UNIVERSITY OF ABERDEEN

AUTHENTICATION POLICY

1. Purpose

This policy sets out the principles and responsibilities for the identification and authentication of any person accessing data and/or services provided by the University of Aberdeen. This usually involves a username, password and possibly another authentication method, for example if systems are configured for multi-factor authentication.

2. Scope

This policy applies to:

- All individuals, including staff, students, contractors and visitors, who have access to the University of Aberdeen digital services, information, login credentials and technologies.
- All facilities, technologies, and services that are used to process the University of Aberdeen information.
- All information processed, accessed, manipulated or stored by the University of Aberdeen.
- Internal and external processes and systems that are used to store, transfer or process the University of Aberdeen information.
- External parties and suppliers that provide information storage, hosted systems, transferal or processing services to the University of Aberdeen.

3. Objectives

This policy is designed to:

- Ensure University of Aberdeen Information is appropriately protected from theft or accidental loss of the device on which it is stored.
- Ensure University of Aberdeen Information is appropriately protected when it is being transferred from system to system.
- Protect the confidentiality, integrity and availability of University digital assets, services and data.
- Ensure controls and mitigations are appropriate and effective by identifying and managing the information security threats and risks.
- Reduce information related risk to acceptable levels.
- Clearly define responsibilities for maintaining information security.
- Provide assurance to information owners, individual and organisational, both within and outside of the University that their information is appropriately protected.

- Support secure information sharing and collaboration.

4. Roles and Responsibilities

- **All users, including staff, students, contractors and third parties** at all levels are responsible for protecting the University's information, adhering to all relevant policies, guidelines and procedures and making informed decisions to protect the information that they process. Users are expected to familiarise themselves with the relevant policies governing the information and systems they access.
- **Heads of Schools and Directors of Professional Services** are accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within their areas of managerial responsibility.
- **University Officers and Managers** are accountable for ensuring that information in their category is not put at undue risk. They will approve all use and sharing of information in their category, having considered the risks and benefits.
- **The Information Governance Committee (IGC)** has executive responsibility for information governance and security within the University of Aberdeen. Specifically, The Information Governance Committee has responsibility for overseeing the management of the security and governance risks to the University of Aberdeen's staff and students, its infrastructure and its information.
- **The Director of Digital and Information Services** has delegated responsibility for establishing and maintaining the University of Aberdeen's ISMS to ensure the availability, integrity and confidentiality of the University of Aberdeen's information. The Director of Digital and Information Services will lead on the definition and implementation of the University of Aberdeen's information security and governance arrangements and make judgement calls when situations arise that are not covered by the current information security management framework.
- **The Information Risk Working Group (IRWG)** is responsible for reviewing information governance and security risk, advising on risk treatment efforts and ensuring consistent implementation of this policy.
- **The Operational Security Group (OSG)** is an internal Digital and Information Services (DIS) group responsible for compliance monitoring and improvements, information security maturity assessment, policy review and assessment of security risk and issues. DIS technical service owners and managers are responsible for the deployment and configuration of digital services and systems.
- **The Information Security Manager** is responsible for the development and improvement of the University Information Security posture.

5. Policy

5.1. **Users of University of Aberdeen digital services and data**

Staff, students, contractors and third parties with University issued credentials must:

- Use University issued credentials when accessing all University of Aberdeen Information Systems or Networks.
- Ensure that usernames and passwords are kept secure and not shared with, or disclosed to, any individual.
- Use multi-factor authentication where possible and required.
- Not write passwords down or leave them unsecured.
- Ensure that passwords are suitably obscure, so they are not easily guessed by other people or computer systems. Don't use anything obvious like a name, a dictionary word in any language, a password used on another site, or a password you've used before.
- Always use different passwords for individual logins and services. Never reuse the same password. For example, do not use the same password for University purposes as for personal purposes.
- Ensure that any other authentication mechanism such as a multi-factor authentication token or corporate device is always kept safe and secure.
- Notify the IT Service Desk immediately if they become aware or suspect that their credentials have become compromised.
- Protect credentials by never passing them over unsecure networks or in plain text.
- Never enter username and password to access sites and services on a public or shared device e.g. airport/kiosk device.

5.2. **Individuals and teams involved with the technical management of University of Aberdeen digital services and data**

Devices connected to University of Aberdeen networks, and digital services and applications provided by the University, must:

- Have a designated person responsible for the device.
- Have all “built in” or “default” accounts disabled unless not possible to do so.
- Have all required credentials stored centrally within the University approved password management system.
- Have appropriate permissions and access controls in place within the Password Management System in line with principle of Least Privilege.
- Have the password changed if it is known or suspected that credentials have been compromised.
- Have the password changed if the authorisation of any person who has access via the Password Management System is withdrawn. For example, through a change in role or departure from the University.
- Implement log-in to the application/service using Active Directory or one of the federated authentication methods (Shibboleth/LDAP) unless not possible to do so.

- Implement failed login throttling at the application/service edge unless it is not possible to do so in which case throttling must fall back to recognised authentication mechanisms (AD/LDAP/Shibboleth)
- Have multi-factor authentication must be enabled where it is possible to do so.
- Restrict access to authentication data and logs using the principle of least privilege.

6. Exceptions

Any exceptions to the requirements defined in this policy must be justified, documented and approved following a risk assessment by the Information Security Manager and Data Protection Officer.

7. Compliance

7.1. The University of Aberdeen shall conduct information security and risk audit, compliance and assurance activities to ensure information security objectives and the requirements of this policy are met. This right will be exercised across all University owned and operated networks, devices connected to these networks and hosted systems that store University data.

7.2. Audit reports and any non-compliance will be presented to IGC as the body with executive responsibility for information governance and security within the University.

7.3. The University of Aberdeen's Internal Audit function will undertake independent reviews of the implementation of the Information Security Policy and the supporting policies, Codes of Practice, Procedures and Guidelines.

7.4. Non-compliance with this policy will be treated extremely seriously by the University of Aberdeen and may result in enforcement action on a group and/or an individual.

7.5. A breach of this policy shall be a breach of the University of Aberdeen Conditions for using IT Facilities and will be dealt with under the provisions of those conditions.

8. Review and Development

This policy is reviewed on at least annually to ensure it:

- Remains fit for purpose and accurate.
- Reflects changes in technologies.
- Is aligned to industry best practice.
- Supports continued regulatory, contractual, and legal compliance.

Approval/Review History

Version	Date	Action
1.0		Approved
2.0	September 2019	Approved
3.0	Information Governance Committee, 2nd March 2021	Approved

Policy Metadata

Title	Authentication Policy
Author / Creator	Gary Fisher, Information Security Manager
Owner	Information Security Manager
Date published / approved	2nd March 2021
Version	3.0
Reviewed	March 2021
Date of next review	March 2022
Audience	All staff, students, partners, suppliers and contractors who work for or on behalf of the University.
Related documents	Information Security Policy Data Protection Policy Authentication Policy Guidance
Subject / Description	Purpose of this policy is to ensure that the audience described above are aware of and comply with methods of authentication for accessing University of Aberdeen systems, networks and services.
Document status	Policy
Equality Impact Assessment	N/A
Theme	IT Security, Information Security Management, Information Management
Keywords	Authentication, Password, Access, Security, Information Security, IT Security, Acceptable Use, username, Least Privilege