THE COMMUNITY
COLLECTIVE QLD

Information Security Policy

Purpose & Scope

Information security or infosec is concerned with protecting information from unauthorized access. The scope involves preventing or reducing the probability of unauthorized access, use, disclosure, disruption, deletion, corruption, modification, inspect, or recording.

This policy applies to all those engaging with The Community Collective QLD (TCCQ); including but not limited to; staff, contractors, and suppliers.

Policy Objective

TCCQ focuses on implementing information security to ensure we comply with our contractual obligations and maintain ethical standards with the data we process.

It is applicable to all those who deal with TCCQ or our clients' data. There are three objectives for the information security:

Confidentiality—prevents unauthorized users from accessing information to protect the privacy of information content. Confidentiality is maintained through access restrictions. Breaches of confidentiality can occur due to human error, intentional sharing, or malicious entry.

Integrity—ensures the authenticity and accuracy of information. Integrity is maintained by restricting permissions for editing or the ability to modify information. Loss of integrity can occur when information is not protected from environmental conditions, digital information is not transferred properly, or when users make unapproved changes.

Availability—ensures that authorized users can reliably access information. Availability is maintained through continuity of access procedures, backup or duplication of information, and maintenance of hardware and network connections. Loss of availability can occur when networks are attacked due to natural disasters, or when client devices fail.

Our commitment

Is to ensure that TCCQ:

- Implement and maintain an effective and auditable ISM
- Maintain appropriate systems to ensure integrity and protection against unauthorised alteration or destruction.
- Employees and users of TCCQ systems have timely and reliable access to information and services.
- Promote security of information and information systems.
- Communicate with all stakeholders on the importance of information security compliance with policy, processes, and procedures regarding information.
- Implement relevant controls for identified risks, threats, and vulnerabilities.
- Set a baseline for information security and continue to improve the management system.
- Comply with statutory, legislative and government direction regarding information security.
- Assure the Department and the community that information held with TCCQ is appropriately protected and handled.

The following principles underpin this policy statement:

- Compliance to the Departments ISM Statement of Applicability
- Alignment and compliance with requirements of ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems

Contractual & Legislative Requirements

- Information Access and Protection Standard
- Privacy and Personal Information Protection Act 1998
- Government Information (Public Access) Act 2009

Related Documentation

Information and Communication Technology Policy, Procedures and Processes
Incident Reporting App

[end]