ICT User Access Policy

Version 2.0
February 2024

1 Purpose and Scope

The purpose of this policy is to ensure the protection of NSW SES' information assets through the establishment of user access controls. These controls provide members with authorised access to information systems, data, and assets in line with their role requirements and the context in which access to systems, information and processes is controlled, restricted and managed.

This policy applies to:

- User access controls and user access management of all accounts on any NSW SES information systems, data, and assets.
- All users of these accounts, including but not limited to: ○ Staff (ongoing, temporary and agency); volunteers, contractors, and consultants.
    - ○ Vendors supporting IT systems. ○ Partner business and government agency employees.
    - ○ Visitors to 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 user access

1) Access to information assets must be driven by requirements. These requirements must be translated into controls which deliver appropriate and enforceable access management.
2) Requests for user accounts must be formally submitted via the NSW SES service desk and documented and appropriately approved by the information asset owner, delegate, or where acceptable, the supervisor.
3) Dormant or inactive accounts must be deactivated or disabled, and access rights must be removed as soon as practicable.

2.1 Access control

1) Access to information assets must be driven by requirements. These requirements must be translated into controls which deliver appropriate and enforceable access management.
2) Access control is provided based on the principle of limited privilege and a 'need to know' basis.
3) Access controls in systems correspond to risk management objectives.
4) Access to information and resources must be granted in a controlled manner. Appropriate approval from the information asset owner, delegate, or where acceptable the requestor's supervisor, must be sourced prior to the delivery of access.
5) Where possible, the principle of 'least privilege' should be applied to ensure individuals have appropriate access to only the information required to conduct their role.
6) Ensure segregation of duties is applied.

2.2 User access management

1) Requests for user accounts must be formally submitted via the NSW SES service desk and documented and appropriately approved by the information asset owner, delegate, or where acceptable, the supervisor.
2) Accounts must be registered in such a way that they uniquely identify the user.
3) User registration and de-registration of access must be implemented and documented when granting or revoking rights:
    a) Authorisation from appropriate management to perform the registration or deregistration must be recorded.
    b) Verification that the registration or de-registration action has been performed correctly must be recorded.
4) These documents must be kept for an acceptable period and comply with the NSW SES Records Management Policy.
5) Access to NSW SES information resources must be authorised by the information asset owner or delegate prior to access being provisioned. It is the responsibility of the information asset owner to ensure that access privileges: a) are aligned with the needs of the business,
    b) meet the information management requirements,
    c) are assigned on a need-to-know basis, and
    d) are communicated to custodians.
6) Procedures for access provisioning must:
    a) be documented step-by-step.
    b) ensure that access requests and approvals are documented.
7) Removal and/or adjustments of a user's access rights must be documented and follow an approved process with appropriate approvals.
8) All users requiring privilege access for a temporary period for a specific task, are required to obtain approval from the information asset owner or delegate.

9) Request for privilege access must be formally documented and approved by the system and or business process owner.

10) Frequency of auditing user access will be based on the system's risk profile.

2.3 Managing dormant and inactive accounts

1) Accounts which are inactive for 90 days will be automatically deactivated unless otherwise specified.

2) Dormant accounts must be disabled after defined retention period has expired.

3) Access rights will be disabled or removed as soon as practicable when the user's role is terminated or ceases to have a legitimate reason to access NSW SES systems.

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.

Information Asset Owner and/or Delegate

- Ensuring processes are conducted in accordance with this policy.

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)
- *ITSS_04 Identity & Access Management Standard* (NSW SES)
- *Records Management Policy* (NSW SES)
- *Records Management Policy Guideline* (NSW SES)
- *NSW Cyber Security Policy*
- *NSW Government Cyber Security Strategy*
- Government Sector Employment Act 2013 (NSW)
- Privacy and Personal Information Protection Act 1998 (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
Administrator	A user account with privileges that have advanced permissions on an IT system necessary for the administration of the system.
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.
Data owner	A Senior Manager or functional owner responsible for a system, application, or business process, who has responsibility for the quality, integrity, and security of the data.
Information	Any collection of data that is processed, analysed, interpreted, classified, or communicated to serve a useful purpose. Information is typically considered to be at a higher level of abstraction than Data.
Information security	Processes, methodologies, and technologies with the objective to preserve the confidentiality, integrity, and availability of information.
Information system	Software and hardware which stores, processes, interprets, or communicates information.
Term	**Definition**
IT assets	Any device or service that connects to, or is used by, NSW SES in its business, research, training and learning activities such as a data link, physical device, application (including firmware), database and middleware.
Privilege access	Privilege access refers to user accounts with elevated authority over a computer system such as administrators or superusers.
User access controls	An approach to restricting system access to authorised users.

Document Control Sheet

Title	ICT User Access 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	ICT User Access Policy 1.0 October 2020
Topic	Security
Function	ICT
Key Words	User Access, Privilege Access, Access Controls

Version History

Version #	Creation Date	Author	Summary of changes
1.0	27/10/2020	ICT	Authorised
2.0	15/11/2023	ICT	SCHEDULED REVIEW - Principles reworded into actionable sentences. - Added 2.3.1 and 2.3.2. - Added section 2.3. - Minor edits throughout. - 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