Identity and Access Management Policy

Information Security

This document can only be considered valid when viewed via the University website. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one on the University website. Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Contents:

1. Introduction

The University has a wide range of users who need access to many different information systems. Some of these systems are either critical and / or hold sensitive information. To manage the risks associated with access to university information systems, access must be appropriately controlled and restricted.

Identity and access management processes provide effective and consistent identification, authentication, access, accountability, and administration mechanisms across the University.

This policy is to be read and understood by systems owners, system administrators, and anyone responsible for managing access to information systems.

2. Objective

2.1 The aim of this policy is to ensure the confidentiality, integrity, and availability of the University of Bradford’s information assets by providing a basis for the effective management of user identities and access to the University's IT systems and applications.

3. Scope

3.1 This policy applies to all employees, contractors, vendors, and third-party users who access University of Bradford resources, including but not limited to:

- University-owned devices
- Internal networks and systems
- Cloud-based applications and services
- Data repositories and sensitive information

4. Governance

4.1 The University's IT Services department is responsible for the implementation, administration, and enforcement of this policy.

5. Responsibilities

The IT Director has delegated authority from the Executive Board to review and approve this policy. Other responsibilities are as follows:

Managers

5.1 Managers are responsible for ensuring their teams read and comply with this policy.

System Administrators

5.2 IT System administrators shall administer access to IT Infrastructure and systems.

5.3 Where agreed with the Service Owner, System Administrators outside of IT shall administer end user access to the applications, otherwise this is a function of IT Systems Administrators.

5.4 All System Administrators shall comply with this policy and any applicable legislation.

Service Owners

5.5 Service Owners shall ensure that any users with privileged access to the systems they are responsible for have been properly approved and trained; and

5.6 Shall maintain a register of business administrators and the information systems to which their teams have privileged access.

IT Services

5.7 IT Services shall enable system administrator access to IT and users in the University, after approval is received from the requester’s manager and a second approval by the IT Associate Director or IT Director.

Individuals

5.8 Individuals shall be responsible for selecting strong passwords following the Password Policy, keeping passwords secure, and reporting any unauthorised use of accounts.

Head of IT Security

5.9 The Head of Security shall oversee any unauthorised access incidents and investigation; and

5.10 Conduct regular access reviews of user access rights within IT Services.

IT Risk and Compliance Manager

5.11 The IT Risk and Compliance Manager shall ensure regular access reviews are carried out for audits.

6. Principles

Identity management

6.1 **Identity and access management:** Access to information, IT applications, and systems will be controlled and restricted using the principal of 'least privilege', where the access provided should be the minimum required for the user to be effective in their role, be provided based on business security requirements, and appropriate to a user's responsibilities.

6.2 **User account management:** User accounts must be managed consistently and securely throughout their lifecycle – that is, initial account creation, change of role, and end of employment.

User access management

6.3 **Documented access control standards and procedures:** Access control standards and procedures must be documented by System Administrators, regularly reviewed, and updated as necessary to ensure that access rights are granted based on the principle of least privilege.

6.4 Access control arrangements must be supported by the following:

- Acceptable Use Policy
- Information Classification and Handling Policy
- Requirements set by information asset owners and / or System Owners
- legal, regulatory, and contractual obligations
- the need for individual accountability
- the need for additional security controls for users with special access privileges and the need to provide segregation of duties

Authorised access

6.5 Access rights for business users and technical staff must be approved by an appropriate business representative, such as a manager, information asset owner, or System Owner, and must default to the lowest level of access required.

6.6 Any privileged accounts or administrative access needed on applications must be approved by the business owner's manager.

6.7 Access to the mailbox and one drive of a staff in their absence, must be justified by a legitimate business need, limited to the minimum necessary to perform the required tasks and approved by the relevant Manager and HR personnel.

Access through shared / generic accounts

6.8 Access rights must not be assigned using shared, or generic accounts, unless exceptional circumstances apply. Access rights for these types of accounts must be:

- documented
- approved by an appropriate business representative and the IT Director or IT Associate Director
- assigned to a nominated responsible and accountable person, and
- subject to additional controls and regularly reviewed

Special access privileges

6.9 Wherever possible, the account used to exercise privileged access should be associated with an identifiable individual, and not used by anyone other than that individual. The use of anonymous privileged accounts such as 'root' or 'administrator' should be avoided as far as possible.

6.10 Role based access should be used to identify which individuals require privileged access.

6.11 Privileged accounts must not be used to bypass or circumvent security controls or policies, or to access data or systems that the user would not otherwise have access to.

6.12 Privileged accounts must not be used for routine business activities, such as checking email, browsing the web, or performing other non-security related tasks.

6.13 Logging and reviewing of the use of special access privileges, and regular review of the need to have special access privileges will be carried out by IT Services. Privileges granted by business owners will be reviewed by the business owners.

6.14 Wherever possible, all actions carried out using privileged access should be logged. Ideally, this should be done using a mechanism such that the log cannot be subsequently deleted or altered even using privileged access.

System Administrators

6.15 IT privilege access requests and approvals shall be recorded and logged in ServiceNow.

6.16 System Administrators shall not reveal confidential or highly confidential information they might learn during their activities other than for the specific purposes for which the activity was authorised, for the purposes of law enforcement, to prevent a crime, or to prevent harm to individuals.

Access control procedures review

6.17 Access control processes and procedures must be reviewed by IT and business owners on a bi-annual basis and updated in response to new threats, capabilities, and user access controls:

6.18 Multi-factor authentication must be used wherever possible.

6.19 The use of passwords for access control must be supported by the Password and Acceptable Use policies.

User system sign-on process

6.20 **System sign-on process:** Sign-in processes must ensure that only authorised users can access University information systems.

6.21 **Sign-in configuration:** Where supported by the system, sign-in mechanisms must be configured so that they:

- where possible, limit the number of unsuccessful sign-in attempts which are allowed
- where possible, restrict additional sign-in attempts
- limit the duration of any one sign-in session for high-risk systems and applications.

Sign-in information

6.22 Sign-in mechanisms must be configured to provide information so that they:

- display no identifying details until after sign-in is successfully completed
- warn that only authorised users are allowed access
- record all successful and unsuccessful sign-in attempts
- display non-specific messages where there is a sign-in failure, and

6.23 All sign in information should be recorded, and logs sent to the University's logging servers.

Sign-in authentication details

6.24 Where possible sign-in mechanisms must be configured so that they do not store or send authentication details as clear text. Passwords must be obscured at any sign-in prompt.

System access controls

6.25 **Controlling access to applications and their information:** Security controls must be used to restrict access to and within applications and application software. Application systems must:

- control user access to information and application system functions, in accordance with this policy.
- provide protection from unauthorised access by any malicious software that could override or bypass system or application controls, and
- not compromise other systems with which they share information resources.

6.26 **Information access restriction:** Access to information and application system functions must be clearly defined with documented roles and responsibilities and regularly reviewed.

6.27 **Authorised access to operating systems:** Security controls must be used to allow authorised users access to operating systems. The controls must:

- authenticate authorised users only
- record successful and failed system authentication attempts
- record the use of special system privileges
- where possible, issue alarms when system security policies are breached
- provide appropriate methods of authentication
- prohibit unlimited time access to services and apply inactivity or session timeouts where appropriate

6.28 **Use of system utilities:** The use of utility programs that might override system and application controls must be restricted and tightly controlled.

6.29 **Controlling access to networked services:** Access to both internal and external networked services must be controlled to ensure that:

- appropriate authentication mechanisms are applied for users and equipment, and
- control of user access to information services is enforced.

6.30 **Remote access and user authentication connections:** Access by remote users must be controlled by using approved multi-factor authentication methods.

6.31 Third party access:

- Access to the University's systems, data, and resources by third-party entities must be approved in advance by the appropriate designated authority.
- Access privileges must be granted based on the principle of least privilege, with permissions tailored to the specific needs of the third party for fulfilling their contractual obligations.
- Authentication and authorisation mechanisms, such as unique user accounts, strong passwords, multi-factor authentication, and role-based access controls, must be implemented to verify the identity and permissions of third-party users. Exceptions may be permitted in approved exceptional cases.
- Security measures may include encryption, secure transmission protocols, antivirus software, intrusion detection / prevention systems, and regular security updates and patches.
- Access should be granted through a secure portal and activity recorded or monitored.

7. Data Centers and server rooms

All entry points to server rooms and data centres must be equipped with access control systems, such as keylocks, card readers, and PIN pads.

All individuals entering secure areas must be identified and authenticated using authorised access credentials, such as ID badges, key cards, or biometric systems.

All access to secure areas must be logged manually or automatically, including details such as the identity of the individual, time of entry, and area accessed.

8. Implementation and training

Line managers within IT and the business services should raise awareness of all new and updated policies.

The IT Services department will work with Faculties and Directorates to provide guidance and support to line managers regarding the implementation of this policy, where required.

9. Incident and breach reporting

Any data or information security related events or suspicions, including the following, must be reported via IT ServiceNow or by calling IT Servicedesk on **01274 233333** as soon as possible:

- Any infringement of this policy
- Any information security event (actual or suspected)
- Technical problems, requests, or concerns regarding a suspected information breach

Note: All breaches involving personal information must be reported to the Data Protection Officer through the IT Risk and Compliance Manager.

10. Infringement

Breach of this policy or wrongful disclosure of confidential information will be handled by the staff disciplinary processes available through People, Culture and Wellbeing.

A breach of this policy may lead to sanctions being imposed.

In cases where the Staff Disciplinary Policy does not apply - that is, where an alleged breach has been committed by someone who is neither a member of staff nor a student - an investigation will be conducted by the IT Director or IT Associate Director in conjunction with the Legal and Governance team.

Breach by a third party may lead to termination of contract and remedies under contract terms being invoked.

Where an offence has occurred under UK law, it may also be reported to the police or other appropriate authority and could lead to civil or criminal proceedings.

If you need any assistance with interpreting or applying this policy, you should contact IT Services through IT ServiceNow.

11. Related policies and standards

This policy forms part of the Information Technology Policy Framework and should be read in conjunction with the policies, regulations, standards, and procedures contained therein, in particular:

- Acceptable Use Policy
- Password Policy
- Data Protection Policy
- Student Disciplinary Procedure
- Staff Disciplinary Procedure

12. Policy exemptions

Every effort must be made to comply with all University information security policies. Where it is not possible to apply or enforce any part of this policy, either for operational or legitimate academic reasons, a policy exemption request should be submitted to itriskandcompliance@bradford.ac.uk. The IT Risk and Compliance Manager and the Data Protection Officer, if required, will review the business justification, advise on the potential risks involved, and agree to any exceptions.

13. Monitoring and review

This policy will be reviewed annually, or as appropriate, and in response to changes to legislation or University policies, technology, increased risks and new vulnerabilities, or in response to security breaches.

14. Terms

System Administrator

An individual in IT an department responsible for managing, configuring, and maintaining the IT infrastructure – that is, servers, networks, software, and other computing resources for the University. This include individuals outside of IT

Service who are responsible for administering end user access to business applications.

Business Service Owner

The individual responsible for ensuring that any business users with privileged access to the systems they manage have been properly approved and trained.

IT Service Owner

The individual responsible for ensuring that business application users in IT with privileged access to the systems they manage have been properly approved and trained.

IT applications

A software program designed to perform specific tasks to support University processes – for example, software that supports business functions such as finance, and human resources (ERP systems).

15. Document and version control information:

Version control information heading	Details
Owner	IT Services
Author	IT Risk and Compliance Manager
Approved by	IT Director
Date of approval of this version	5 November 2024
Next review date	5 November 2025
Version number	V1.0
Applicable statutory, legal, or national best practice requirements	• General Data Protection Regulations (GDPR) • Computer Misuse Act 1990 • Cyber Essentials • ISO 27001:2013 Information Security Management Standard
Equality impact assessment completion date	Not applicable
Data protection impact assessment completion date	Not applicable