Mobile Device Policy

Version 2.0
February 2024

1 Purpose and Scope

The purpose of this policy is to:

- Ensure that mobile devices are protected from cyber security risks and other threats that may cause loss or damage to the NSW SES.
- Ensure all users are aware of their responsibilities when working on mobile devices and understand the associated risks.
- Ensure that all users understand their own responsibilities for protecting the privacy, integrity, and availability of the data that they handle remotely.
- Protect NSW SES from liability or damage through the misuse of NSW SES Information and Communications Technology (ICT) assets.
- Provide information security direction for members in the use of mobile electronic devices when travelling overseas, with the aim of protecting digital information, NSW SES and NSW Government IT networks and the reputation of the NSW SES and NSW Government.

This policy applies to:

- NSW SES employees, volunteers, contractors, consultants, temporary and other workers, including third parties.
- Mobile devices connecting to NSW SES systems, whether agency owned, personal, or otherwise, including but not limited to mobile phones, smartphones, wearables, tablets, laptops, portable electronic devices, and other portable internet-connected devices.
- Privacy and physical controls when using mobile devices.

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 mobile device use

1) All users should consider data protection while accessing NSW SES systems remotely or using their mobile device.
2) To ensure confidentiality and integrity, data should be available to individuals based on need-to-know basis.
3) NSW SES will not provide any support or advice for personal devices during normal business situations.
4) Personal device owner is responsible for, voice or data charges, software or application acquisition fees and support or insurance costs.
5) Devices containing agency data that have been stolen must be reported in a timely manner.
6) NSW SES owned devices must be used only for business purposes.
7) All Mobile/remote devices should be protected with the security management software.

2.1 Personal mobile devices

NSW SES recognises some members desire to have the freedom to choose their own mobile device and mobile carrier, and therefore NSW SES have adopted a Bring Your Own Device (BYOD) approach.

The following applies in the circumstances where NSW SES members use a personal device (BYOD) to connect to NSW SES networks and information resources:

a) It is the responsibility of the member to ensure that the device does not present an unacceptable security risk.
b) Permission to access or connect to NSW SES systems via a personal device is subject to management approval and is at the sole discretion of NSW SES.
c) Except by written agreement from Director ICT, NSW SES will not provide any support or advice for personal devices during normal business situations. Acceptations will be made for extraordinary situations i.e., cyber security breach.
d) Device owners are responsible for the security and protection of their devices. Reimbursement or replacement of mobile devices must comply with the *NSW SES Injury Management Procedure*.
e) All costs associated with the use of a personally owned device will remain the sole responsibility of the device owner. These include, but are not limited to, voice or data charges, software or application acquisition fees and support or insurance costs.
f) Personal devices are not to be left logged in to any system which contains NSW SES data.
g) In the event NSW SES suspects a security breach is related to a personal device, the agency may, with or without notice, take all actions deemed appropriate to secure agency or member data and the NSW SES network. Actions may include, but are not limited to, disconnecting the device from the network, action against the individual, seizure of the device or potential legal action.

h) In the case of device theft and or upon termination, all NSW SES data must be remotely and securely wiped where possible.

2.2 NSW SES mobile devices

a) If a member requires an NSW SES mobile device, they are encouraged to discuss this with their manager prior to making a request to ICT.

b) NSW SES may issue personnel with a mobile device to access the organisation's information and systems that do not present an unacceptable security risk.

c) NSW SES devices taken off site are not to be left logged in to any system which contains NSW SES data.

d) All devices which are required to access any NSW SES systems for a task are required to disconnect from NSW SES data sources containing agency data at the end of the access session.

2.3 The use of mobile electronic devices when travelling overseas

a) Any member planning to access NSW SES systems internationally with a mobile device, (including a privately-owned mobile device with BYOD access), must contact the Service Desk for advice at least 30 days prior to any planned international travel. A risk assessment will be conducted to determine the risks associated with the request.

b) There must be a demonstrated need to use the device overseas, i.e., device use must be for official NSW SES business only.

c) These mobile electronic devices must comply with the relevant circular – e.g., Department of Premier and Cabinet Circular C2016-04-Information Security Policy for Ministers, Ministers' Staff, Department Secretaries and Senior Executives Travelling Overseas.

2.4 Privacy notice for personal (BYOD) & NSW SES mobile devices

a) All electronic and telephonic communication systems, including NSW SES email, internet access and NSW SES provided equipment and communication devices, including computers, fax machines, and similar communications devices are the sole property of NSW SES. In addition, any information transmitted by, received from, or stored in such devices, or personally owned BYOD, are the sole property of NSW SES.

b) All messages, data and materials transmitted by, retrieved from, or stored within NSW SES systems shall be regarded as non-personal NSW SES communications or data. NSW SES has, and expressly reserves, the right to inspect any data contained in, received, transmitted by, generated on, or sent to or from a NSW SES system, to any electronic device a staff member has used to access or connect to a NSW SES system whether the device is provided by NSW SES or is personally owned (BYOD) by the staff member. Such an inspection may take place at any time, with or without notice to the staff member, and for any purpose deemed acceptable by NSW SES in its sole discretion.

2.5 Physical security of mobile devices

a) Members must always exercise care when using mobile devices.

b) Mobile devices must not be left unattended in any location where theft is possible.

c) Mobile devices must never be left unattended in motor vehicles except where out of sight.

d) Members are encouraged not to leave their mobile devices unattended at their desk.

e) Members are encouraged to activate a device locking feature.

f) If a device is lost or stolen this must be immediately reported to NSW SES Service Desk and NSW Police. Remediation activities will be immediately performed.

2.6 Prohibited & accepted use of personal & NSW SES mobile devices

a) Members are prohibited from using any mobile device in any manner which may violate any federal, state, or local law, regulation, or ordinance. Members are not authorised to use any mobile device in any unlawful manner. Members are responsible for ensuring that their use of any mobile device complies with all applicable laws.

b) Members are specifically prohibited from using any mobile device for any of the following purposes: unlawful surveillance; wiretapping or eavesdropping; harassment of any person, including sexual, racial, religious, and other forms of unlawful harassment. Whether a mobile device is NSW SES-provided or personally owned (BYOD), uses of such device are for NSW SES business purposes only and are governed by NSW SES policies, including but not limited to, the *NSW SES Code of Conduct and Ethics* and the *NSW SES ICT Acceptable Use Policy*.

c) All users of mobile devices whether provided by NSW SES or personally owned (BYOD), which access or connect to NSW SES systems must diligently protect such devices from loss and disclosure of confidential information belonging to or maintained by NSW SES.

d) Endpoint protection software must be installed on all Laptops before connecting to NSW SES Network.

e) Mobile devices must be enrolled in mobile device management (MDM) prior to be onboarded on NSW SES Network.

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)
- *Cyber Security Policy* (NSW SES)
- *ICT Acceptable Use Policy* (NSW SES)
- *ITSS_01 Encryption Standard* (NSW SES)
- *Injury Management Procedure* (NSW SES)
- *NSW Cyber Security Policy*
- *NSW Government Cyber Security Strategy*

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
Application	Software designed to assist end users to carry out useful tasks. e.g., Microsoft Office.
Availability	Property of something that is accessible and usable only by an authorized person, entity, or process when required.
Asset	Item or property owned by NSW SES.
Bring Your Own Device (BYOD)	Any electronic device personally owned, leased, or operated by an employee or contractor of NSW SES which is capable of storing data and connecting to a network.
Confidentiality	Property of the information that can be accessed or disclosed only to authorized persons, entities, or processes.
Data	Information, (electronic or paper document). Refers to data owned, originating from, or processed by NSW SES systems.
Information security	Processes, methodologies, and technologies with the objective to preserve the confidentiality, integrity, and availability of information.
Information security management	Management of processes that cover the identification of situations that may put information at risk, and the implementation of controls to address those risks and protect the interest of the business and other relevant interested parties (e.g., customers, employees, etc.).
Integrity	Consistent, complete, and free of error (lack of corruption).
Member	Includes all staff, contractors, casual employees, and volunteers.

Term	Definition
Mobile Device	Includes mobile phones, smartphones, wearables, tablets, laptops, portable electronic devices, and other portable internet-connected devices.
Mobile Working	Carrying out work (i.e., the creation, storage, processing and transport or transfer of data/ information) as an employee of NSW SES from outside of NSW SES premises.
Wearables	A small computer or advanced electronic device that is worn or carried on the body. E.g., watches, fitness monitors, etc.
Wipe	A security feature that renders the data stored on a device inaccessible.

Document Control Sheet

Title	Mobile Device Policy
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	Mobile Device Policy V1.0 February 2020
Topic	Cyber Security
Function	Information and Communications Technology
Key Words	Protect, Remote Access, Mobile Access, BYOD, Bring Your Own Device

Version History

Version #	Creation Date	Author	Summary of changes
1.0	24 February 2020	Policy Team	Authorised
2.0	15/11/2023	ICT	SCHEDULED REVIEW - Principles reworded into actionable sentences. - Added 2.2h, 2.7d, 2.7e. - Minor edits throughout. - Related documents 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	21/02/2023	2.0