02. Cybersecurity

Overview

With the rapidly evolving technological landscape and increasingly interdependent ecosystems, threats to cybersecurity have become a mainstream issue. Preserving the resilience and security of our network and systems is important to minimise the risk of service disruptions and data breaches resulting in reputational damage.

CelcomDigi's Information Security Policy sets out the principles and scopes of safeguarding the company's operations, assets, services, customers and information from current and future security risks and threats. Other referencing documents supporting the policy includes Information Security Manual, Identity and Access Management Manual, Business Continuity Management Manual, Telco Network Security Manual and Crisis Management Manual.

The Cyber Security Officer is responsible for ensuring the confidentiality, integrity, and availability of information and information processing facilities, including telecommunication systems and infrastructure, as well as protecting against cyberattacks, fraudulent activities, information loss, and other internal and external security risks and threats.

Our Response

- Stringent monitoring of the frequency of scams and fraud across all systems and processes
- Maintaining compliance with the ISO27001 standards on information security, including safe storage and management of information
- Strategic investment in modernised security controls and tools to strengthen cybersecurity infrastructure and mitigate any potential malicious cyberattacks
- Enhancing our data security management to limit access to and impose stringent controls on the collection of sensitive information

How do we ensure our network security controls?

The Telco Network Security Manual (TSNM) defines the network security controls for all network assets, including interfaces and interconnections. TSNM is based on the framework provided by ITU-T X.805, a telecom standard for end-to-end security of communication network. The manual further sets guidance for the following;

- Secure the end-to-end communications network for providing continued and secure network services;
- Identify the value of network assets and to understand the vulnerabilities and threats that may expose the network assets to risk, through periodic network risk assessment exercise;
- Establish a network security management system to proactively identify the emerging threats and vulnerabilities in the system and define mitigating measure to control the associated impact; and
- Ensure compliance with regulatory and contractual requirements for telecom network assets, operations, and services.