Group Technology Policy

Policy Level:	2
Accountable Executive:	Chief Information Officer
Date Approved:	20 November 2017
Date Effective:	20 November 2017

auspost.com.au

Contents

Statement of Policy

Overview

This policy deals with the provision of information technology resources by Australia Post and the associated responsibility of authorised users when accessing these information technology resources.

Rationale & Scope

Authorised users include Australia Post employees, consultants, contractors, third parties (including Australia Post franchisees,) or any individuals (referred to as "Users") with access to Australia Post's information technology resources including, but not limited to, the Australia Post network, desktop computers, laptops, tablets, data, software, printers, fax machines, mobile/smart phones, mobile devices, information systems, access to the Internet, electronic mail, telephony and related services (referred to as "Australia Post Resources").

The principles of this policy also apply to non-Australia Post supplied resources, such as where a user has chosen to "bring their own device" (e.g. a mobile phone).

Audience

All Users with access to Australia Post's resources.

Application

This policy applies to the Australia Postal Group (APG).The APG is defined as the Australian Corporation and its subsidiaries.

This includes, but is not limited to, employees, workers, consultants, contractors, Licensed Post Offices, franchisees, service providers and business partners.

These may also be referred to as individuals, workers, persons or employees in this policy

Policy Principles

1. Acceptable Usage

All Australia Post resources are the property of Australia Post and must be used by our Users responsibly, professionally and consistently with "Our Ethics" for the purpose of pursuing Australia Post business objectives. Users accessing Australia Post Resources must take reasonable and prudent steps to protect the confidentiality and integrity of the Australia Post Resources. Damage and/or loss of Australia Post Resources (e.g. laptops) must be reported

2. User Security

Any access to corporate systems must be approved and all Users must comply with Australia Post's security requirements.

3. Mobile Devices

All Australia Post staff who are eligible for a mobile device are governed by this policy and conditions pertaining to device usage, including acquisition, disposal and security.

4. Data Ownership

All electronic data and communications stored on or transmitted through Australia Post networks are the property of Australia Post regardless of their form or storage location. Australia Post reserves the right to access such data (including emails and the results of Internet usage).

5. Privacy

Australia Post Users must comply with Australia Post's internal Privacy Policy and the requirements under all relevant Privacy Legislation

6. Monitoring of Usage

Users must be aware that usage of Australia Post Resources will be monitored by Australia Post, including email and internet activities on its IT equipment. Monitoring of Australia Post Resources will be continuous and ongoing.

7. Non APG provided resources

Users may use their own mobile devices to connect to Australia Post resources and will need to comply with the principles of this policy.

Awareness, Training & Induction

Awareness and training programs for this policy and associated standards will be delivered to new and continuing staff.

Enforcement & Monitoring

Management has accountability to enforce this policy and deal with intentional non-compliance through both the performance management and disciplinary processes. We will at our discretion conduct periodic reviews to ensure ongoing compliance with this policy.

Breaches, Variations & Exemptions

An exemption process must be maintained. Management may seek exemption or variation to policy requirements through the use of the exemption process. As requirements are largely specified by legal, statutory, regulatory, risk management or contractual obligations, compensating controls may be required.

Breaches of this policy will be addressed as prescribed in appropriate Australia Post policies, contracts and agreements relating to human resources, contractors, partners, and service providers. All potential policy breaches will be investigated.

In support of this policy, Australia Post will follow a formal disciplinary process for those who breach this policy or the supporting Australia Post Information Security Standards. Disciplinary action for breaching this policy or causing a security breach will be as appropriate, up to and including termination and/or possible criminal/civil charges.

Reporting

The Information Security Office will be responsible for establishing and maintaining compliance reporting both internally (to management and the appropriate boards and committees), and externally (to regulators) as appropriate.

Incident and breach escalation:

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

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

Review

This policy will be reviewed at least every three years.

Policy Guidelines

Acceptable Usage

All Australia Post Resources are the property of Australia Post and must be used responsibly, professionally and consistently with "Our Ethics" for the purpose of pursuing Australia Post business objectives. Users accessing Australia Post resources must take reasonable and prudent steps to protect the confidentiality and integrity of Australia Post resources. Damage and/or loss of Australia Post resources (e.g. laptops, mobile devices, etc.) must be reported.

Australia Post allows limited, reasonable and occasional personal use of Australia Post Resources. However, personal use of Australia Post Resources must not interfere or conflict with Australia Post's functions, operations and objectives. Reasonable personal use is at the manager's discretion and must constitute a minor use of the Australia Post Resource.

Emails received at Australia Post's email or internet addresses are deemed to be messages addressed to Australia Post.

Use of Australia Post email facilities by union delegates for union-related business is conditional upon that use complying with this policy requirement, including that any use must not be against the interests of Australia Post and is not excessive. The use of facilities by union delegates for internal communications of union matters is subject to prior authorisation on each occasion by the relevant Australia Post facility/line manager.

Examples of Unacceptable Use

The following is a non-exhaustive list of actions or activities that would generally constitute unacceptable use of Australia Post resources. This list is intended to be a guideline for users when considering what unacceptable use (i.e. policy violations) of Australia Post resources is.

Users must not:

- Allow other users to access Australia Post information systems by sharing or writing down access credentials
- Conduct unlawful or unethical (i.e. not conforming to accepted standards of social or professional behaviour) activities, e.g.
    - Unauthorised use of copyright material from the Internet, such as downloading copyright music or movie content.
    - Unauthorised attempts to break into, or illegally access or damage, other computer systems or data.
- Send/transmit, store or participate in spam, chain, junk or hoax email.
- Copy/store, send/transmit or access/view any unacceptable material including drawings, cartoons, jokes, texts, photographs, animations or videos that are racist, pornographic, sexually explicit, abusive or sexist.
- Copy/store, send/transmit or access/view any unacceptable material that has the potential to degrade, offend or embarrass a person because of their disability, age, sex, religion, ethnicity or any grounds described in Australia Post's Harassment, Discrimination and Bullying policy, or perform any activity that otherwise constitutes harassment, discrimination, bullying or otherwise constitutes a breach of "Our Ethics".
- Copy/store or send/transmit or access/view customer payment card data outside of Australia Post approved processes or procedures. Customer payment cards include, but are not limited to, customer credit cards, debit cards and charge cards. Payment card data includes the Account Number, Expiry Date and the Card Security Code. The limitations on customer payment card data do not apply to Australia Post corporate credit card data and personal payment card data of Australia Post Users.

– Access websites or applications that deal with criminal activities, including, but not limited to, those involving or related to illegal drugs, computer hacking/cracking, the creation of malicious software (malware), terrorism, and illegal weapons, unless specifically authorised to access such websites or applications for legitimate business purposes relevant to required role(s).

– Publish, send/transmit or copy content or messages, over the Internet, via email or any other means that disclose Australia Post information (e.g. personal information, financial information, intellectual property, security controls, etc.) without authorisation.

– Access websites or applications for personal use that consume excessive network resources for long periods of time, such as multiplayer games, virtual worlds, large file transfers and streaming media.

– Use Australia Post Resources to operate a business or any undertaking that offers commercial gain outside the scope of the User's authority.

User Security

Any access to corporate systems must be approved and all users must comply with Australia Post's security requirements.

Users may be required to undergo an appropriate level of employment checking (e.g. background check, reference check etc.) to provide assurance about the suitability of personnel authorised to access Australia Post Resources.

All Users will be provided with security awareness training and awareness updates from time to time.

Mobile Devices

All Australia Post staff who are eligible for a mobile device are governed by this policy and conditions pertaining to device usage, including acquisition, disposal and security.

Users are responsible for the proper use, care and maintenance of Australia Post provided mobile devices. The User must:

- Protect their mobile and voice mail by retaining active Personal Identification Number (PIN) and security numbers as appropriate. Additionally, users should retain a record of their handset International Mobile Equipment Identity (IMEI) number (included in the delivery information that comes with the device) to assist with blocking the handset if lost or stolen

- Not browse Internet sites that are deemed inappropriate as per this policy

- Not use the mobile device for any unlawful activity, commercial purposes not authorised or unrelated to Australia Post

- Include their allocated mobile number in their Outlook Properties to allow staff to readily contact them.

- Australia Post allows limited, reasonable and occasional personal use of corporate mobile devices and telephony facilities. However, personal use of an Australia Post mobile device and telephony facilities must not interfere or conflict with Australia Post's functions, operations and objectives

- Must employ reasonable physical security measures and are not allowed to make any reconfiguration of the mobile device.

Any attempt to contravene or bypass the centralised security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Australia Post Information Security Policy.

In the event of a lost or stolen mobile device it is incumbent on the User to report this to the Australia Post IT Service Desk immediately where necessary actions will be taken to remotely wipe off the data from the device.

At the end of employment, all Australia Post staff must return to their manager/supervisor, mobile devices issued to them.

Data Ownership

All electronic data and communications stored on or transmitted through Australia Post networks are the property of Australia Post regardless of their form or storage location. Australia Post reserves the right to access such data (including emails and the results of Internet usage).

Use of Australia Post systems constitutes permission by the user for Australia Post to access such data as permitted by law.

As per the Information Classification and Handling Standard, all data should be processed, stored, transmitted, communicated and handled according to its classification and only on approved systems/solutions provided in-house or by third party service providers.

Data Security

All Australia Post Data should be used and protected as per Australia Post's Information Classification and handling standard.

Information Usage

Australia Post information should only be used with the purpose for which the information was initially collected or created. Misuses of Australia Post information consist of malicious or accidental abuse that go against the original purposes of the information.

Users should only share Australia Post information with authorised persons who have a legitimate reason to access said information to perform their job duties.

Confidential Australia Post information should be cleared and stored in a secure location when users are away from their desks.

Privacy

Australia Post Users must comply with Australia Post's internal Privacy Policy and the requirements under all relevant Privacy Legislation.

Users are reminded that personal information must be appropriately managed in accordance with our privacy obligations. This includes when using Australia Post's Resources.

All IT equipment and software used and the personal information stored on or transmitted to or from Australia Post IT systems, remains at all times, to the extent permissible by law, the 'property of Australia Post'.

Managers should be reminded that - notwithstanding Australia Post's ownership of stored data - they have an obligation to maintain confidentiality over data created by Users who have left or are no longer contracting with or affiliated contractually with the organisation and to respect the privacy of individuals at all times.

Monitoring of Usage

Users must be aware that usage of Australia Post Resources will be monitored by Australia Post, including email and internet activities on its IT facilities. Monitoring of Australia Post Resources will be continuous and ongoing.

Australia Post reserves the right to access, inspect and disclose all activities and electronic communications on the Australia Post network and systems, using Australia Post's IT systems and facilities. As part of this monitoring, Australia Post may:

- Create log files to track use and perform audits of that activity as necessary

- Access files and emails stored on Australia Post's IT facilities and on computer systems connected to those facilities
- Bypass any password protection or encryption measures necessary to enable monitoring activities.

Users must not attempt to hide Internet activity for the purpose of evading corporate monitoring.

Roles & Responsibilities

Policy Governance

Requirement	Responsible area/Role	Activities
The Enterprise Risk & Compliance (ER&C) must report on to the implementation of governance frameworks and policies.	ER&C	The ER&C will ensure appropriate governance mechanisms and control frameworks are in place.
Chief Information Officer	Accountable Executive	To oversee the application of the Policy

Policy Operation

Requirement	Responsible area/Role	Activities
Identifying and managing the use of resources	Managers	Fostering an environment that encourage compliance with the principles of the policy
Comply with regulatory obligations, policies and procedures. Undertake relevant training.	Employees	Complying with regulatory obligations, policies and procedures relevant to their work responsibilities and behavioural Guidelines .

Policy Monitoring & Oversight

Requirement	Responsible area/Role	Activities
Compliance	Information Security Office	Oversee and ensure APG compliance to the principles of the Policy.
Breach & Incident Reporting	Information Security Office	Will undertake remediation and reporting for related matters to the Executive Committee (EC).
Periodic review of compliance to this policy	Internal Audit	Undertake periodic review to ensure this policy is complied with and reporting of Breaches and incidents to the EC and ARC.

Glossary

Term	Definition
APG	Australia Post Group (APG).The APG is defined as the Australian Postal Corporation and its subsidiaries.
Mobile Devices	Mobile phones, tablet computers, laptops, and other portable internet connected devices used for voice, text and data communications.

Document Reference

Document	Link
Our Ethics	https://pogo.corp.auspost.local/dafiles/intranet/pogo/ourorg/ourvalues/culturepillars/Our%20Ethics%20booklet.pdf
Information Classification and Handling standard	https://pogo.corp.auspost.local/dafiles/intranet/pogo/atwork/itandtechsupport/security/Information%20Classification%20and%20Handling.pdf

Policy Administration

Key Policy Information

Administrative Area	Policy Information
Document Title	Group Technology Use Policy
Policy Level	2
Version No	2.1

Policy Owners and Governance Forums

Administrative Area	Owner / Forum
Accountable Executive	Chief Information Officer
Policy Owner	Chief Information Security Officer
Policy Administrator	General Manager, Risk & Compliance
Policy Content Owner	Manager, Technology Governance Risk and Compliance
Review and Approval Body	Executive Committee - Management Forum

Key Dates

Administrative Area	Date
Policy Approval Date	20 November 2017
Policy Effective Date	20 November 2017
Next scheduled review	20 November 2020