Australia Post

Group Information Technology Policy

Policy Level	2
Accountable Executive	Chief Information Officer
Date Approved:	5 December 2019
Date Effective:	5 December 2019

Contents

Statement of Policy

Overview

This Group Information Technology Policy sets the fundamental principles and objectives on how Information Technology ("IT") is to be managed across the Australia Post Group ("Group"). It aligns to the Group Information Security Policy, Enterprise Risk Management Framework, Customer Data and Use Policy, Architecture Governance Framework, and other related policies and frameworks.

Supporting the principles in this policy are a set of IT Standards and architecture principles that specify minimum baseline requirements. The appendix at the end of this policy includes a list of the supporting Technology standards.

Rationale & Scope

IT is critical to Group business operations. As such, it is important to ensure that technology is used and managed in a consistent way across the Group and consistent with policies and standards that safeguard business operations. This policy defines the intended governance of IT.

In the context of this document the word IT refers to the information assets including infrastructure, applications, services, functions and data that electronically store, process, and transmit information. This document applies to all IT that is used in the Group.

Audience

This policy applies to all staff with authorised access to Group information assets. This includes, but is not limited to, employees, consultants, contractors and business partners.

Application

All requirements covered by in this policy and associated standards must be complied with for any new projects, activities or initiatives. Existing information assets should work toward complying with these new requirements but are not subject to retrospective compliance obligations.

If there are limitations to complying with new requirements, a policy exemption will be requested following the Standards Exemption process. For variation and exemption to this policy, please refer to the Breach, Variation and Exemption section below.

Policy Principles

The Group's IT policy principles expect all Group employees and workforce participants must:

1. Operate within the obligations relating to the acceptable use of Group technology assets. Technology must be used responsibly, professionally and consistently with "Our Ethics" for the purpose of pursuing Group business objectives, and not in contravention of any law or regulatory obligations, the best interests of the Company, or the direction of management.
2. Ensure any change to Information Technology Assets shall be subject to a formal risk analysis; controlled and managed in a consistent and transparent change management process, to safeguard and avoid disruption to existing services.
3. Ensure any incident related to Information Technology Assets shall be assessed and managed in a single, standardised approach to minimise the impact to IT services thus maintaining a consistent level of service quality and availability. Please refer to Group Enterprise IT Incident Management Standard.
4. Make certain all underlying weaknesses and problems in Information Technology Assets are formally registered and managed to maintain consistent and improved IT services.
5. Proactively manage all IT requests for services through centrally managed procedures to ensure timely, consistent and accurate delivery to the requestor.
6. Design IT services clearly so that the transparency of the service offered to the business is known thus the ability to demonstrate the cost and service level performance.

7. Deliver IT services with assurance that all Service Level Agreements (SLA) with the business will be met.
8. Prior consideration of purchase of any technology through a cloud service provider or third party, individuals must engage with their designated technology partner and receive endorsement from the Chief Technology Officer and the Information Security Office.
9. Prior to consideration of purchasing a new IT asset or service from a third party, individual business must engage with their technology partner and obtain architecture governance and chief technology endorsement first.
10. All Technology assets (both hardware and software) must be purchased through the IT & Services Procurement team to ensure strategic alignment with Technology Architecture principles and standards defined by the Chief Technology Officer. Any exceptions to this must be recorded by the architecture governance exemption process. Misalignment between business and technology must be escalated to the architecture governance to obtain CIO approval.
11. Ensure all Information Technology Assets are recorded as Configuration Items (CIs) in a central configuration management process, ensuring their ownership, attributes and relationships are maintained across the life of the asset.
12. Maintain all Information Technology Assets so that the asset and its technology remain current, vendor-supported and updated with the latest patches where required; ensuring all information assets comply with the relevant policies, standards and agreed business demands.
13. Maintain the IT investment governance process with a supporting technology strategy and roadmaps and standards for all technology investments (e.g. projects, change requests and BAU/OPEX funded investments). This is so that the IT solutions planning, architecture, design and build adheres to the endorsed principles and direction. Deviation from technology investment governance process shall be approved by appropriate levels of management.
14. Make certain all Information Technology Assets are physically secured against unauthorized access and protected against environmental damage (natural disaster, utility disruption, etc.). Physical access to Information Technology Assets shall be limited and be granted to approved and authorised person only.
15. Ensure a consistent level of IT service is provided across the Group, and capacity and performance of Information Technology Assets shall always be able to meet the agreed business demands.
16. Deliver and assure compliance with the IT Policy and Standards, Information Security Policy and Standards and all relevant regulatory and legal obligations is applied as mandatory. Information Technology Assets and associated management processes shall be subjected to regular assessment of their compliance to Policies and Standard.
17. Ensure critical Information Technology Assets have an IT Service Continuity Management and Technology Recovery Plan that addresses how services shall be managed in the event Information Technology Assets and services become unavailable. This shall include plans to recover the Information Technology Assets to the state prior to the interruption.

Awareness, Training & Induction

Policy awareness, training and support will be provided for applicable staff where relevant. This training is tailored to role requirements, is delivered within the relevant area of the business and will be facilitated by the office of the CIO. For more information or assistance with this Policy, contact the office of the CIO.

Enforcement & Monitoring

The CIO Office has accountability to enforce this policy and deal with intentional non-compliance. Where inappropriate conduct warrants it, disciplinary action may be taken in accordance with the applicable Group process or policy. The Group shall conduct reviews to ensure ongoing compliance with this policy and supporting standards. These reviews and audits shall be undertaken regularly by the Chief Information Office, Internal and/or External Audits.

Breaches, Variations & Exemptions

If there are limitations to complying with any requirement(s), it needs to be raised to and resolved with the CIO office or its delegated authority, with a formal risk assessment performed to minimise any risks through compensating controls. As requirements are largely specified by legal, statutory, regulatory, risk management or contractual obligations, compensating controls may be required.

Any request for exemptions to this policy shall be raised through the relevant business EGM and approved by the CIO Office. All exemptions must be centrally recorded, assigned an owner and formally reviewed, at minimum every 6 months.

Any behaviour that breaches this policy or the supporting standards will be managed through the applicable investigation and disciplinary processes. A proven breach may result in disciplinary action including termination.

All employees are responsible for identification and reporting of actual or potential breaches and risks. This requirement is contained in the Incident Management Policy.

Where breaches of this policy by a contractor is proven, the contract for services between the contractor and the Group may be terminated.

Note: All policy breaches must be escalated to Group Compliance and will be escalated to the Board Audit & Risk Committee if appropriate.

Reporting

The CIO office or its delegated authority shall be responsible for establishing and maintaining compliance reporting both internally (to management and the appropriate boards and committees), and externally (to regulators) as appropriate.

Policy breaches must be escalated to the respective management governance forums where appropriate.

Review

The Policy shall be reviewed for currency every 12 months, and at a minimum submitted for re-approval once every three years. It is the responsibility of the Accountable Executive to consider whether at any time there has been a change in circumstances that warrants a review and changes to the Policy.

.

Roles & Responsibilities

Policy Governance

Requirements	Responsible area/role	Activities
The Board must report on the implementation of governance frameworks and policies.	Board of Directors	The Board will ensure appropriate governance mechanisms and control frameworks are in place.
Accountable Executive	Chief Information Officer	Oversees the application of the Policy.

Policy Operation

Requirements	Responsible area/role	Activities
Identifying and managing the use of resources.	Managers	Fostering an environment that encourages compliance with the principles of the policy.
Comply with regulatory obligations, policies and procedures. Undertake relevant training.	Employee	Complying with regulatory obligations, policies and procedures relevant to their work responsibilities and behavioural guidelines.

Policy Monitoring & Oversight

Requirements	Responsible area/role	Activities
Compliance	CIO Office	Oversees and ensure compliance to the principles of the Policy.
Breach & Incident Reporting	CIO Office	Undertakes remediation and reporting for related matters to the Executive Council (EC)/Board of Directors.
Periodic review and/or internal audit for compliance to this policy	Group Compliance	Option to undertake periodic review and/or internal audit to ensure this policy is complied with and reporting of Breaches and incidents to the EC, and ARC.
Periodic internal audit for compliance to the policy.	Internal Audit	Option to undertake internal audit to determine level of compliance with the Policy, and ensure Breaches and Incidents are realised and reported appropriately.

Glossary

Term	Definitiion
Australia Post Group	Australia Post Group (Group). The Group is defined as the Australian Postal Corporation and its subsidiaries.
ARC	Audit & Risk Committee
CI	Configuration Item - Asset information identifying asset ownership, support contacts, dependencies and relationships recorded within the CMDB repository
CIO	Chief Information Officer
CMDB	Configuration Management Database – The central repository of all IT and related assets.
CTO	Chief Technology Officer
EC	Executive Council
EGM	Executive General Manager
EPF	Enterprise Portfolio Forum
Information Technology Assets	Information Technology Assets refer to IT infrastructure, applications and/or information.
IT	Information Technology

NOTE: Ensure Glossary is in alphabetical order.

Policy Administration

Key Policy Information

Administrative Area	Policy Information
Document Title	Group Information Technology Policy
Policy Level	2
Version No.	2.0

Policy Owners & Governance Forums

Administrative Area	Owner / Forum
Accountable Executive	Group Chief Operations Officer & EGM eCommerce Delivery
Policy Owner	Chief Information Officer
Policy Administrator	General Manager Group Compliance
Policy Content Owner	Chief Information Officer
Review & Approval Body	Audit & Risk Committee (Endorse) The Board (Approve)

Key Dates

Administrative Area	Policy Information
Policy Approval Date	5 December 2019
Policy Effective Date	5 December 2019
Next Scheduled Review	December 2020

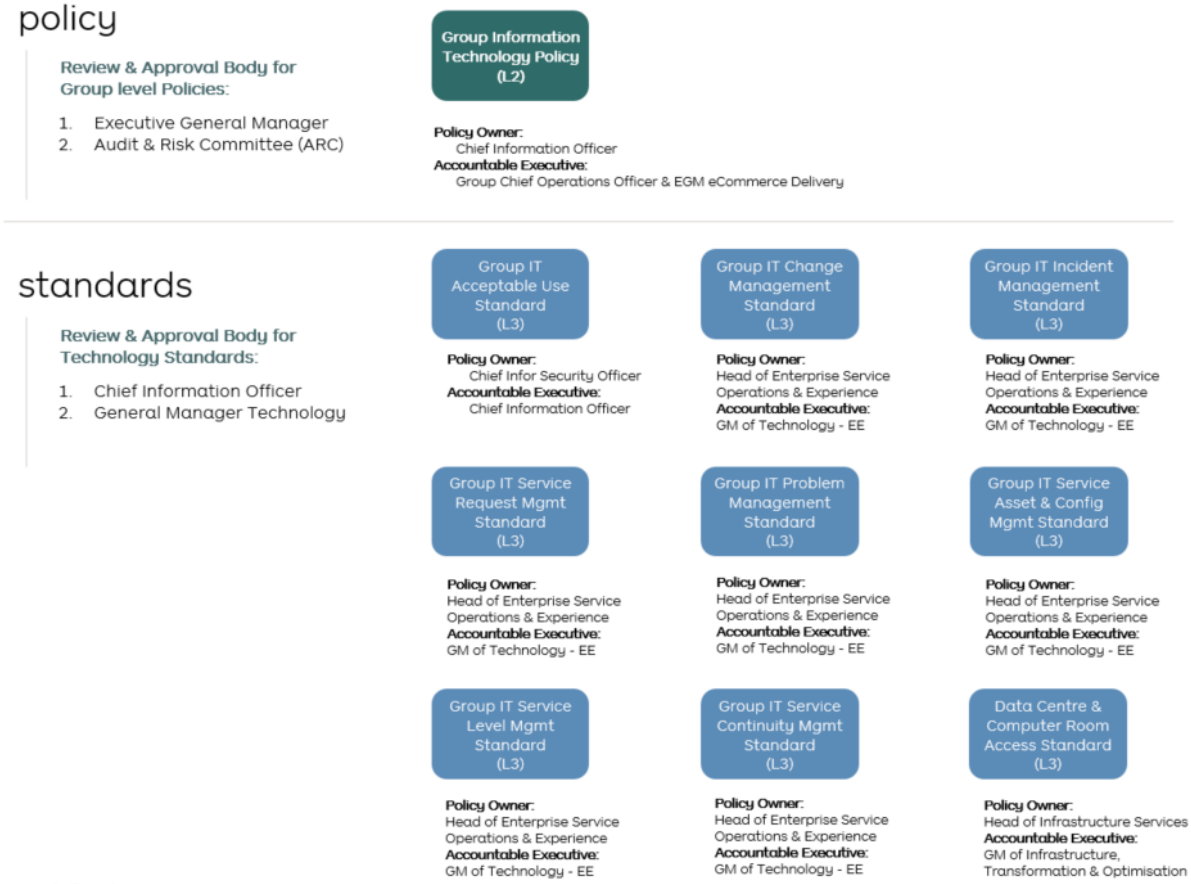
Appendix

Supporting Technology Standards & Documents

The following list identifies the 9 supporting IT Standards which outline how the principles of the Group Information Technology Policy should be met.

1. Group Information Technology Acceptable Use Standard (Level 3)
2. Group Enterprise Technology Change Management Standard (Level 3)
3. Group Enterprise Incident Management Standard (Level 3)
4. Group Enterprise Problem Management Standard (Level 3)
5. Group Enterprise Request Management Standard (Level 3)
6. Group Information Technology Service Asset & Configuration Management Standard (Level 3)
7. Group Information Technology Service Level Management Standard (Level 3)
8. Group Information Technology Service Continuity Management Standard (Level 3)
9. Data Centre & Computer Room Access Standards (Level 3)

Image 1 – the 9 'Information Technology Standards' supporting the policy principles



Classification: Internal