow ComputerTalk's *Cloud Services Information Security Policies – Third-Party Summary*. Any third party will receive a summary of the *Cloud Services Information Security Policies – Third Party Summary*. That party must confirm in writing that they have reviewed the policy and agree to abide by it before ComputerTalk proceeds with access provisioning.

b) **Data center physical security and resilience:** Each Cloud Services Environment is housed within a secure and hardened colocation data center facility that provides secured and monitored entry points, surveillance cameras, on-site access validation with identity checks, and access only to persons on an access list approved by ComputerTalk. Each facility that ComputerTalk uses has an on-site network operations center staffed 24x7x365 and is equipped to provide redundant external electrical power sources, redundant uninterruptible power supplies, backup generator power, and redundant temperature and humidity controls.