Australia Post

Group Cyber Security Policy

Rationale and Scope

This Policy and the supporting standards set out the intent in managing cyber security and the expectation to safeguard information and technology assets for the Australia Post Group (Group), defined as the Australian Postal Corporation and its subsidiaries.

Information and technology are essential to Group business operations. The confidentiality, integrity and availability of these assets must be protected from cyber threats to minimise the risks to our customers, community, workforce, finances, reputation, compliance with legal and regulatory requirements and Group business continuity.

This Policy applies to technology and the information handled by the Group regardless of how it is collected, created, processed, distributed, stored, archived or decommissioned. This Policy applies to all directors, employees and contractors within the Group.

Policy Principles

The cyber security principles outline the expectations towards the protection of the Australia Post Group business, information and technology assets from cyber threats. These principles are grouped into four key cyber security activities of govern, protect, detect and respond. This policy endorses a “risk-based” approach to the management of cyber security across the Group.

Govern: Cyber security risk management.

- The confidentiality, integrity and availability requirements of information and technology must be determined and documented.
- Cyber security risk management must be embedded as part of the enterprise risk management framework and processes.
- Cyber security risks must be identified, documented, managed and accepted both before information and technology systems are authorised for use and continuously throughout their operational life.
- Business units are accountable ensure they follow and comply with all technology and security policies and standards to ensure they limit the enterprise exposure to cyber security risk.

Protect: People, process, and technology controls must be implemented to reduce cyber security risks.

- Technology systems must be designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.
- Technology systems must be delivered and supported by trusted suppliers.
- Technology systems must be configured to reduce their exposure to cyber-attacks.
- Technology systems must be administered in a secure, accountable and auditable manner.
- Security vulnerabilities in technology systems must be identified, prioritised and mitigated in a timely manner.
- Vendor supported and secure operating systems, applications and computer code must be operated on technology systems.
- Information of value must be secured via encryption.
- Information communicated between different technology systems must be controlled, inspectable and auditable.
- Due diligence must be undertaken prior to granting access to technology systems and data repositories.
- Users must be granted the minimum access to technology systems and data repositories required for their duties.
- Users must undertake ongoing cyber security awareness training.
- Physical access to systems, supporting infrastructure and facilities must be restricted to authorised users.

Detect: Detecting and understanding cyber security events.

- Cyber security events and anomalous activities must be detected, collected, correlated and analysed in a timely manner.

Respond: Responding to and recovering from cyber security incidents.

- Cyber security incidents must be identified and reported both internally and externally to relevant bodies, as required, in a timely manner.
- Cyber security incidents must be contained, resolved and recovered from in a timely manner.
- Business continuity and technical recovery plans must be developed, tested and enacted when required.

Policy Support and Administration

This Policy is supported by the technology and security standards published on the Group internal intranet site. The Information Security Office has the responsibility to support the implementation and management of non-compliance.

Policy Sponsor: Executive General Manager Transformation and Enablement

Policy Owner: Chief Information Security Officer

Version Number: V 4.0

Approved By: The Board

Approved On: 25 June 2021

Effective Date: 25 June 2021

Next Review Date: 25 June 2024

Glossary

Term	Definition
Cyber security events	An event constitutes an evident change to the normal behaviour of a network, system or user.
Cyber security incidents	An incident is an event that is not part of normal operations that disrupts operational processes.
Cyber Threat	Any circumstance or event with the potential to harm Australia Post's business, information or technology. Examples include malicious action by trusted insiders, malware, ransomware, spyware, distributed denial of service attacks, abuse of privileged access and secondary targeting.
System	A system is a combination of interacting elements such as hardware, software, data, humans, processes, materials that are organised to achieve one or more stated purposes.
Technology	Technology refers to both Information Technology such as applications, databases, operating systems, telecommunications systems, hardware, software and Operational Technology such as processing equipment, industrial control equipment, self-service terminals, building management system, fire control systems, physical access control mechanisms and parcel lockers.
Users	Users include Australia Post Group employees, consultants, contractors, third parties (including Australia Post franchisees) or any individuals with access to the Group's information technology resources.