2024/4/15

Information Security Policy

TDCC adopts information and communication security technologies to construct a comprehensive and effective information security protection mechanism, ensuring the confidentiality, integrity, and availability of information assets.

Scope and Statement

Information Security Policy applies to TDCC's operations, entrusted services, and other services involving personal data. To meet TDCC's goals of information security maintenance, we follow our information security policy, organization development needs and information asset risk considerations to establish a comprehensive, feasible, and effective information security management system.

Information Security Organization Structure

1. Information Security Governance Team and Cyber Defense Team of Digital Development & Information Security Department are designated special tasks to coordinate the implementation of information security rules and guidelines from an integrated perspective to manage information security risks, while all other departments conduct various information security operations to enhance TDCC's information security maintenance capabilities.
2. Senior Executive Vice President supervising information security operations is designated as the Chief Information Security Officer (CISO) of TDCC to oversee the development, implementation and enforcement of security policies.

Information Security Protection Mechanism

1. TDCC’s IT departments are in charge of maintaining the hardware, software, networks, and equipment involving information security of various information systems. Considering regulation requirements, regulators, stakeholders’ interests, external technological threats and the operational needs, we establish information protection, control measures, and monitoring mechanisms to conduct appropriate protection and monitoring

for TDCC's information systems and equipment to ensure uninterrupted operation.

2. TDCC has implemented an Information Security Management System (ISMS) and our control measures comply with the standards of certified ISO/IEC 27001:2022 and CNS 27001:2023.
3. TDCC has adopted the Taiwan Personal Information Protection and Administration System (TPIPAS) and recognized as the Data Privacy Protection Seal.

Business Continuity Operations

TDCC has a Business Continuity Plan (BCP) for disaster recovery management. According to the plan, human resources and other resources needed for recovery are identified and classified by three levels, core business, important business, and general business, to ensure an adequate workforce and resources for disaster prevention, preparation and emergency response. It provides execution steps for timely and prioritized recovery. We also conduct testing and drills to confirm the adequacy and suitability of the Business Continuity Plan.

Response Protocol for Information Security Incident

1. TDCC monitors various information and alerts, analyzes whether they require tracking, and identify potential risks to develop response measures as early as possible and to reduce the possibility of information security incidents.
2. When an information security incident occurs, TDCC follows "Regulations on the Notification and Response of Cyber Security Incident" to promptly identify and report information security incidents, assess and manage impacts, and mitigate damages caused by the incident.

Cyber Security Reminders

1. Install antivirus software and set up firewalls on devices to prevent hacker intrusions, and regularly update antivirus software and virus definitions.
2. Do not click suspicious links or download unapproved programs on web pages or in the emails. Always be careful of the attachments sent via email or instant messaging.

3. Must download and install TDCC's ePASSBOOK App from App Store® or Google Play™.