Authentication Policy Guidelines

Overview
This document is intended to provide assistance in implementing the University of Aberdeen Authentication Policy. It provides guidelines and details of best practice that should, in most cases, be sufficient to ensure that the above policy is complied with.

Guidelines
Paragraph numbers below refer to the numbering of the Authentication Policy.

General

4.a.i. Username and password is the most common method for authenticating users at the University of Aberdeen. Swipe/proximity cards (University ID card) are also used to provide access to print and photocopy services and further use may be possible.

4.a.ii. Unauthenticated access may be permitted by the Director of IT. In such cases access to information must be strictly limited. In particular general access to network services are prohibited, including access to web and messaging (e.g. email). Access to a specific set of web pages may be possible, as long as there is no way to navigate the web in general.

4.a.iii. For general computing devices (e.g. PCs) suitable accounting information must be kept. This must include details of who was using the system and at what dates/times. This information should be kept for at least 6 months. Care should be taken to preserve this information if the system is rebuilt.

Passwords

4.b.i. Passwords should not be written down, sent in email or kept on mobile devices without strong encryption.

4.b.ii. The frequency of password change should be determined by considering the risks involved. Factors that should be taken into consideration include:

- Impact of a password being compromised, i.e. what is the value of the resource it protects.
- Exposure of the password e.g. Is it transmitted over public networks (e.g. used from home)? Is it used in an environment where onlookers (including colleagues) may see it being typed at a keyboard?
- Users are likely to keep insecure notes of their passwords if they are changed too frequently.

For most systems used at the University of Aberdeen a change frequency of 1 year will be appropriate. Examples of extremes where this might not be appropriate are:
• Access to sensitive personal information from home PCs. In this case the password may require to be changed after every use. The use of such “one-time” passwords will usually need special hardware support to provide users with the passwords. e.g. RSA secureID tokens.

• Configuration access to a temperature probe, where the password is rarely used after the device has been set up. In this case no password changes are required once the default password has been replaced.

4.b.iii. Passwords should be protected in use:

• System implementers should ensure that passwords are encrypted when users are requested to supply them. e.g. Web logon pages should use https.

• Users should take care to ensure the system they are entering their password on is genuine. e.g. it is a genuine University web page, checks should include the page has the correct URL and has a valid certificate issued to the University of Aberdeen.

4.b.iv. When passwords are reset, new passwords should usually only be supplied to:

• The user presenting their staff or student ID card.

• emailed to the user’s University email account. (Where the password isn’t for said email account).

• The user supplying the correct authentication information to the online password reset system.

4.b.v Passwords should not be overused.

4.b.v.1. University of Aberdeen passwords should only be used to access bona fide University resources. University usernames and passwords must never be used when creating accounts on non University systems (e.g. a Facebook)

4.b.v.2. System accounts (e.g. PRV accounts) should only be used to log into those systems on which they are required. They should never be used to logon to insecure systems even where this system is being used as a ‘terminal’ to access the secure system.

In this context an insecure system is one where the integrity of the system cannot be guaranteed e.g. a general PC where several people, including end users, have admin access and so may have installed (perhaps unintentionally) malicious software.

4.b.vi. Where possible passwords should be constructed as:

Must contain at least 8 and no more than 14 characters

Must not contain the first 6 characters of a dictionary word, or the first 6 characters of your username

Must contain at least 1 lowercase character (a-z), 1 uppercase character (A-Z), 1 alphabetic character, and 1 numeric character (0-9).
May contain no more than 2 consecutive duplicate characters (i.e. xx is OK but xxx is not)

May contain sequences of no more than 3 characters (i.e. abc is OK but abcd is not)

Personal Passwords

4.c.i. Examples of the circumstances where sharing passwords might be appropriate are:

- Read only access to a web site where the information is only to be made available a group whose members don’t already have individual accounts. (e.g. an external group).

4.c.ii. Users must never tell anyone else their password, not even University of Aberdeen Support Staff. If you suspect someone else knows our password you should reset it immediately or inform the DIT Service Desk. Where support staff that need access to an account they should either ask the account owner to “log in” for them or reset the account password and use the new password for the work. On completion of the work the account owner should be given the new password and asked to reset it.

Device passwords

4.d.i The “Responsible Person” is responsible for ensuring that ‘their’ devices comply with this policy. In the case of Devices administered by Directorate of Information Technology this will be the Director who may delegate the implementation.

Authentication Data Storage

4.e.ii. Authentication servers, e.g. Domain Controllers, should be located in a secure environment (e.g. Data Centre or locked cabinet). Disks on these servers should be encrypted if possible. Only those services that are an integral part of providing authentication should be run on these servers. (e.g. they must not be used as file servers). Special care should also be taken to ensure all data is properly erased when the servers and their disks are disposed of.

4.e.iv For general user accounts, these will be disabled, for a period of 15 minutes, when an incorrect password is tried more than 100 times in a period of 15 minutes. Care should be taken that mechanisms intended to protect attacks do not create a vulnerability to Denial of Service Attacks.

Third Party Hosted Services

This policy applies to user access to services provided to the University of Aberdeen hosted by third parties. It does not apply to access to such systems by the third party themselves or staff contracted to them.

The preferred method of authenticating access to third party services is through federated authentication, where authentication is passed to University of Aberdeen authentication systems using University of Aberdeen usernames and passwords. Where this in not possible
and authentication is undertaken by the third party directly, University of Aberdeen usernames and passwords must not be used, as required by paragraph 4.b.v. Authentication for user access to these systems must meet the requirements of paragraphs 4.a, 4.b, 4.c and 4.e.

**Definitions**

<table>
<thead>
<tr>
<th>Systems Administrator</th>
<th>A person charged with the maintenance and operation of a computer system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials</td>
<td>Those things you either know or have that are used to authenticate you.</td>
</tr>
</tbody>
</table>