Authentication Policy

1. Overview

Authentication is any process by which you verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints.

It is common to use only a single factor for authentication, but where additional security is required two factors may be used. These are typically ‘something you have’ e.g. a smartcard and ‘something you know’ e.g. a PIN number.

Nothing in this document should be taken to override the University of Aberdeen Information Security Policy or the JANET Acceptable Use Policy. Where there is any conflict the above policies take precedence.

2. Purpose

The information which the University manages must be appropriately secured in order to protect the University and its members from the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. A key requirement for this is to ensure that only authorised persons can access University information and services. In order to do this we first need to reliably authenticate the person requiring access.

It is also necessary to be able to hold individuals to account for their actions when accessing University of Aberdeen Information systems and services, in order to do this we need to reliably know who the person is.

As authentication data, e.g. passwords, are a critical component of ensuring the security of University of Aberdeen information, we must make certain that it is managed and protected appropriately.

3. Scope

All staff, students and other users of University of Aberdeen Information Systems or devices connected to University of Aberdeen networks must abide by this policy.

There are many different types of device connected to the University of Aberdeen networks, ranging from temperature probes to servers containing critical staff data. This policy applies to all devices connected to the University networks or providing access to them.

Services hosted by third parties on behalf of the University of Aberdeen must also abide by this policy.

4. Policy

a. General

i. A suitable method of authentication must be used by all users and systems accessing University of Aberdeen Information Systems or Networks. In most cases this will be a University of Aberdeen issued username and password.

ii. Unauthenticated access will be permitted only in exceptional circumstances (e.g. kiosks) and such systems must be explicitly configured for such use.

iii. For general computing devices (e.g. PCs) appropriate accounting information must be kept.

iv. Unused accounts must be disabled and default or blank passwords must be changed.
b. Passwords

i. Passwords must be kept secure; they should never be divulged to anyone not authorised to know them.
ii. Passwords should be changed at regular intervals.
iii. Passwords must be protected in use; in particular they should not be passed over unsecure networks in clear text.
iv. The user’s identity must be clearly established before a password is issued to a user.
v. Passwords should not be overused.
   • University of Aberdeen usernames and passwords should not be used with non University of Aberdeen systems.
   • Separate usernames and passwords should be used for trusted and untrusted systems.
vi. Password should be complex and obscure, such that they are not easily guessed by people or computer systems.

c. Personal Passwords

i. Personal passwords should not be shared; only in exceptional circumstances will passwords be issued to groups of users.
ii. Personal passwords must be kept secure; they should never be divulged to anyone, not even support staff.

d. Device passwords

i. All devices connected to University of Aberdeen networks will have a person responsible for that device.
ii. ’Built in’ or default user accounts should not be used if possible. These accounts should be disabled and personal user accounts used to administer the device.
iii. Where inbuilt accounts must be used, only those with a need to know should have access to the password.
iv. Passwords for devices must be held securely with access restricted to only those who have access specifically authorised.
v. A record of who knows device passwords will be kept.
vi. Device passwords will be changed whenever anyone who knows them has authorisation to access them withdrawn. e.g. someone leaves.

e. Authentication Data Storage

i. There is a need to process Authentication Data to manage user accounts and to allow Information Systems to be able to authenticate users. Typically Authentication Data is held electronically in directories (e.g. MS Active Directory) or in databases.
ii. The systems holding Authentication Data should be hardened to enhance their security and should not be used for any additional purpose that might compromise their security.
iii. All electronic copies of Authentication data must be encrypted.
iv. Authentication Data must be protected from Brute Force Attacks. (e.g. password guessing).
v. Access to Authentication Data should be restricted such that only the data necessary is available to each member of staff. Particular care is required to restrict access to password files.
vi. Where Authentication Data is available in plain text (e.g. print outs) staff should be aware of its sensitivity, ensuring its protection and secure disposal.
f. Responsibilities

i. It is the responsibility of the 'Responsible Person' to ensure that devices are configured in compliance with this policy.

ii. It is the responsibility of users to ensure they keep their password (and any other credentials) secure.

iii. It is the responsibility of IT Services to provide guidelines and advice on implementing this policy.

5. Auditing

Periodic audits will be undertaken to ensure this policy is adhered to. When available system features should be used to ensure this policy is complied with, e.g. enforcing minimum password lengths.

6. Enforcement

Where possible, systems will be configured to automatically enforce this policy, e.g. require minimum password lengths.

A breach of this policy shall be considered a breach of the University of Aberdeen Conditions for using IT Facilities and will be dealt with as provided in them.

In particular IT Services has the authority to refuse to provide a network service to or restrict the service provided to any device or user it believes has or will breach this policy.

7. Definitions

Further guidance and definitions can be found in the Authentication Policy Guidelines.
Approval/Review History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>June 2012</td>
<td>Approved</td>
</tr>
</tbody>
</table>

Policy Metadata

<table>
<thead>
<tr>
<th>Title</th>
<th>Authentication Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author / Creator</td>
<td>Garry Wardrope, IT Security Manager</td>
</tr>
<tr>
<td>Owner</td>
<td>IT Security Manager</td>
</tr>
<tr>
<td>Date published / approved</td>
<td>June 2012</td>
</tr>
<tr>
<td>Version</td>
<td>V 1.0</td>
</tr>
<tr>
<td>Reviewed</td>
<td>November 2018</td>
</tr>
<tr>
<td>Date of next review</td>
<td>November 2019</td>
</tr>
<tr>
<td>Audience</td>
<td>All staff, partners, suppliers and contractors who work for or on behalf of the University</td>
</tr>
<tr>
<td>Related documents</td>
<td>Conditions for using IT Facilities</td>
</tr>
<tr>
<td></td>
<td>Information Security Policy</td>
</tr>
<tr>
<td></td>
<td>JANET Acceptable User Policy (external)</td>
</tr>
<tr>
<td>Subject / Description</td>
<td>The purpose of this policy is to ensure staff and students are aware and comply with methods of authentication for accessing University of Aberdeen systems and networks.</td>
</tr>
<tr>
<td>Document status</td>
<td>Policy</td>
</tr>
<tr>
<td>Equality Impact Assessment</td>
<td>N/A</td>
</tr>
<tr>
<td>Theme</td>
<td>IT Security</td>
</tr>
<tr>
<td>Keywords</td>
<td>Information Security, IT Security, authentication, password, username, data, access</td>
</tr>
</tbody>
</table>