Cloud Services Security Program

ComputerTalk provides its contact center cloud services for North American customers from wholly owned data centers located in Toronto and Markham, Canada, and Chicago, United States. These facilities are hosted in colocation environments and maintained in accordance with ISO 27001:2022, PCI DSS, and SOC 2 Type 2 standards, helping to minimize cybersecurity and data privacy risks. ComputerTalk is committed to delivering a secure, resilient, and highly available cloud service to support customers' business-critical operations.

General Data Security Framework

Formal Control Framework: 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 staff and are subject to annual review and third-party validation.

Security Awareness and Training: All ComputerTalk staff 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 staff involved in software development receive secure coding training annually, based on the Open Worldwide Application Security Project (OWASP) Top 10.

Secure Software Development: ComputerTalk's ice platform development follows a *Secure Software Development Life Cycle Process* 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.

Separation of Production, Development, and Corporate Environments: Production environments are logically separate from development and test environments, as well as from 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.

Change Management: Before implementation, all hardware, software, or configuration changes to the Cloud Services 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 and approval process.

Data Backup and Restoration: ComputerTalk uses a third-party service to perform backups that provide a restore point within 24 hours. Backup data is encrypted both in transit and at rest, and ComputerTalk regularly validates that the service maintains the security certifications required by our standards. 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.

Security Threat Mitigation: ComputerTalk maintains a formal vulnerability management program, including automated patching tools and operational practices, to ensure timely security updates and rapid response to critical and high-priority vulnerabilities. Internal and external vulnerability scans are conducted at least quarterly and after significant changes, with results analyzed to prioritize remediation. Combined with monitoring of industry advisories, this approach enables proactive, risk-based planning. New critical and high vulnerabilities are addressed promptly, with remediation targeted within 30 days of identification, in accordance with established procedures.

Third-Party Penetration Testing: Third-party penetration tests are performed on information assets and information technology infrastructure at least annually, including internal, external, web application, and segmentation tests. Remediation of critical and high vulnerabilities is required for our third-party security controls certification program.

Data Destruction: ComputerTalk follows formal processes to ensure the secure destruction of customer data beyond scheduled retention periods, within 30 days of service termination, or at the customer's direction. ComputerTalk uses a qualified vendor for the secure destruction of retired or decommissioned data storage equipment.

Network Security

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

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.

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

Antivirus and Antimalware Protection: ComputerTalk deploys advanced antivirus tools with File Integrity Monitoring (FIM) to ensure services are protected against malware that could disrupt service operations or cause customer data or services to be breached, damaged, or rendered inoperable.

Infrastructure Hardening: ComputerTalk uses configuration guides and group policies to ensure that all infrastructure components are hardened consistently and effectively, that unnecessary services are disabled, and that data encryption is limited to trusted, secure protocols.

Intrusion Detection System (IDS): ComputerTalk has implemented IDSs across the Cloud Services Environment. Wireless access is not permitted. Real-time scanning and alerting are deployed to identify any rogue wireless connection attempts.

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, uses secure encryption methods (e.g., SSL/TLS, HTTPS, SFTP).

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

Logging, Monitoring, and Alerting: Internal platform monitoring and alerting are continuously performed to detect system health and performance issues, component failures, and potential security 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 the response to an alert matches its urgency.

User Access Control

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

Customer's User Access: The customer manages user access controls within the application. The customer defines the roles and password characteristics for its users (e.g., length, complexity, and expiration timeframe). The customer is entirely responsible for any failure by itself, its agents, contractors, or staff (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, including managing usernames and

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

ComputerTalk Privileged Access: ComputerTalk creates role-based privileged accounts for staff who have a business need to access the ComputerTalk Cloud Services Environment. The following guidelines are followed regarding ComputerTalk user account management:

a) User accounts are requested and authorized by the Security Governance Group.
b) Strong password controls are systematically enforced.
c) Connections are made via secure remote access technology using strong passwords that expire every 90 days.
d) Dormant or unused accounts are disabled after 90 days of non-use.
e) Session time-outs are systematically enforced.
f) User accounts are promptly disabled upon staff termination or role transfer, eliminating a valid business need for access.

Business Continuity and Disaster Recovery

Disruption Protection: The ComputerTalk cloud service platform is configured using a high-availability architecture and is logically separate from ComputerTalk's corporate network. 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.

Business Continuity: ComputerTalk maintains and tests, on an annual basis, a Business Continuity Management (BCM) process to identify 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 to enable it to resume or continue operations quickly under adverse or abnormal conditions.

Disaster Recovery: ComputerTalk offers a range of options to meet customer requirements. Customers generally choose a single data center option with our standard high-availability architecture. Off-site encrypted backup enables rapid return to service, with a restoration objective of fewer than 24 hours. Customer solutions that cannot tolerate downtime can be hosted in physically diverse data centers and designed to run on one.

Security Incident Response

Security Incident Response Program: ComputerTalk maintains a program to identify and respond to suspected and actual security incidents involving customer data. The program is reviewed, tested, and updated at least annually. A security incident is 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 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.

Notification Details: ComputerTalk will provide the following details regarding the confirmed security incident to the customer: the date the security incident was identified and confirmed; the nature and impact of the security incident; actions already taken by ComputerTalk; corrective measures to be taken; and an evaluation of alternatives and next steps.

Ongoing Communications: ComputerTalk will continue to provide appropriate status reports to customers regarding security incident resolution and will continually work in good faith to prevent and correct such incidents in the future. ComputerTalk will, upon a reasonable customer request, cooperate to investigate and resolve the security incident.

Third-Party Service Providers

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 third-party services. ComputerTalk ensures that each third-party provider holds security certifications that meet the required security controls. ComputerTalk performs an annual review of each service provider 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, including suppliers, customers, or otherwise, must be apprised and agree to follow ComputerTalk's *Cloud Services Information Security Policies – Third-Party Summary*. Each third party will receive a copy of the summary and must confirm in writing that they have reviewed the policy and agree to abide by it before access is provisioned.

Data Center Physical Security and Resilience: Each Cloud Services Environment is housed within a secure, hardened colocation data center facility that provides secure, 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 24/7/365 and is equipped to provide redundant external electrical power sources, redundant uninterruptible power supplies, backup generator power, and redundant temperature and humidity controls.