ice Azure Platform Security Program

Regionally situated ice platforms leverage the industry-leading security controls of Microsoft's Azure public cloud. With the addition of carefully chosen security technologies and ComputerTalk's operational security control framework, the security program for ice platforms in Azure provides high protection for customer data against unauthorized access, alteration, disclosure, or destruction.

ComputerTalk's information security program is based upon principles established in leading industry security frameworks. Based upon standard deployment practices, risk considerations, and unfavourable cost factors, the Azure ice platform benefits from comprehensive cybersecurity controls but is not part of ComputerTalk's formal third-party validation program.

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 are required to complete information security and awareness training at the time of hire and annually thereafter. 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 on a pre-production basis.

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 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: All hardware, software, or configuration changes to the cloud service production environment are subject to formal review that ensures key risk factors, consistency with established practice, security considerations, and testing methodology are considered, addressed, and documented to the satisfaction of identified senior technical resources before approval and implementation.

f) Data storage and backup: Unless otherwise directed by the customer, all customer data, including backups, will remain within the local Azure instance. Backup data for critical non-database production servers will be retained for approximately 30 calendar days. Backup data for critical production database servers and transactional data will be retained for at least seven days. By default, audio recordings are not backed up.

g) Security threat mitigation: Formal operational practices and patching automation tools are used to ensure the timely application of security updates and proactively address critical and high-security vulnerabilities. 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) Data destruction: ComputerTalk follows formal processes for the secure destruction of customer data beyond scheduled retention intervals when the services are no longer being used or at the direction of the customer.

Network Security

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

a) Firewall configuration: ComputerTalk employs web application firewalls with active threat detection to reduce the likelihood of a security threat impacting the services. Firewalls are hardened only to permit connections to secure trusted endpoints.

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

c) Antivirus and antimalware protection: ComputerTalk deploys advanced antivirus tools to ensure that the services are protected from any program, routine, subroutine, or data (including malicious software or "malware," viruses, worms, and Trojan horses) 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) Data connections between the customer and services: ComputerTalk uses SSL/TLS to secure connections to the ice platform between browsers, client apps, and mobile apps. Connections traversing an untrusted network (e.g., the Internet) will use SSL/TLS.

e) Data at rest encryption: ComputerTalk uses Azure-native technologies to encrypt customer data. The customer is responsible for keeping sensitive data out of the recordings via the agent toolbar (iceBar), such as using the pause functionality.

f) Real-time monitoring: ComputerTalk deploys threat detection monitoring and ice platform performance monitoring to identify and investigate events that may indicate a security or service availability issue.

User Access Control

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

b) Customer's user access: The customer is responsible for managing user access controls within the application. The customer defines its users' usernames, 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 user access: ComputerTalk creates individual user accounts for each of its employees that 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:

- User accounts are requested and authorized by ComputerTalk management.
- Strong password controls are systematically enforced.
- Connections are made via secure remote access technology using strong passwords that expire every 90 days.
- Dormant or unused accounts are disabled after 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.

Security Incident Response

a) Security incident response program: ComputerTalk maintains 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 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 the 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 further investigate and resolve the security incident.