

Key Cyber and Data Security Essentials



Cybersecurity

Update – Software Updates

- Install software updates on your devices and systems promptly.

Secure/Protect – Virus/Malware Protection, Access Control, Secure Configuration

- Use anti-malware and anti-virus solutions to protect against malicious software.
- Implement access control measures to control access to your data and services.
- Use secure settings for your organisation's procured hardware & software.

Backup – Backup Data

- Back up essential data and store them separately.

Asset – People, Hardware & Software, Data

- Equip staff with cyber-hygiene practices as the first line of defence.
- Identify and protect the hardware and software used in your organization.
- Identify the types of data your organisation has, where they are stored, and secure them.



Data Security

Secure – Storage, Reproduction, Conveyance Requirements

- Store your health information securely to prevent unauthorised access.
- Do not reproduce copies of health information unless necessary.
- Transport health information properly to avoid unwanted data exposure.

Identify – Classification and management of health information

- Identify and manage health information to apply appropriate safeguards.
- Differentiate and mark health information.

Access – Authorised Users

- Restrict access to health information for valid and relevant purposes.



Common Cyber & Data Security Requirements

Outourcing & Vendor Management

- Understand the responsibilities set between your organisation and vendor.

Incident Response

- Be prepared to detect, respond, and recover from incidents.

Disposal Requirements

- Proper disposal of health information mitigates the risk of unauthorised access.

Emergency & Contingency Planning

- Maintain the ability to withstand service disruptions to ensure business continuity.

Review Security & Internal Audit

- Conduct regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities.