UNIVERSITY OF ABERDEEN

AUTHENTICATION POLICY

1. Purpose

This policy sets out the principles, responsibilities and obligations for the verification of identity of any person accessing controlled data and/or services provided by the University. This usually involves a username and password but can include any other method of confirming identity, such as a smart card, retina scan, voice recognition, Two Factor Token or fingerprint.

2. Scope

This policy and its supporting guidance apply to the verification of identity as follows:

- The policy applies to all staff, students and other users of the University of Aberdeen Information Systems, devices or data repositories connected to University of Aberdeen networks.

- The policy applies to all types of devices connected to University of Aberdeen networks.

- The policy applies to all services hosted by third parties on behalf of the University of Aberdeen.

3. Roles and responsibilities

The roles that carry responsibilities under this policy are as follows:

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

    - Use University issued credentials when accessing all University of Aberdeen Information Systems or Networks. In most cases this will comprise of a University of Aberdeen issued username and password.

    - Ensure that credentials are kept secure, not written down or in any other way divulged to any individual not authorised to know them.

    - Ensure that any other authentication mechanism such as a security dongle or corporate device is always kept safe and secure.

    - Notify the Service Desk in a timely manner 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. Examples include but are not limited to HTTP, Telnet, FTP.

- Never enter username and password to access sites and services on a public or shared device e.g. airport/kiosk device.

- Never reuse the same password for example, using the same password for University purposes as for personal purposes.

- Ensure that passwords are suitably obscure such that they are not easily guessed by other people or computer systems.

- Change their passwords on a regular basis in line with Authentication Guidance which can be found in Policy Zone.

- Staff, students and third parties with University issued credentials must not:

    - Write down or otherwise share their University issued credentials with any other person.

    - Use their University password(s) for personal purposes.

    - Use their personal password(s) for University purposes.

- Devices connected to University of Aberdeen networks 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 Thycotic Password Management System.

    - Have appropriate restrictions in place within the Password Management System in line with Least Privilege.

    - Have a record maintained in the Password Management System of who has access to the credentials.

    - 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.

- Where Authentication Data Storage is employed it is mandatory that:
    - Electronic systems holding Authentication Data are hardened to enhance their security.
    - Electronic systems holding Authentication Data are not utilised for any other purpose.
    - All copies of Authentication Data are encrypted at rest and during transmission.
    - Authentication data is protected against Brute Force Attacks, for example password guessing.
    - Access to Authentication data is restricted to individuals with legitimate purpose.
    - Printed copies in plain text are secured in safes or other accepted secure storage.
    - Electronic and printed copies are irrevocably destroyed when no longer required.

- The Director of Digital and Information Services may:

    - Grant unauthenticated access to individuals or systems e.g. Kiosks, in exceptional circumstances.

    - Revoke the credentials of individuals, in line with HR and other policies where inappropriate or illegal activity has occurred or is suspected or for the purposes of investigation.

4. Auditing

Periodic audits will be undertaken to ensure that this policy is adhered to. Generally, such audits will occur no less than annually.

5. Enforcement

Where possible, systems and services will be configured to automatically enforce this policy.

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

6. Review and Development

This policy shall be reviewed on an annual basis by the IT Security Manager and, if required, recommendations for amendment made to the Information Governance Committee following a period of consultation with the Operational Security Group.

Glossary of terms

Identity	The characteristics determining who or what a person or thing is.
Credentials	A document or other mechanism proving a person's identity
User Name	An identification used by a person with access to a computer, network, or online service.
Password	a string of characters that allows access to a computer system or service.
Authentication	the process or action of verifying the identity of a user or process.
Least Privilege	The principle means giving a user or process only those privileges which are essential to perform its intended function.
Encryption	the process of converting information or data into a code, especially to prevent unauthorized access.

Title	Authentication Policy
Author / Creator	Mark Marooth
Owner	Garry Wardrope IT Security Manager
Date published / approved	Approved May 2019 Published September 2019
Version	1.0 Original Version 2.0 This Version
Date for Next Review	September 2020
Audience	All staff, students, partners, suppliers and contractors who work for or on behalf of the University.
Related	Conditions for using IT Facilities Information Security Policy JANET Acceptable User Policy (External)
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.
Equality Impact Assessment	N/A
Section	Digital and Information Services
Theme	IT Security and Acceptable Use
Keywords	Authentication, Password, Access, Security, Information Security, IT Security, Acceptable Use