ITSS_05 IT Security Standard – User Access

Version	Approved by	Approval date	Effective date	Next review date
1.1	Administrative update by the Director of Governance	17 January 2017	17 January 2017	7 June 2017

Standard Statement		
Purpose	User access must be provided according to the principles of “least privilege” and "need to know" required for achieving the desired function. The purpose of this Standard is to set out the rules under which access to UNSW information systems are provided, controlled and managed. UNSW has established and follows specific access control practices to protect their information and systems from unauthorised access; modification, disclosure or destruction and to ensure that information remains accurate, confidential, and is available when required. Information systems include: • Operating Systems. • Applications. • Databases. • IT services such as Internet and email. • Network Equipment (e.g., firewalls, routers, switches etc) and infrastructure appliances.	
Scope	This standard applies to all users of UNSW Information and Communication Technology resources – including (but not limited to) staff (including casuals), students, consultants and contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments and visitors to UNSW.	
Are Local Documents on this subject permitted?	☐ Yes, subject to any areas specifically restricted within this Document	☐ No
Standard		

1. Controls

1.1 Access Control

1.1.1 On a per service basis and where practical, access to UNSW information systems must be controlled by a centralised Authentication, Authorisation and Accounting system, (i.e. TACACS for network infrastructure or Active Directory windows domains).

1.1.2 Locally authenticated accounts are not permitted unless a valid academic, business or technical justification has been assessed and approved via the risk management process.

1.1.3 In line with this standard, access control requirements process and procedure must be developed to manage locally authenticated accounts.

1.2 General Access Provisioning and De-provisioning

1.2.1 All accounts must be associated with an owner i.e. one to one relationship and where possible assign to a group.

1.2.2 Access requests are approved by an appropriate authority (individual's manager) prior to implementation by the IT systems and application administrators.

1.2.3 Where possible, the following access control models must be considered and implemented for user authentication. For example: Role Based Access Control (RBAC) to allow UNSW users to access information systems based on their role (e.g., prospect, student, alumni, academic staff) inheriting a pre-defined set of access rights.

1.2.4 Account and relative access rights must be removed or disabled when a user no longer needs access due to changing roles or leaving UNSW.

1.2.5 Accounts for UNSW contractors must always have an expiration date aligned with the contract period.

1.2.6 In case of an emergency (i.e. third party vendor requires access during a severity 1 situation) access requests are approved and documented retrospectively.

1.2.7 For applicable systems, owners or delegates must perform annual account revalidation to validate continued business need with the authorising authority. Accounts assigned to individuals in perpetuity such as "alumni" are exempt from annual revalidation.

1.2.8 The authenticating systems (i.e. TACACS, Active Directory) should reflect the current list of approved individuals.

1.3 Generic Accounts

1.3.1 Shared or generic accounts are not permitted unless a valid academic or business, justification has been assessed and approved via the risk management process.

1.3.2 For shared or generic accounts a process must be deployed and documented to detail purpose, ownership, accountability and security:

a) A responsible focal point is assigned to manage the account.

b) Purpose of account use, such as, short course accessing system XYZ.

c) Names and contact details of individuals using the account.

d) Duration of account use i.e. temporary or permanent.

e) Account passwords are reset when any individual no longer has a valid need to use the account.

f) Business or academic need of the account and associated individuals must be revalidated annually.

1.4 Remote User Access

1.4.1 All remote access requests used to connect to UNSW's information systems must be approved by an appropriate authority (e.g., individual's manager). Remote access to UNSW's information systems must be strictly controlled and implemented according to the Network Security Standard. Remote access is subject to the following restrictions:

a) Users are securely authenticated (via a username/password pair or where applicable using an additional, second authentication method such as PIN or smart card) prior to the establishment of a remote connection.

b) "Highly Sensitive", "Sensitive", and "Private" data must be encrypted when the data is transferred through public networks (i.e., Internet).

c) Remote access accounts with privileged rights for administrative use must be limited to authorised personnel and strictly controlled via:

- Two-factor authentication i.e. smart card, soft token or PIN.
- Regular monitoring of event logs.
- Periodic reviews, at least annually, of access rights to verify the ongoing appropriateness of access rights.

d) Users must not attempt to circumvent remote access (VPN) security controls. Any deviations must be addressed from a risk perspective and approved by the remote access and end point system business owner.

1.5 Federated User Access

Federated access to allow UNSW to reuse identities and simplify user account management.

1.5.1 Trusted third parties must be selected as federated partners.

1.5.2 UNSW must retain control over the access rules for granting access to the sensitive information it owns. Please refer to the "Federation Governance Document" for direction.

1.6 User Accountability

1.6.1 All UNSW users are personally responsible for the use of their account and must:

- Select and use strong passwords.
- Change their password if they know or suspect that their account has been compromised.
- Keep passwords secure, and not reveal them under any circumstances.
- Not attempt to use any account other than their own, unless for legitimate support or security incident purposes.
- Not share their user account with other individuals.

1.7 Account Management

1.7.1 UNSW staff and contractors are assigned with a single user identifier to be used when accessing UNSW's information systems (e.g., default z-ID).

1.7.2 A standard Naming Convention scheme is followed when creating accounts in order to facilitate the accountability of user actions.

1.7.3 User account management controls must be established to lock user accounts after a defined number of failed authentication attempts:

Account Management Characteristics	Account Management Policy
Account lockout threshold	Ten (10) consecutive invalid password attempts
Account lockout duration	Thirty (30) minutes
Account inactivity lockout	Note: This must be determined according to the account type (e.g., student, alumni, staff & academic staff) and detailed within the IDAM process documentation.
Maximum user screen lock out inactivity	The maximum user inactivity timeout, requiring password re-entry, thirty(30) minutes

**The above account management policy requirements apply to all UNSW staff and students as well as privileged/administrator users.*

1.8 Password management

1.8.1 Passwords are mandatory for all user accounts on all networked and standalone information systems including operating systems, applications, databases, end user computing hardware and mobile devices (notebooks, tablets etc):

Password Management Characteristics	Password Policy
Minimum length ensuring passwords are not easily derived.	Minimum Eight (8) and a recommended Fourteen (14) characters or more and;
Complexity ensuring passwords are not easily derived.	A Password must comply with any Three (3) of the following: • *Minimum* One (1) Alpha (upper) • *Minimum* One (1) Alpha (lower) • *Minimum* One (1) Numeric

	characters • *Minimum* One (1) Special character (e.g., %,#) And; • NOT contain *Account Name*, First name, Surname or Full Name.
Maximum password age limiting the utility of a breached password.	One hundred and eighty (180) days
Minimum password age to prevent users from reverting to their old password immediately after an enforced password change.	Five (5) days
Password history to prevent users from reusing their twelve (12) previous passwords.	Twelve (12) passwords

**The above password policy requirements apply to all UNSW staff and students as well as privileged / administrator.*

1.8.2 Where technically feasible, users must change their password at first logon.

1.8.3 Passwords must not be displayed "in the clear" on input and fixed screens, hard copy reports or electronic files.

1.8.4 Default passwords shipped with any information system must be immediately changed upon installation of the software.

1.8.5 Passwords must not be based on anything that can be easily guessed or obtained using collateral information. The following must be avoided:

a) Passwords related to Names, Date of Birth, Telephone Numbers, Family information, etc.

b) Common words found in dictionaries.

c) Common words or terms; relating to UNSW.

1.9 Privileged User Access Management

1.9.1 For the purpose of this Standard the following definitions have been used for IT specific user accounts:

IT User Accounts	Description
Privileged accounts	A personalised account that has elevated access rights to information systems to perform administrative activities
Functional accounts	Default accounts provided from software vendors such as Administrator, Guest, Root, DBA, Built In, Hardcoded
System accounts	Accounts used for system to system communication such as Oracle Listener, Nagios, TACACS pre-shared keys, IPSEC pre-shared keys, SNMP strings.
Service accounts	Group mailbox accounts. Approved shared or generic accounts.

1.10 Privileged accounts

1.10.1 Privileged access enables certain users to perform administrative and maintenance tasks on UNSW information systems. Privileged access to an information system must be provided to users only if they have a need for such access as part of their job responsibilities and UNSW business needs.

1.10.2 Every privileged account must have a one-to-one relationship with an individual.

1.10.3 Privileged access rights must be controlled via two-factor authentication (i.e., smart card, soft token or PIN).

1.10.4 In the event a staff member, who has privileged access, has resigned or is terminated the account must be disabled within a reasonable timeframe consummate with the level of perceived risk and documented within ID Access Management (IDAM) process and procedure.

1.11 Functional accounts

1.11.1 The ownership and business purpose of functional accounts must be documented and maintained.

1.11.2 Where technically possible, functional account privileges (root) must be substituted i.e. assigned to an individual (Linux Sudo rights). Where not, functional accounts (hardcoded) must be afforded the same controls as generic accounts (2.3.2 b, c, e and f).

1.12 System accounts

1.12.1 The ownership and technical purpose of system accounts must be documented and maintained and only made available to individuals with a valid technical need.

1.12.2 Management of system account "passwords" or "pre shared keys" used to authenticate or encrypted inter system communication must be considered from a risk perspective. Appropriate controls must be selected to mitigate potential the breach of access.

1.13 General

1.13.1 Consideration from a risk perspective to segregation of duties must be afforded and documented within the system design documentation.

1.13.2 Access controls are established such that system users/administrators are not able to modify critical system data (for example event logs).

2. Control Exceptions

All exemption requests must be reviewed assessed, and approved by the relevant business stakeholder. Please refer to the ISMS Base Document for more detail.

3. ISMS Mapping with Industry Standards

The table below maps the ITSS_05 User Access Management Standard with the security domains of ISO27001:2013 Security Standard and the Principles of Australian Government Information Security Manual.

ISO27001:2013	Information Security Manual
9 Access Control	Access Control

4. Document Review, Approval & History

This section details the initial review, approval and ongoing revision history of the standard. Post initial review the standard will be presented to the ISSG recommending the formal UNSW policy consultation and approval process commence.

A review of this standard will be managed by the Chief Digital Officer on an annual basis.

4.1 Quality Assurance

This document was designed and created by external and internal consultants in consultation with internal key technical subject matter experts, business and academic stakeholders.

4.2 Sign Off

Endorsement	Date
ISSG - Information Security Steering Group	30th July 2015
ITC - Information Technology Committee	27th August 2015
CDO – Chief Digital Officer	7th June 2016

Accountabilities	
Responsible Officer	Chief Digital Officer
Contact Officer	ITpolicy@unsw.edu.au
Supporting Information	
Parent Document (Policy)	IT Security Policy
Supporting Documents	Nil
Related Documents	Data Classification Standard Data Handling Guidelines ISMS Base Document
Superseded Documents	Nil
UNSW Statute and / or Regulation	Nil
Relevant State / Federal Legislation	Nil
File Number	2016/16925 [ITSS_05]
Definitions and Acronyms	
No terms have been defined	

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-President, Finance and Operations	7 June 2016	7 June 2016	This is a new document
1.1	Administrative update by the Director of Governance	17 January 2017	17 January 2017	Section 1.8.1 – corrected and reordered for clarity.