Microsoft Azure Deployment Security Program

Regionally deployed ice platforms leverage Microsoft's industry-leading security controls within the Microsoft Azure public cloud. By combining these controls with carefully selected security technologies and ComputerTalk's operational security framework, the Microsoft Azure ice platform provides robust protection for customer data against unauthorized access, modification, disclosure, or destruction.

ComputerTalk's information security program is grounded in recognized industry security frameworks. While the Microsoft Azure ice platform benefits from comprehensive cybersecurity controls based on standard deployment practices and risk considerations, it is not currently included in ComputerTalk's formal third-party validation program.

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.

150 Commerce Valley Drive West,
Suite 800,
Markham, Ontario, Canada, L3T 7Z3

1-800-410-1051 1-905-882-5000
1-905-882-5501
www.computer-talk.com

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 Storage and Backup: Unless otherwise directed by the customer, all customer data, including backups, is stored within the designated local Microsoft Azure instance. Backup data for critical non-database production servers is retained for approximately 30 calendar days. Backup data for critical production database servers, including transactional data, is retained for a minimum of seven (7) days. By default, audio recordings are not included in backup processes.

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. 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.

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.

Network Security

ComputerTalk implements robust network security controls to ensure that customer data is protected, segmented, and isolated from other customer environments within the Cloud Services Environment. These controls include, but are not limited to:

Firewall Configuration: ComputerTalk uses web application firewalls with active threat detection to mitigate the risk of security threats affecting services. Firewalls are hardened and configured to permit connections only to trusted and secure endpoints.

Antivirus and Antimalware Protection: ComputerTalk deploys advanced antivirus and antimalware solutions to protect the services from malicious programs, including viruses, worms, and Trojan horses. These controls are designed to prevent unauthorized access, service disruptions, and the compromise, damage, or loss of customer data.

Infrastructure Hardening: ComputerTalk uses group policies to ensure all infrastructure components are consistently and effectively hardened.

Data Connections Between the Customer and Services: ComputerTalk uses industry-standard encryption protocols (SSL/TLS) to secure data in transit between the ice platform and customer interfaces, including browsers, client applications, and mobile applications. All connections

traversing untrusted networks (e.g., the Internet) are encrypted using SSL/TLS to protect the confidentiality and integrity of data.

Data at Rest Encryption: ComputerTalk leverages Microsoft Azure-native encryption technologies to protect customer data at rest. Customers are responsible for ensuring that sensitive information is not captured in call recordings, including by using available controls in the agent toolbar (iceBar), such as pause and resume.

Real-Time Monitoring: ComputerTalk implements continuous threat detection and platform performance monitoring to identify, alert on, and investigate events that may indicate potential security incidents or service availability issues.

User Access Control

Access Control: ComputerTalk uses appropriate access controls to ensure only authorized users can access the ice platform and customer data.

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 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 User Access: ComputerTalk creates individual user accounts for each of its staff who have a business need to access customer data or customer systems within the ComputerTalk Cloud Services Environment. The following guidelines are followed regarding ComputerTalk user account management:

a) User accounts are requested and authorized by ComputerTalk management.
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.

Security Incident Response

Security Incident Response Program: ComputerTalk maintains a program aligned with industry standards to identify and respond to suspected and confirmed 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.