1 IDENTITY AND ACCESS MANAGEMENT STANDARD

Title	Identity and Access Management Standard
Reference	ISS-01
Status	PUBLISHED
Version	1
Date	October 2023
Review	TBD
Classification	Public

2 SUMMARY

This standard is part of the University's Information Security Policy and sets out the requirements for the effective management of identities, accounts, and access rights. This management is essential to ensure that access to the University's information and information systems is restricted to authorised users.

limit access to Information Assets to authorized users or groups of users and to audit, authenticate, monitor, and control this access.

ensure that users can access only the information and computer resources needed to do their job or conduct business.

ensure actions taken on the Enterprise's networks or involving our information can be traced back to an individual.

all other applications and infrastructure as substantive changes

3 SCOPE

All information systems used to conduct University business, or which are connected to the University network, must be managed in accordance with this standard. This Standard applies to:

a. all university constituents
b. applications, services, and infrastructure designated as being subject to the Standard.
c. systems, applications, and infrastructure connected to the university network.
d. information assets that have been deemed, through the Information Classification process, to require a degree of protection.

Whenever circumstances or technologies make immediate compliance with this Standard impractical, the exception process outlined in the Information Security Policy will be used.

4 STANDARDS

4.1 ACCOUNTS MUST BE ASSIGNED TO ELIGIBLE INDIVIDUALS.

Accounts will only be issued to those who are eligible for an account and whose identity has been verified using approved credentials. User accounts will only be provided for:

a) Current university staff, and active students.
b) Emeritus staff and those who have otherwise been granted honorary or associate status (associates will include staff from other organisations which provide services to the University who may require access to the University's information systems to fulfil their contractual obligations to the University.)
c) Students waiting to graduate.
d) Guests of the University who may be granted temporary access to the University's network.
e) Retired staff who are permitted email accounts granted by the collective agreement.

4.2 ASSIGN ACCOUNT WITH A UNIQUE IDENTIFIER.

When an account is created in the authoritative system of record, a unique identifier (userID) will be assigned to the individual user for their individual use. This userID may not be assigned to any other person at any time (userID's will not be recycled).

Each user on a production system must be issued a unique ID and password. Shared user accounts may only be issued for non-production systems (e.g. systems in development and testing, IDs used for training on isolated systems).

4.3 ADMINISTRATION

The management of user accounts and privileges on the University's information systems is restricted to trained and authorised members of staff.

4.4 ACCOUNT MANAGEMENT

1. Users (including temps, consultants, and contractors) shall formally request access to systems with only the rights necessary to perform their job functions.
2. A manager or above and the system owner shall formally approve user roles and access requests. System administrators shall act as the final gatekeeper to ensure access is granted appropriate to the identified role.
3. Usernames shall follow a consistent naming methodology to allow for proper attribution (e.g., generally consisting of the first initial and first five letters of the user's surname).
4. Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (e.g. when a member of staff changes their role or a member of staff or student leaves the University).
5. Avoid assigning security rights that copy one user's rights to another user.

6. Periodic review of users' access and access rights shall be conducted to ensure rights are appropriate for the users' role.
7. Inactive user accounts are to be reviewed and disabled and/or removed every ninety (90) days. Exceptions shall be documented, reviewed, and approved by Information Security.
8. Enable accounts used by vendors are only active during the period required. Ensure vendor activity is monitored where appropriate.
9. Ensure minimal, controlled use of administrator, local administrator, enterprise admin, and/or schema admin profiles.
10. Ensure that the Principle of Least Privilege using role-based access control (RBAC) is followed for all users.
11. Control and monitor addition, deletion, and modification of usernames, credentials, and other identifier attributes on accounts.
12. Remote access to UFV networks shall only to be granted to personnel and/or authorized third parties and shall use two-factor authentication (TFA) or multifactor (MFA) authentication.

5 PRIVILEGED ACCOUNT STANDARDS

Privileged accounts are accounts used for the administration of information systems and are distinct from user accounts. These accounts must only be used by system administrators when undertaking specific tasks which require special privileges. System administrators must use their user account at all other times.

5.1 PROVIDE ADMINISTRATIVE USERS WITH UNIQUE PRIVILEGED ACCOUNTS.

Users who regularly require elevated access privileges on a system must be provided with a unique account that has been assigned these privileges. This account must:

a) specify the purpose of the account in the identifier (e.g. by prefacing the ID with "admin"),
b) be used only for situations that require the use of the assigned privileges.

5.2 RESTRICT PRIVILEGED USER ACCESS ON INFRASTRUCTURE.

Privileged users must be given access only to the commands necessary to accomplish their function.

5.3 LIMIT DEVELOPER ACCESS TO PRODUCTION ENVIRONMENTS.

Developers must not have administrator or change access to the production environment. If necessary for on-call troubleshooting and code releases, a formal process must be defined for allowing such access.

5.4 LIMIT ACCESS TO THE ADMINISTRATOR ROLES ON WORKSTATIONS.

Workstation user accounts must not be provided with local administrator rights.

5.5 REVIEW THE ACTIONS OF PRIVILEGED USERS

Controls must be applied to privileged users (e.g. ‘administrators’, ‘root’, or application users with privileges beyond those of typical users), which include:

a) logging of all actions taken by an individual with root or administrative privileges,
b) reviewing the use of special access privileges for suspicious activity regularly - at least weekly.

5.6 ASSIGN OWNERSHIP FOR SHARED PRIVILEGED ACCOUNTS.

Privileged accounts are any accounts that have control over the administration of an application, device, or operating system. Administration includes the ability to manage users, change configuration settings, and/or modify security policies or controls.

These accounts must be owned by a senior leader or other, as delegated by the Information or Infrastructure Owner, who must:

a) assume accountability for the use of the account,
b) inform users of these accounts of their obligations to conform with all relevant policies and standards,
c) maintain a central register of shared administrator accounts they own.

5.7 CONTROL THE USE OF SHARED PRIVILEGED ACCOUNTS.

Additional controls must be applied to shared administrator accounts (e.g. ‘root’ in UNIX or ‘administrator’ in Windows systems), which include:

a) restricting their use to narrowly defined circumstances and times,
b) requiring individual approval for their use (e.g. by a sufficiently senior business representative),
c) logs must be kept determining which users have access to the account at any given time,
d) local administrator account passwords must be different across servers in different security zones,
e) being managed by a privileged account management (PAM) tool if available.

5.8 CONTROL BATCH / SYSTEM ACCOUNTS.

Accounts used for batch / system processing must be:

a) application specific,
b) restricted to only those functions required to run batch processing,
c) non-interactive where supported by the technology,
d) limited to a specific IP where appropriate,
e) protected by securing credentials that may be stored in batch processes.

1. Administrators shall only log into systems with user ids attributable to them or follow processes that would not break attribution. For example, administrators shall use the su command to obtain root privileges, rather than login as root onto UNIX or Linux systems.

2. Access to databases containing Personal Data, or PII shall always be authenticated. This includes access by applications/services, administrators, and all other users or sources.
3. All access shall be removed for users who administer or operate systems and services that process Personal Data and PII where their user controls are compromised (e.g., due to corruption or compromise of passwords, or inadvertent disclosure).
4. The reissuance of de-activated or expired user IDs for systems or services that process Personal Data and PII shall not be permitted.
5. Where possible no one person will have full rights to any system. The I.T. Department will control network/server passwords and system passwords will be assigned by the system administrator in the end user department.
6. The system administrator will be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.
7. Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number/biometric.
8. Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster, for example a fire safe in the I.T. Department.

5.9 ACCESS CONTROL POLICY

a) Integrity and confidentiality of data shall be maintained through discretionary and mandatory access controls as applicable.
b) Establish process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.
c) IT Department shall be notified of all personnel leaving the University by human resources prior to or at the end of their employment. As soon as possible after notification, not to exceed twenty-four (24) hours, rights to all systems shall be removed unless a specific exception request is received from HR, Legal or Information Security.
d) All logins shall be secured through an encrypted connection (e.g., HTTPS, ssh) and appropriately authenticated.

5.10 PROVIDE APPROPRIATE AUTHORIZATION CONTROLS.

Applications and infrastructure must employ appropriate authorization mechanisms to provide or limit access to the Information Assets and applications' functions based on the role of the individual and the confidentiality of the Information Assets (i.e. role-based access control).

5.11 LIMIT DIRECT ACCESS TO PRODUCTION DATA.

Direct access to production data must be limited by:

a) ensuring that business rules are consistently applied by only allowing application users access to production data/databases via the application interface,
b) restricting direct access to production data by application users,
c) only permitting production support and/or administrator access to production data through the DBMS to ensure proper controls, logging and accountability are in place.

5.12 PREVENT THE COMPROMISE OF USER CREDENTIALS

User credentials must be protected against compromise via social engineering or brute force attacks by:

a) filtering access to known phishing web sites,

b) filtering inbound email for suspicious content (e.g. phrases associated with malware, phishing attacks or known undesirable websites),

c) verifying the source IP address of senders' emails (e.g. using an email validation system such as the Sender Policy Framework or Sender ID that check the Domain Name System (DNS)) to limit spoofing,

d) limiting access to Internal distribution lists by external parties unless explicitly required.

1. The I.T. Department will be notified of all employees leaving the University's employment. The I.T. Department will then remove the employees' rights to all systems.
2. Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster.
3. Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.
4. I.T. Department staff will not login as root on to UNIX, Linux systems, but will use the 'su' command to obtain root privileges.
5. Use of the 'administrator' username on Windows is to be restricted.
6. Default passwords on systems such as Oracle and SQLServer will be changed after installation.
7. On UNIX and Linux systems, rights to rlogin, ftp, telnet, ssh will be restricted to I.T. Department staff only.
8. Where possible users will not be given access to the UNIX, or Linux shell prompt.
9. Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the I.T. Department.
10. File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and File scan rights to directories, files will be flagged as read only to prevent accidental deletion.

5.13 ACCESS CONTROL POLICY

1. Integrity and confidentiality of data shall be maintained through discretionary and mandatory access controls as applicable.
2. Establish process for linking all access to system components (especially access with administrative privileges such as root) to each individual user.
3. IT Department shall be notified of all personnel leaving the University by human resources prior to or at the end of their employment. As soon as possible after notification, not to exceed twenty-four (24) hours, rights to all systems shall be removed unless a specific exception request is received from HR, Legal or Information Security.
4. All logins shall be secured through an encrypted connection (e.g., HTTPS, ssh) and appropriately authenticated.

6 ACCESS REVIEW STANDARDS

6.1 REVIEW AUTHORIZED APPROVERS.

The list of authorized access approvers must be reviewed at least annually by the Information Owner. Information Owners and Infrastructure Owners must review and validate users with access to Information Assets.

The list of users with access to information assets must be reviewed:

a) to ensure that access privileges remain appropriate,
b) to check that redundant authorizations have been deleted (e.g. for individuals who have changed roles or are no longer active),
c) on a regular basis - at least every 12 months,
d) every 6 months for privileged users.

6.2 REVIEW USER ACCESS LOGS FOR SUSPICIOUS ACTIVITIES.

Access control event logs must be reviewed:

a) at least monthly for critical systems,
b) at least daily for systems in scope for Payment Card Industry (PCI),
c) to identify, investigate and escalate suspicious activities (e.g. multiple failed authentication events, off-hours access, changes in privileges).