

Access Control Policy

DOCUMENT CLASSIFICATION	[PUBLIC / CYHOEDDUS]
DOCUMENT REF	USW-ISMS-DOC-A09-1-EN
VERSION	1.1
DATED	01 June 2023
DOCUMENT AUTHOR	Jon Phillips, Senior Information Security Analyst
DOCUMENT OWNER	Ross Davies, Chief Technology Officer Ian Anderson, Head of Core Technology
REVIEW BY DATE	01 June 2025

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	17 May 2022	Ross Davies	ISSG Review
1.1	01 JUN 2022	Jon Phillips	Removal of password complexity requirements

Approval

NAME	POSITION	APPROVER	DATE
ISSG	ISSG Chair	Mark Milton	01/06/2023

Contents

1	Introduction.....	4
1.1	Scope Statement.....	4
1.2	Roles & Responsibilities	5
2	Business requirements of access control	6
3	User access management	7
3.1	User registration and deregistration	7
3.2	User access provisioning	8
3.3	Removal or adjustment of access rights	8
3.4	Management of privileged access rights	9
3.5	Permissible Authentication Mechanisms	10
3.6	User authentication for external connections	10
3.7	Third-party remote access.....	11
3.8	Review of user access rights	11
3.9	User authentication and password policy	12
3.10	Administrative Accounts and Password Policy	13
3.10.1	Administrator User Accounts	13
3.10.2	System/Service Accounts	13
3.11	Logging and Monitoring of Authentications	14
4	Principles of Security Control	14
5	Policy Exceptions	15
6	User responsibilities.....	15
7	System and application access control.....	16
8	ISMS Conformance.....	17
8.1	Areas of ISO/IEC 27001:2013 addressed.....	17
8.2	Related Policies and Regulations	17
8.3	Compliance.....	18

Tables

Table 1: Passwords policy.....	12
Table 2: Administrator account passwords policy.....	13

1 Introduction

The control of access to USW's information assets is a fundamental part of a defence in depth strategy to information security. If the University is to effectively protect the confidentiality, integrity and availability of its data then it must ensure that a comprehensive mix of physical and logical controls are in place.

Our policy regarding access control must ensure that the measures we implement are appropriate to the business requirements (flexible/hybrid studying and working) for protection and are not unnecessarily strict.

These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service
- Relevant legislation that may apply e.g. the Data Protection Act 2018 and UK GDPR
- The wider regulatory framework in which the University of South Wales and its systems operate
- Contractual obligations to external third parties
- The threats, vulnerabilities and risks involved
- The University's appetite for risk

This access control policy is designed to take account of the business and information security requirements of the University and is subject to regular review to ensure that it remains appropriate.

The business and information security requirements set out in this policy:

- Define standards for connecting to the University's network from any authorised device and its location.
- Protect the University from damage which may result from unauthorised access to resources. Damage includes the loss of sensitive or USW confidential data, intellectual property, damage to public image, damage to critical university internal systems, etc.
- Protect all information networks, regardless of connectivity, whether USW-owned, leased, or contractor operated, from unauthorised access.

1.1 Scope Statement

This control applies to those with affiliation to the University who have or are responsible for an account (or any form of access that supports or requires authentication) on any system that:

- resides at any University of South Wales facility
- provides cloud-based services (IaaS/PaaS/SaaS) supporting University of South Wales activities

- has access to the University of South Wales network
- stores any non-public University of South Wales information

together with the owners and administrators of the systems such accounts provide access to.

University of South Wales affiliates include all colleagues, students, governors, suppliers, contractors, and other third parties accessing university information assets (including email and Office files), systems, and network infrastructure regardless of whether their client device is university-owned or otherwise.

This policy applies to remote access connections used to do work on behalf of the University including reading or sending e-mail and viewing Intranet web resources. This policy applies to all individuals and software programs that access or administer access to information resources.

1.2 Roles & Responsibilities

IT Services Information Security Team: responsible for maintaining and updating this policy; periodic monitoring of access events; detection, investigation and resolution of anomalies and incidents; provision of consultation to other teams and departments regarding access management.

IT Services System Administrators: responsible for collaborating with HR and managers for issuing/terminating access to USW's corporate network to employees.

Human Resources Team: responsible for communicating relevant employee lifecycle events that affect colleague accounts (e.g. employment, role changes, and termination) to IT Services processes.

Academic Registry: responsible for communicating relevant student lifecycle events that affect student accounts (e.g. enrolment, course/module changes, and graduation) to IT Services processes.

The IT Customer Support Team: responsible for providing end-user guidance and assistance to queries and issues in respect of their compliance to this policy.

System Business Owners: An IT system is the combination of infrastructure and software implemented to provide services meeting a set of business requirements. The system may be hosted on USW premises, in the cloud, or a combination. The business owners of these systems are responsible for requesting user privileges and third-party accounts on the systems they own.

End-users: this includes colleagues, students and any other person given a USW IT account. It is the responsibility of every end-user to comply with this policy. Any system to which they are granted access must only be used for tasks and to access data to which they have been authorised.

2 Business requirements of access control

Business requirements for access control must be established as part of the requirements-gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design.

Information security requirements concerning access control must be clearly stated within the requirements specification and service design documentation of any system or service. and must take account of the University's secure system development standards.

In addition to the specific requirements, several general principles will be used when designing access controls for the University of South Wales systems and services.

These are:

- **Defence in Depth:** security must not depend upon any single control but be the sum of a number of complementary controls
- **Least Privilege:** the default approach taken must be to assume that access is not required, rather than to assume that it is
- **Need to Know:** access is only granted to the information required to perform a role, and no more. For example a lecturer may have legitimate requirements to access data on the students they teach but not those belonging to an unrelated faculty.
- **Need to Use:** users will only be able to access physical and logical facilities required for their role. For example a student accessing their record may be able to view and modify their contact details but only view their assessment grades.

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities and therefore the number and severity of security incidents that occur.

As part of the selection of cloud service providers specifically, the following access-related considerations must be taken into account:

- User registration and deregistration functions provided
- Facilities for managing access rights to the cloud service
- To what extent access to cloud services, cloud service functions and cloud service customer data can be controlled on an as required basis
- Availability of multi-factor authentication for accounts
- Procedures for the allocation of secret information such as passwords

Addressing these requirements as part of the selection process will ensure that the provisions of this policy can be met in the cloud as well as within on-premises systems.

3 User access management

In this section standard end-users are directed to sections 3.9 and 3.11.

Formal user access control procedures must be documented, implemented and kept up to date by system owners for each application and information system they are responsible for to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks and only used for these activities.

3.1 User registration and deregistration

User accounts for access to the University's network and computer systems must undergo an approval process according to a formal procedure that ensures that correct authorisation is obtained prior to user account creation.

Due to fundamental differences in the business requirements and use cases, standard operating procedure(s) must cover the creation, update, permission assignment, and removal of the following account types:

- colleague accounts.
- student accounts.
- Any other user accounts.
- System administrator accounts.
- O365 Guest accounts.
- Test accounts.
- Remote support accounts.
- Open Day / Visitor / Applicant accounts.

Where user accounts are manually created, the principle of segregation of duties should apply so that the creation of the user account and the assignment of permissions are performed by different people.

Each user account must have a unique username that is not shared with any other user and is associated with a specific individual i.e. not a role or job title.

Generic user accounts i.e. single accounts to be used by a group of people **must not** be created as they provide insufficient allocation of responsibility and issues around non-repudiation of user activity.

An initial strong password must be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account.

When a colleague leaves the University under normal circumstances, their access to computer systems and data must be suspended at the close of business on their last working day.

In exceptional circumstances e.g. where there is perceived to be a significant risk that the colleague may take action that may harm the University prior to or upon termination, a request to remove access may be approved and actioned in advance of notice of termination being given. Approval for this must be given by both the relevant HR business partner and Compliance department. This precaution will especially apply in the case where the individual concerned has privileged access rights e.g. a domain administrator.

Acknowledging student accounts are a specific use case and constitute the majority of user accounts, a defined process must be in-place for rescinding access to university computer systems and data for student accounts.

User accounts must be initially suspended or disabled only and not deleted. User account names must not be reused as this may cause integrity issues, particularly in the event of a later investigation.

3.2 User access provisioning

Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the activities they are expected to perform. In general, this will be role-based i.e. a user account will be added to a group that has been created with the access permissions required by job role, academic course etc.

Group roles must be maintained in line with business requirements and any changes to them must be formally authorised and controlled via the Joiners Movers Leavers (JML) process.

Ad-hoc additional permissions must not normally be granted to user accounts outside of a group / role assignment; if such permissions are required this must be addressed as a change to existing group / role permissions or creation of a new group or role.

Access permissions based on roles and group memberships is a relatively new paradigm for the University to implement, formalised in this policy for the first time. It does not invalidate prior practices around access provisioning.

3.3 Removal or adjustment of access rights

Where an adjustment of access rights or permissions is required e.g. due to an individual changing job role or academic course, this must be carried out as part of that JML process.

For colleagues, it must be ensured that access rights no longer required as part of the new role are removed from the user account. If a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role must be requested by their

Line Manager / IT Coordinator via JML process. Due consideration of any issues of segregation of duties must be given.

Under no circumstances are administrators permitted to change their own user accounts or permissions.

3.4 Management of privileged access rights

Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled by system owners.

In general, technical users (such as IT support colleagues) must not make day-to-day use of user accounts with privileged access, rather a separate “admin” user account must be created and used only when the additional privileges are required. These accounts must be specific to an individual; generic admin accounts must not be used as they provide insufficient identification of the privileged user.

Access to admin level permissions must only be allocated to authorised individuals whose roles require them and who have received enough training to understand the implications of their use. Such accounts must utilise multi-factor authentication wherever possible. Business Owners are responsible for the appropriate authorisation ensuring it is in line with the requirements set out in this policy.

A formal record must be maintained detailing individuals who have been given access to systems at an “administrator” level together with the relevant account name(s). Authorisation for such individuals must be controlled by a formal process.

Administrator-level accounts must only be used to conduct activities when and for which their elevated privileges are required. They must not be utilised for general user activities such as email access or web browsing.

Regular reviews must be conducted of administrative-level accounts by the relevant system owners. Any users who no longer need administrative access to carry out their role should have it removed.

The use of user accounts with privileged access in automated routines such as batch or interface jobs must be avoided where possible. Where this is unavoidable the password used must be protected and changed on a regular basis.

3.5 Permissible Authentication Mechanisms

In addition to the provision of a unique account identifier and password conforming to the requirements set out in this policy, a secondary form of authentication must be enforced where possible. This is known as Multi-Factor Authentication (MFA).

To avoid repeated user-experience requests to sign-in and to give enhanced technical control, USW systems should, where possible, support the University's core Single Sign-On (SSO) mechanism.

The University of South Wales recognises a paradigm shift is underway that provides stronger security posture to "basic" or "legacy" username/password authentication. Known as "modern" authentication, these token-based protocols should be used instead of "basic" authentication where possible.

Increasingly, "modern" authentication is being combined with biometric mechanisms such as facial feature detection. The University is open to considering these emerging forms of user authentication however any new usage of biometric authentication at USW must be approved. All requests must be considered by the IT Security Manager and the USW Information Compliance Manager.

Passwords are not always the most appropriate authentication mechanism between IT systems. Digital certificates and tokens may form part of the authentication for such solutions and the University core Single Sign-On (SSO) mechanism. Use of such mechanisms must be approved by USW IT Services after consideration of the technical standards and best practices supplied by approved platform and application vendors.

3.6 User authentication for external connections

Where USW colleagues require remote access to the on-premise University network, the University-provisioned Virtual Private Network (VPN) solution must be used.

Where students require remote access to USW on-premises resources (e.g. lab machines) this must be via the applicable USW-provisioned remote-access system.

In both instances, a policy of using multi-factor authentication for remote access will be used in order to reduce the risk of unauthorised access should a password be compromised.

Multi-factor or "Strong"¹ authentication must also be implemented for user accounts providing access to university-provisioned cloud-based SaaS applications.

For further information please refer to the Mobile Device Policy.

¹ "Strong" authentication relies on technologies other than or in addition to a password to securely and reliably confirm a user's identity.

3.7 Third-party remote access

Consideration must be given on a case-by-case basis of any requirement for supplier or other third-party access to USW systems. The principle of “least privilege” must be used to determine the solution to any such requirement.

The USW Guest Registration App has been provisioned to allow authorised colleagues to invite non-USW persons onto the University’s collaboration platform to fulfil general academic and business purposes.

Where there is a requirement to allow a third-party access to a system beyond what is provided via the Guest Registration App then a request from the business owner of the system concerned should be made to the IT Services Systems team. Prior to the creation of any third-party account:

- The technical account parameters required to fulfil the requirements should be assessed to determine conformance to least privilege and potential for introducing vulnerabilities. Any such vulnerabilities identified require risk-managing.
- A check must be made with USW Compliance to determine relevant protections (such as Non-Disclosure Agreements, Data Protection Act requirements) are in place.

Where access is required by a vendor to support a system, this requirement and its implementation must be documented in the system’s service design documentation.

In line with the “least privilege” principle, third-party accounts should only be enabled for the minimum time(s) necessary to fulfil the activities for which they are required.

The system owner must immediately communicate any relevant changes to a third-party’s status (e.g. on termination of a contract) to the IT Service Systems team so that access can be updated or disabled.

3.8 Review of user access rights

Asset and system owners must regularly review who has access to their areas of responsibility and the level of access in place. This will be to identify:

- People who should not have access (e.g. leavers that may have been missed by an exit process)
- User accounts with more access than required by the role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification, e.g. generic or shared accounts
- Any other issues that do not comply with this policy

This review will be performed according to a formal procedure and any corrective actions identified and carried out.

A review of user accounts with highly privileged access (for example, “Global Administrators” will be carried out by the Information Security Manager on a regular basis to ensure that this policy is being complied with.

3.9 User authentication and password policy

A strong password is an essential barrier against unauthorised access. Unfortunately, this area is often proven to be the weak link in an organization’s security strategy and a variety of ways to improve the security of user authentication are available, including various forms of two factor authentication and biometric techniques.

The University of South Wales’s policy is to implement and enforce additional multi-factor and/or modern authentication methods wherever possible.

Single Sign-On (SSO) will be leveraged where supported by relevant systems and applications unless the security requirements are deemed to be such that a further explicit sign-in is required.

Whether single or multi-factor authentication is used, the quality of colleague and student user passwords must be enforced in all networks and systems using the following parameters:

PARAMETER	VALUE
Minimum length	12
Maximum length	No maximum length should be configured
Re-use cycle	Cannot be the same as any of the previous 32 passwords
Change Frequency	▪ MFA-provisioned accounts: at least every 400 days. ▪ Non-MFA accounts: at least every 120 days.
Account lockout	On five consecutive incorrect logon attempts within a 10-minute period.
Account lockout action	Where an authorised system timeout is not in place, any sign-in prevented account must only be re-enabled following authorisation of the information security team.
Other controls	Password cannot contain the username Password must not be on a list of common passwords e.g. password1

Table 1: Passwords policy

Any exceptions to these parameters, for example where deployed technology cannot meet aspects of them, must be authorised by the Information Security Manager.

Strong password guidance must be made available to USW colleague and students to further enhance technical password policy controls.

3.10 Administrative Accounts and Password Policy

The following statements additionally apply to administrative and system accounts.

3.10.1 Administrator User Accounts

The password of a user account having domain administrator privileges must be at least 16 characters in length and.

Other user accounts having administrator level privileges to any systems or services must meet one of the following combinations of controls:

ALL SYSTEMS AND SERVICES HAVE MFA	MINIMUM PASSWORD LENGTH	PASSWORD CHANGE FREQUENCY
No	16 characters	120 days
Yes	16 characters	400 days

Table 2: Administrator account passwords policy

Any exceptions to these parameters, for example where deployed technology cannot meet aspects of them, must be authorised by the Information Security Manager.

3.10.2 System/Service Accounts

System/Service account passwords must be at least 16 characters and expire within a maximum of 400 days.

System/service accounts utilising non-password authentication factors such as API keys and certificates must follow the current USW development standards. The method used for them to authenticate to a particular USW system must be agreed and stated within the system's service design documentation.

A password on a system/service account must be changed whenever an individual with authorised knowledge of the password leaves the organisation or changes roles such that authorisation is withdrawn.

A system/service account should only be used to support the specific system/service.

Use of a standard user IT account to run system services is prohibited.

System/Service accounts must adhere to the principle of least privilege. For instance, accounts used for automated processing should be set to 'No Interactive Logins' and prevented from remote login.

Vendor-supplied default and/or blank passwords must be identified and reset upon installation of the affected application, device, or operating system.

3.11 Logging and Monitoring of Authentications

Authentication events to its systems and services are an auditable activity required to protect the University, its colleagues and students. In some instances, USW is required to keep a record by law and may be asked to provide these by agencies with statutory investigatory powers.

USW monitors and uses these events, both individually and in aggregate, to assist with:

- System health and performance maintenance
- Troubleshooting
- Security monitoring and alerting
- Incident response and investigation

The University's Logging & Monitoring Policy covers this control area.

4 Principles of Security Control

The deployment of systems, devices or applications utilising "default" passwords is prohibited. Where systems or devices are procured by USW with vendor-configured passwords these must be changed to one conforming with characteristics set by this policy.

Where an access control mechanism provides the facility for the setting of a password, it must be enabled, or an equivalent or stronger method used.

Where a system provides features for protecting against brute-force password attacks, (e.g., temporary user account lockout or host blocking), they shall be enabled.

Use of embedded passwords in program scripts, configuration files, or system environment variables is not recommended. Where there is no alternative available, access to the script or configuration files must be controlled to prevent unauthorised disclosure. To the extent possible, accesses must be logged and monitored to detect unauthorised access.

Wherever possible, Multi-Factor Authentication (MFA) must be used.

5 Policy Exceptions

Departments or other units may impose stronger minimal password and access control requirements for certain purposes, as appropriate, and those specific controls will take precedence over this policy. This should be done in consultation with the IT Services Security Team to ensure any access control requirements are indeed stronger than those set out in this policy.

Other exceptions to this policy may be requested by contacting the Head of Information Security. A case should be provided that explains why an exception is necessary.

6 User responsibilities

In order to exercise due care and try to ensure the security of its information, the University of South Wales expends a significant amount of time and money in implementing effective controls to lessen risk and reduce vulnerabilities. However, much still depends upon the degree of care exercised by the users of networks and systems in their day-to-day roles.

Many recent high-profile security breaches have been largely caused by unauthorised access to user accounts resulting from passwords being stolen or guessed.

It is vital therefore that every user plays their part in protecting the access they have been granted and ensuring that their account is not used to harm the University.

Colleagues, students, and other users are responsible for activity performed with their user account.

In order to maximise the security of our information every user must:

- Use a strong password i.e. one which is in line with the rules set out in this policy and associated guidance
- Never tell anyone their password or allow anyone else to use their account
- Not record the password in writing or electronically in unencrypted form e.g. in a text file, Office document or email
- Avoid using the same password for other user accounts, either personal or business-related
- Ensure that any PC or device they leave unattended, for any length of time, connected to the network is locked or logged out
- Leave nothing on display that may contain access information such as login names and passwords

Every user of university IT systems has a duty to report any identified access control breach or non-conformance with this policy to the IT Services Security team.

Colleagues and students and other users must follow the up to date best practices contained in the USW Password Guidance document.

7 System and application access control

As part of the evaluation process for new or significantly changed systems, requirements for effective access control must be addressed and appropriate measures implemented.

These must consist of a comprehensive security model that includes support for the following:

- Creation of individual user accounts
- Definition of roles or groups to which user accounts can be assigned
- Allocation of permissions to objects (e.g. files, programs, menus) of different types (e.g. read, write, delete, execute) to subjects (user accounts and groups)
- Provision of varying views of menu options and data according to the user account and its permission levels
- User account administration, including ability to disable and delete accounts
- User logon controls in conformance with the measures set out in this policy.
- User inactivity timeout
- Password management, including
 - Ability for user to change password
 - Controls over acceptable passwords
 - Password expiry
 - Hashed/encrypted password storage and transmission
- Security auditing facilities, including logon/logoffs, unsuccessful logon attempts, object access and account administration activities

Systems and devices should only contain necessary and approved user accounts that are regularly required to support the business function of the system. Where possible, privileged administrator accounts should only be enabled when activities requiring these privileges require performing and then disabled.

Individual user accounts should not be used to support automated business processes.

Where bespoke software development is undertaken, program source code must be protected from unauthorised access in accordance with the current USW development standards.

Access to privileged utility programs that provide a method of bypassing system security (e.g. data manipulation tools) must be strictly controlled and their use restricted to identified individuals and specific circumstances e.g. as part of a named project or change.

8 ISMS Conformance

8.1 Areas of ISO/IEC 27001:2013 addressed

The following areas of the ISO/IEC 27001:2013 standard are addressed by this document:

- A.5 Information security policies
 - A.5.1 Management direction for information security
 - A.5.1.1 Policies for information security
- A.9 Access Control
 - A.9.1 Business requirements of access control
 - A.9.1.1 Access control policy
 - A.9.1.2 Access to networks and network services
 - A.9.2 User access management
 - A.9.2.3 Management of privileged access rights
 - A.9.3 User responsibilities
 - A.9.3.1 Use of secret authentication information
 - A.9.4 System and application access control
 - A.9.4.1 Information access restriction
 - A.9.4.2 Secure log-on procedures
 - A.9.4.3 Password management system
 - A.9.4.4 Use of privileged utility programs
 - A.9.4.5 Access control to program source code

The following areas of the ISO/IEC 27018:2014 standard are addressed by this document:

- ISO/IEC 27018 Extended Control Set
 - A.10 Information security
 - A.10.10 Userid management
 - A.10.8 Unique use of userids
 - A.10.9 Records of authorized users

8.2 Related Policies and Regulations

The following policies and procedures are relevant to this document:

- Mobile Device Policy
- Working Flexibly Policy
- User Access Management Process
- Network Security Policy
- Cloud Computing Policy
- Internet Acceptable Use Policy
- Supplier Information Security Evaluation Process

8.3 Compliance

Where any USW IT account is determined to have been compromised or is reasonably judged to be at imminent risk of compromise, IT Security reserve the right to:

- block sign-ins
- end any running user sessions
- suspend authorisations and abilities the user may have, for example sending/receiving email, access to files and applications.

Colleagues, students and other IT account owners must assist with any incident or investigation regarding the (mis-)use of their USW IT accounts. Any instruction given by the IT security Manager or their delegate to perform a corrective or preventative action must be followed.