Privacy & Security Policy

Last Updated: December 22nd, 2023

At TeamsCX, safeguarding the integrity, confidentiality, and availability of our information and technology assets is of paramount importance. This Security Policy outlines our commitment to maintaining a secure and resilient environment, ensuring the protection of sensitive data, and fostering a culture of proactive security awareness throughout our organization.

By adhering to this policy, we demonstrate our dedication to mitigating risks, upholding compliance with industry standards, and continually enhancing our security measures to adapt to an ever-evolving threat landscape.

1. User Access and Authentication

User Roles and Permissions: Through the TeamsCX Portal, you can establish user roles and their corresponding access privileges within Teams CX Dashboards. Both the Authorized Customer Representative and Managing Partners have the capability to enter the Portal and configure dashboard accessibility.

Authentication: TeamsCX makes use of Microsoft Teams accounts for Dashboard and Portal access. MS Teams uses the following authentication protocols, depending on the status and location of the user. Modern Authentication (MA) is the Microsoft implementation of OAUTH 2.0 for client to server communication. It enables security features such as multifactor authentication and Conditional Access.

2. Data Protection and Privacy

ISO Certified: We take great pride in introducing our organization as a subsidiary of an ISO-certified parent company (ISO-27001). This esteemed certification underscores our unwavering commitment to maintaining the highest standards of quality, security, and operational excellence across all aspects of our business operations.

Data Handling: All customer data is handled with care by storing it in cloud servers in with at least the minimum-security industry standards.

Encryption: All data (in transit and at rest) is encrypted with the latest industry standards.

Compliance: We only work with tools and partners that have industry standard certifications in place.

Disaster recovery: We always make sure that there is a disaster recovery plan in place for the tool, and for data. This disaster recovery plan is tested multiple times per year and will only be used in case of a disaster.

Security scanning: We have multiple security scanning measures in place to ensure the tool is protected against the latest known vulnerabilities.

3. Communication and Collaboration

Secure Channels: For the utmost protection of sensitive information, it is strongly advised that all confidential communications, discussions, and data sharing transpire exclusively within private chats and secure channels provided by platforms like Microsoft Teams or the TeamsCX Portal. These avenues offer encryption and controlled access, bolstering the confidentiality of our discussions and safeguarding against unauthorized exposure. By adhering to this practice, we ensure that sensitive matters are handled with the highest level of security and discretion.

External Sharing: We uphold a strict policy of not sharing private information with any third parties, unless express and explicit consent has been obtained beforehand. This principle reflects our unwavering commitment to safeguarding the confidentiality and privacy of our stakeholders' personal and sensitive data. We adhere rigorously to this standard to ensure that information entrusted to us remains under controlled and protected conditions, bolstering the trust our partners and clients place in us.

File Sharing: File sharing within our organization is conducted in compliance with stringent security protocols. When sharing files, it is imperative to utilize approved platforms and mechanisms that ensure end-to-end encryption and controlled access. This practice guarantees that sensitive information remains shielded from unauthorized access and maintains the highest level of data integrity. By adhering to these file sharing guidelines, we collectively contribute to the preservation of our data's confidentiality and security.

4. App and Integration Management

Third-Party Apps: We advise users customers to follow the provided instructions and installation files via the Teams CX Portal and no other mediums to ensure the files/packages are not tampered with.

App Permissions. We advise customers to follow the installation guide when configuring app permissions and to avoid providing extended permissions when not necessary.

5. Reporting Security Incidents

Incident Reporting: Utilize the TeamsCX Portal to report any instances of security incidents, breaches, or suspicious activities. Our dedicated team will promptly conduct an investigation and reach out to you at the earliest convenience.

Inquires: If you have any additional inquiries related to security matters, please feel free to reach out to us at support@teamscx.com. Your proactive engagement assists us in ensuring the safety of our environment.

Contact Information: TeamsCX Official contact details as published on www.teamscx.com