ICT Acceptable Use Policy

Version 2.0
February 2024

1 Purpose and Scope

The purpose of this policy is to inform members of the appropriate use of NSW SES information, systems, network, data, assets, and resources.

This policy is in place to protect NSW SES and its members. Inappropriate use of NSW SES information, systems, network, data, assets, and resources exposes NSW SES to security risks including virus attacks, compromise of network systems and unauthorised use of information.

This policy applies to:

- the use of all NSW SES information, systems, network, data, assets, and resources.
- all NSW SES members and third parties engaged by NSW SES, regardless of location.
- equipment that is owned or leased by NSW SES.

This policy is to be read in conjunction with its' parent policy *Cyber Security Policy* (NSW SES) to ensure business continuity by preventing and minimising the impact of security incidents with NSW SES information and IT assets.

2 Policy principles for ICT acceptable use

1) Members and third parties must take responsibility for using NSW SES information systems, network, data, assets, and resources in an ethical, secure, and legal manner.
2) Members and third parties have a responsibility to be vigilant and know how to protect themselves and the organisation in line with the acceptable use policy principles.
3) Any members and third parties found to have violated this policy may be subject to:
    - disciplinary action, up to and including termination of employment, and related civil or criminal penalties.
    - sanctions up to and including removal of access rights, and termination of contract(s).

2.1 Information management and handling

Members and third parties must, always, safeguard NSW SES information systems, network, data, assets, and resources against inappropriate or unauthorised access. In particular:

- NSW SES information systems, data, assets, and resources must be used primarily for NSW SES activities.
- Members must adhere to the requirements of the NSW SES Records Management Policy, Record Management Policy Guideline and Privacy Management Plan in relation to the collection, storage, access, accuracy, use and disclosure of personal information.
- Disposal of all documents must comply with the NSW SES Records Management Policy.
- All Sensitive material must be disposed of securely.

2.2 Intellectual property

a) Members and third parties must ensure they comply with the NSW SES Intellectual Property Policy and Intellectual Property Procedure.

b) If a member has any queries regarding Intellectual Property, they should seek guidance from the NSW SES Intellectual Property Policy Owner, NSW SES Chief of Staff.

2.3 Media and equipment

a) Members are personally accountable in their use of NSW SES resources and are responsible for the equipment assigned to them or their position. Members and third parties must:

    - report all lost or stolen equipment immediately (including approved personally owned 'bring your own device' (BYOD) used to access NSW SES information services) to their manager, the Service Desk and NSW Police, refer to NSW SES Mobile Device Policy.
    - not modify the security controls and settings on NSW SES computer equipment or devices e.g., remove or disable anti-virus software.
    - not download, install, or use software on NSW SES computer equipment or devices that has not been licensed and authorised by NSW SES.
    - not connect unauthorised devices or equipment to NSW SES internal networks, e.g., non-NSW SES laptops, routers, wireless access points etc.

b) Members and third parties must adhere to the following requirements when using removable media such as USB sticks, portable disc drives, DVD ROMs etc.:

    - Any disks, removable media, CD-ROMs, or other electronic media must be appropriately handled whilst stored or transferred to premises outside NSW SES.
    - All Sensitive information must be encrypted prior to transfer via removable media.

- Removable media containing NSW SES information which has been lost or stolen must be reported to the member's manager and the Service Desk immediately.
- Removable media containing NSW SES information must comply with the NSW SES Record Management Policy Guidelines.
- Removable media must not be used as a repository for NSW SES records and information.

c) NSW SES ICT systems must not be used to store personal movies, music, photos, or other non-incidental data. NSW SES may, without notice or employee approval, investigate, replicate and/or remove any illegal or unacceptable material from its computing resources where clearly not related to work purposes.

2.4 Clear screen work areas

a) Members must lock their screens when away from their devices (e.g., desktop computers, laptops, tablets, phones etc.).

b) Members and third parties using devices from remote locations (e.g., public transport) should be aware of unauthorised people viewing their device. Sensitive information must not be accessed on the device when viewable by unauthorised persons.

c) Unattended remote access sessions must be locked to prevent unauthorised access.

2.5 User access

a) Access to NSW SES information systems, network, data, assets, and resources is restricted through user identification and authentication controls. Each user (member/third-party) will be uniquely identifiable to ensure accountability.

b) Members and third parties must ensure they comply with NSW SES ICT User Access Policy.

c) Members agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited. Members are fully responsible for their use.

2.6 Passwords

Members must ensure that passwords used to access NSW SES information systems, network, assets, and resources comply with the NSW SES Password Policy.

2.7 Internet and electronic communication – personal use

Reasonable personal use by members of information systems such as the internet and personal email is permitted outside of core business hours, i.e., during lunch breaks, and at the beginning/end of the day, (provided members are not claiming this time on their time sheet).

2.8 NSW SES email and electronic communication

a) All members represent NSW SES when using agency systems and resources to access and use the internet. Members and third parties must not attempt to bypass, circumvent, or otherwise negate any controls that NSW SES may implement in support of the secure and effective operation of its email and electronic communication services.

b) Emails sent or received through NSW SES email accounts are not private and are stored and accessible by NSW SES.

c) With approval from the Deputy Commissioner Corporate Services and the Director, People and Development, emails sent or received through NSW SES email accounts (active or archived) may be accessed at any time by NSW SES for an authorised purpose, such as for an investigation or where otherwise required by law.

d) Members are prohibited from:

- installing unauthorised email software on NSW SES computers.
- using their NSW SES email address to subscribe to mailing lists except in relation to work or professional development purposes.
- any form of harassment via email, telephone, or paging, whether through language, frequency, or messages.
- unauthorised use, or forging, of NSW SES email header information.

e) Members must not use another member's email account to send email messages unless this is included as part of their role and have been given explicit permission to do so from the account owner.

f) When engaging in online communication, including the use of social networking sites in organisational and personal capacity, members:

- are expected to uphold the values, obligations and expectations of members outlined in the NSW SES Code of Conduct and Ethics.
- must ensure that comments relating to personal views do not imply endorsement by NSW SES.
- must not divulge Sensitive NSW SES information.

2.9 Internet usage

a) The use of the internet or email to make or send fraudulent, unlawful, offensive, or abusive information or messages is prohibited. Members are to report receipt of any such messages to their immediate manager.

b) The following activities are not permitted whilst using internet and email services provided by NSW SES. Users must not:

- intentionally access, create, transmit, distribute, or store any offensive information, data or material that violates Australian or State regulations or laws. NSW SES reserves the right to audit and remove any illegal material from its computers without notice.
- undertake any form of computer hacking (illegally accessing other computers).

- use the internet or email for activities that might be questionable, controversial, or offensive, such as gambling, gaming, accessing chat lines, transmitting inappropriate jokes, or sending junk programs.
- intentionally transmit copyright-protected material which subsisting intellectual property rights exist without the written permission of the owner.
- illegally download, stream, or upload copyright protected content such as videos, music, and other data.
- download and install program files (i.e., executable software). If access is required to additional software, members must complete the appropriate form and forward it to the Service Desk. This process must be followed regardless of the license type of the software (e.g., free trial, freeware, etc.).

2.10 Monitoring

a) To ensure NSW SES security standards are maintained, NSW SES information systems, network, data, assets and resources for internet and electronic communications are always monitored.

b) Use of NSW SES information systems, networks, data, assets, and resources constitutes consent to:

- monitoring of all the systems owned and managed by NSW SES.
- disciplinary action against those who use NSW SES information systems, network, data, assets, and resources in a manner which contravenes policies.

2.11 Incident reporting

Members must report any information security incidents, breaches and weaknesses to their manager and the Service Desk immediately.

Information security incidents may include but are not limited to:

- suspicion that a user account has been used by someone else.
- unauthorised access to a secure area by a third-party.
- breach of confidentiality, misuse of NSW SES Information Assets.
- suspicious approach or persuasion to disclose passwords or other Sensitive information.
- loss or theft of removable media or physical documentation.
- illegal material accessed or stored on NSW SES IT resources.
- computer virus or malware.
- misaddressed emails or communication containing Sensitive information.
- unauthorised changes to NSW SES Information Assets.

3 Roles and Responsibilities

Director Information and Communications Technology (CIO)

- Ensure effective implementation of this policy.

Senior Manager Business Systems (CISO)

- Monitoring, evaluation, and reporting of compliance to this policy.
- Conducting periodic reviews of the policy (when significant legislation or organisational changes require an update).

ICT Senior Managers

- Granting exceptions to policies.

Managers and Supervisors

- Ensuring processes are conducted in accordance with this policy.

All members

- Ensuring compliance with this policy.

4 Related Documents

- *Code of Conduct and Ethics* (NSW SES)
- *ICT User Access Policy* (NSW SES)
- *Password Policy* (NSW SES)
- *Records Management Policy Guideline* (NSW SES)
- *Intellectual Property Policy* (NSW SES)
- *Intellectual Property Procedure* (NSW SES)
- *NSW Cyber Security Policy*
- *NSW Government Cyber Security Strategy*
- Privacy and Personal Information Protection Act 1998 (NSW)
- Spam Act 2003 (Commonwealth)
- Government Sector Employment Act 2013 (NSW)
- State Records Act 1998 (NSW)

5 Support and Advice

You can get advice and support about anything in this policy from:

- the Policy Owner – NSW SES Senior Manager Business Systems (CISO).
- the Policy Sponsor – Director Information and Communications Technology (CIO).

6 Definitions

Term	Definition
Data	Any information, regardless of form, contained in or processed by the agency's information systems, communications networks, or storage media. This data may reside in many forms including but not limited to printed copy, magnetic media, microfiche, online storage, physical materials.
Encrypted	Data that has been modified in such a way that only authorised parties can access.
Information systems	Software and hardware which stores, processes, interprets, or communicates information.
Internet	All online services including, but not limited to, the World Wide Web (www), email, newsgroups, chat groups, electronic message boards, social media services and file transfer protocol (FTP).
Removable Media	USB sticks, portable disc drives, DVD ROMs.
Wireless network	A wireless network is a computer network that uses wireless data connections between network nodes.

Document Control Sheet

Title	ICT Acceptable Use
Current Version	2.0
Directorate	Information and Communications Technology (ICT)
Policy Owner	Senior Manager Business Systems (CISO)
Policy Sponsor	Director ICT (CIO)
Effective date	21/02/2024
Next Review Date	21/02/2029
Rescinds	ICT Acceptable Use Policy V1.1 November 2021
Topic	Security
Function	ICT
Key Words	Password, internet usage, electronic communication, monitoring,

Version History

Version #	Creation Date	Author	Summary of changes
1.0	24/02/2020	ICT	Authorised
1.1	23/11/2021	ICT	Administrative changes
2.0	15/11/2023	ICT	SCHEDULED REVIEW - Section 2 overview edited. - Added 2.5c. - Minor edits throughout. - Definitions updated. - Updated policy template.

Approval

Title		Date	Version signed off
Senior Manager Business Systems	Policy Owner	17/11/2023	2.0
Director ICT	Policy Sponsor	27/11/2023	2.0
Damien Johnston	Deputy Commissioner Corporate Services	11/12/2023	2.0
Debbie Platz	Acting Commissioner	21/02/2024	2.0