Department of Planning and Environment

Corporate policy

# Acceptable Use Policy

## Purpose of this policy

All Department of Planning and Environment (the department) employees need to be aware of their obligations when using the department's Information and Communication Technology (ICT) resources including equipment, services and information. Their use must be ethical, lawful and appropriate, in accordance with the department's values and policies, and in line with any applicable NSW and Commonwealth legislation and regulations.

This policy complements the Code of Ethics and Conduct, and supports the requirements set out within the Information Security Management System (ISMS) so that the department can achieve the following information security objectives:

- Apply appropriate risk-based controls to manage confidentiality, availability and integrity of information, by focusing on sensitive information.
- Ensure continual improvement of security controls in order to maintain an acceptable level of risk.
- Develop associated policies, standards, processes, procedures, guidelines, reports and other artefacts to effectively operate, manage, measure and govern information security as an integral business process.
- Increase information security awareness across the organisation.
- Provide appropriate management of internal and external audit issues.
- Comply with the NSW Cyber Security Policy requirements by achieving and maintaining ISO 27001 certification.

The information security practices in conjunction with this policy preserve the reputation and integrity of the department's information assets.

## To whom this policy applies

This policy applies to all employees accessing the department's information and ICT resources, including individuals seconded from other organisations, volunteers, contingent or labour hire workers, professional services contractors and consultants.

## Policy statement

### Ownership of ICT resources

The department is the legal owner of all physical and electronic information, computing and communication technology resources created or acquired to conduct the department's business.

The department delegates to its employees, daily management responsibility and custodianship of information and ICT resources for their use, maintenance and protection. With best effort and due care, employees are responsible for upholding the department's policies to protect the department's information and ICT resources.

## Personal use of ICT resources

The department provides ICT resources primarily for authorised business purposes. Incidental personal use is permitted, provided that it is limited, and does not impact on service delivery. To protect public interests in the use of public resources, employees have no inherent right to use the department's ICT resources for non-government purposes.

## General use of ICT resources

When using the department's ICT resources, employees must use their best effort and care to:

- safeguard login credentials to prevent unauthorised access by not sharing passwords and implementing an appropriately robust password in accordance with system requirements
- safeguard allocated ICT resources from loss and damage
- respect and protect privacy and intellectual property of all parties
- observe and comply with agency information and record management requirements
- maintain the integrity of the department's information and ICT resources
- lock your screen when you step away from your desk and maintain a clear desk to protect the disclosure of sensitive information
- limit the printing of information and ensure hard copies are securely destroyed
- limit the removal of hard copy information from official departmental locations
- when using email, mobile apps/freeware, web browsing, downloading or sharing ICT resources internally and externally:
    - observe privacy and sensitive information practices to ensure department's information is classified, protected and confidentiality is maintained accordingly
    - use only authorised and trusted channels for information exchange and sharing
    - be cautious of malicious intent and malware infection risks from unknown email sources, attachments, internet browsing, and freeware downloading.

## Use of internet, social media and internal communication channel

The department provides internet and social media access to all authorised users to assist them in the performance of their roles. Access to internet, social media and internal communication channels (such as Workplace, Microsoft Teams and email) using the department's ICT resources must be conducted in compliance with this policy, and any other associated policies including the Code of Ethics and Conduct.

Personal social media channels must not be used to discuss, display or reference sensitive departmental information. Only approved social media channels and accounts may be used to convey officially sanctioned information. Employees are not permitted to create social media channels, digital assets (e.g. websites) or subscription accounts for the department unless authorised to do so.

Use of the department's internet, social media and internal communication channels must not:

- reflect badly on the department or NSW Government, such as pirating software, breaching third party intellectual property rights, hacking, participating in the viewing or exchange of pornography or other obscene materials, or engaging in any other unethical or unlawful conduct
- be used to download or store games, movies or other unauthorised executable files
- be used to conduct non-departmental business activities beyond acceptable use tolerances
- be used to participate in gambling
- be used to promote political commentary
- be used to negatively affect the department's reputation.

## Use of electronic communication

Electronic communication is limited to official business and occasional personal use for communicating, exchanging and sharing information with both internal and external parties.

Prior to sending, users must observe the NSW Government Information Classification, Labelling and Handling requirements to ensure the intended recipients are aware of the contents sensitivity and requirements for protection.

Employees must take reasonable care when opening emails to prevent embedded malware such as ransomware, malicious hyperlinks, and viruses.

Employees must never click on a URL/hyperlink or open an attachment in an email unless they are certain the email comes from a trusted source.

Personal electronic communication conducted on or via departmental resources will not be guaranteed private or absolutely secure, and no access will be granted once employment with the department ceases.

## Use of cloud services

Users are only permitted to use cloud computing services that are officially authorised under a licence arrangement. Access to cloud-based services must only be done via an enterprise user account or an account created for a specific business purpose that has been endorsed for use.

Users should not use official cloud-based services for personal use beyond what is considered acceptable as outlined in this policy. Users should not use personal or unofficial cloud services to transact, transfer or store the department's information and records.

## Remote working

Employees with approval to undertake business from home or other remote working environments must take ownership and responsibility to protect and secure the department's ICT resources and information in a manner consistent with being in the office.

When using mobile Apps, employees must assess the risks, and take reasonable care in accepting the usage agreements of the Apps that may lead to unwanted disclosure of personal and private information. Such disclosure may directly or indirectly impact department's business and policies. Employees must not download or install software (including Apps) on any department equipment unless formally approved by management and such use must comply with any applicable licence agreements for department's business.

When working remotely, employees must utilise, whenever possible, their own private internet connection (ADSL, NBN, Mobile Data) to avoid sensitive information being intercepted whilst being transmitted over the internet. Public Wi-Fi should not be utilised for business purposes.

Employees travelling overseas with the department's information and ICT resources must contact the Service Centre prior to departure, in order to implement any precautionary measures.

## Physical access controls

All doors, windows, desks and facilities containing department's ICT resources must be secured appropriately to prevent unauthorised access. Lost, stolen or damaged passes and keys must be reported to your Service Centre as soon as possible.

Unauthorised physical access through tailgating must be deterred at all times.

## Reporting security incidents

All employees are responsible for reporting any actual, perceived, suspected or potential information security incidents as quickly as possible to the Service Centre.

Alleged or suspected policy breaches must be reported to people leaders or senior officers and referred for investigation to the Chief Information Security Officer or equivalent.

## User awareness training and simulation exercises

All employees must participate in user awareness training and simulation exercises conducted by the Digital and Information Office (DIO) annually or as required and provide feedback to improve the overall awareness of employees.

## Monitoring

Any use of the department's ICT resources is made with the understanding that such use is not absolutely secure, private nor anonymous and is primarily for business use. Employee usage of the department's ICT resources may be subject to authorised investigation for potential policy and Acceptable Use Policy non-compliance or abuse of privileges. Requests for access to information to support authorised investigations must be approved by the Chief Digital and Information Officer or authorised delegate.

The department employs continuous CCTV cameras, physical access controls, computer and application activity logging and monitoring to ensure the safety and security of information, people, assets, property and finances. All reasonable care is taken to protect user privacy. Access to monitoring system records is restricted to authorised personnel.

The department will respond promptly to requests for information arising from criminal investigations and legal proceedings, requests by Parliament under Standing Order 52 notices and requests under the Government Information (Public Access) Act 2009, including the department's information, records and ICT resources. The department, therefore, reserves the right to access any of its information systems and data repositories to inspect, review, store or retrieve data in those systems.

This policy is consistent with the NSW Workplace Surveillance Act 2005, State Records Act 1998 and Government Information (Public Access) Act 2009.

### Exemptions

- Exemptions to this policy shall comply with the ISMS Exemption Request Management Standard.
- Exemptions shall only be approved where it is technically, practically or financially infeasible to comply with this policy.
- Reviews of exemptions shall be performed annually.

## Failure to comply with this policy

Ethical and behavioural standards that employees are expected to demonstrate while working with the department are set out in the Code of Ethics and Conduct. If employees fail to meet those standards, corrective action may be taken in accordance the Code of Ethics and Conduct.

Individuals who are not government sector employees such as volunteers, contingent or labour hire workers, professional services contractors and consultants may have their services, contract or agreement terminated immediately, or legal action could be taken if they are found to have violated this policy.

## Review timeframe

Digital Information Office will review this policy no later than 3 years from the date the document is approved. This policy may be reviewed earlier in response to post-implementation feedback, changes to legislation, or as necessary in accordance with the department's policy and procedures.

## Related documents

A full list of legislative requirements that may impact information security is maintained within the Information Security Management System (ISMS).

- ISO/IEC 27001: 2013 – Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002: 2013 – Information technology – Security techniques – Code of practice for information security management

This policy should be read in conjunction with the following documents:

- Cyber Security Policy
- Access Control Policy
- ISMS Exemption Request Management Standard
- Code of Ethics and Conduct
- NSW Cyber Security Policy
- NSW Cyber Security Strategy

# Policy metadata

Table 1. Policy metadata

| Category | Description |
|---|---|
| **Status** | Final |
| **Date of approval** | 27.05.2021 |
| **Approver** | Group Deputy Secretary |
| **Group** | Corporate Services |
| **Division** | Digital Information Office |
| **Policy owner** | Chief Digital and Information Officer |
| **Document location** | DPE Intranet and Internet |
| **Next review date** | April 2024 |
| **Associated procedure** | N/A |
| **Any additional applicability** | Additional applicability will be considered in the future |
| **Superseded document** | ICT Acceptable Use Policy, Department of Planning and Environment<br>ICT Conditions of Use policy, Department of Industry<br>Information and Communication Technology Acceptable Use Policy, Office of Environment and Heritage |
| **Further information** | cybersecurity@dpie.nsw.gov.au |
| **Document Reference** | POL21/11 |

# Version control

Table 2. Version Control

| Version | Date issued | Change |
|---|---|---|
| **1** | 27.05.2021 | Merged policies of previous departments/agencies for new department policy. |
| **1.1** | 3.05.2022 | Updated to reflect new branding and name change |

# Appendices

Appendix 1 – Definitions

# Appendix 1 – Definitions

Table 3 – Definitions

| Term | Definition |
|---|---|
| Agency | Has the same meaning as defined under the Government Sector Employment Act 2013. |
| Availability | Ensuring that department's ICT resources are accessible for use as, and when they are required. |
| Care | The obligations of the user to take all reasonable action to protect the department's information and ICT resources to prevent damage, harm, injury or loss (including economic loss). |
| Confidentiality | The state of sensitive information being protected from unauthorised access, ensuring that only those with authorisation can access information assets. |
| Department | The governance arrangement of a general government sector entity[1]. |
| Information | Information held by an agency is defined in Clause 12 of Schedule 4of the Government Information (Public Access) Act to mean:<br>• information contained in a record held by the agency<br>• information contained in a record held by a private sector entityto which the agency has an immediate right of access<br>• information contained in a record that is in the possession under the control, of a person in his or her capacity as an officer or member of employee of the agency.<br>This policy uses the word 'information', which includes 'records' and all types of information, as defined in the Act. |
| Information and Communication Technology resources (ICT resources) | Any information, or other assets associated with information and information processing facilities, such as:<br>• information as defined above<br>• laptops, desktops, tablets, external hard-drives, USB memory sticks, memory cards, printers, scanners, faxes, and multi-function devices (devices that provide more than one function e.g. printing, copying scanning)<br>• telephones, mobile phones, and smart phones<br>• secure offices, computer room, network equipment locations,and data centres<br>• network systems, software, applications, apps, and web sites. |
| Information Security[2] | • Preservation of confidentiality, integrity and availabilityof information. |

| Term | Definition |
|---|---|
| Information Security Incident[3] | Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. |
| Integrity | In the context of department's ICT resources, the department can trust the information processed to be complete, accurate and relevant.Other characteristics of integrity may also be observed in Part 2 of the Government Sector Employment Act 2013. |
| Intellectual Property (IP)[4] | What can be legally owned as the product of intellectual activity in the industrial, scientific, literary, artistic, musical and dramatic fields. |
| Login credentials | Login credentials are given to authenticate a user and allow access to ICT resources (e.g. User ID and Password pair, User ID and Password associated with one time password, User ID and Password associated with some personal questions only the user can answer) |
| Remote working | Including working from home, remote working is a method of working that uses technology to facilitate employee working outside of official physical work locations. |
| Personal information | has the meaning as defined in the Privacy and Personal Information Act 1988. |
| Service centre | A single point of contact and communication for business transactions and incident management matters. CS Service Centre provides technology, finance and human resource support for the majority of the Department of Planning and Environment and Department of Regional NSW users. However, some users may rely on support from other Service Centres responsible for the management of their ICT systems and/or devices. |
| User | Employees, contractors, consultants and volunteers engaged by department agency who have access to any department's ICT resources. |

[1] Governance Arrangements Chart, 1 May 2020, NSW Department of Premier and Cabinet

[2] ISO/IEC 27000:2016

[3] ISO/IEC 27000:2016

[4] NSW Intellectual Property Management Framework