Authentication Policy Guidelines for Staff & Students

Overview

These guidelines are intended to assist staff, students and other third parties to adhere to the University of Aberdeen Authentication Policy.

General

1. The most common method for authenticating users at the University of Aberdeen is username and password.
2. Swipe/proximity cards (University ID card) are also used to access to buildings and print and photocopy services; further use may be possible.
3. Other Two Factor Authentication mechanisms and/or devices may be utilised.

Passwords

1. You must never disclose your password, not even to University of Aberdeen Support Staff.
    - Support staff will never ask you for your password. If they need access to your account, they will ask you to log in for them and will turn away while you do so.
2. You should change your password immediately and inform the IT Service Desk when:
    - You suspect or believe that your password has been compromised.
    - You suspect or believe that your password has been exposed electronically, e.g. transmitted over a public network in plain text.
    - You suspect or believe that onlookers (including colleagues) may have seen your password being typed.
3. Passwords should:
    - Be a minimum of 8 characters.
    - Be suitably complex to ensure they are not easily guessed such as:
        i. A random collection of upper- and lower-case letters, numerals, and punctuation characters.
        ii. A random collection of three or more memorable words.
    - Not contain any part of your username.
    - Not be the same as, or similar to, a password you have used before
4. When you change a password, your new password will:
    - Be checked against databases of common words and rejected if found in those databases.
    - Be checked for length.
5. Passwords should be protected in use.
    - Take care to ensure the system you are entering your password on is genuine.
    - If accessing the University (or other) web pages, check the page has the correct URL and is secure. Look for the padlock in the address field.
6. Passwords should not be used for multiple purposes. Use a different password for each account.
7. University of Aberdeen usernames and passwords should not be used with non-University systems and services, e.g. social media, online stores.

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