| | |
|---|---|
| BOND UNIVERSITY | **PASSWORD MANAGEMENT PROCEDURE** |
| Contact Officer | Head, Information Security Services |
| Date First Approved | 10 March 2008 |
| Approval Authority | Director, Information Technology Services |
| Date of Next Review | 22 August 2025 |

## 1. OVERVIEW

The purpose of this Procedure is to establish a standard for the creation of secure passwords, the protection of passwords, and the frequency of password change.

Credentials, consisting of a username and password are an important aspect of information security, as they are the front line of protection for most computer systems. Compromised credentials are the leading cause of data breaches reported to the Australian Government. A poorly chosen password may result in the compromise of your account and Bond University's systems. As such, all authorised users of Bond University services (including all third parties such as contractors and vendors with access to Bond University systems) are responsible for ensuring their passwords are secure, by understanding and taking the appropriate steps, as outlined in this procedure to create a strong password.

## 2. APPLICATION

All Bond University authorised users

## 3. ROLES AND RESPONSIBILITIES

| Role | Responsibility |
|---|---|
| Director, ITS | Approve any variation to this procedure. |
| Head, Information Security Services | Author any variations to this procedure. |

## 4. THE PROCEDURE

### General

a) Two levels of password guidelines are used, each with a different set of requirements for password creation and reset, and these are described in the User Password Guideline Matrix below.
b) The assignment of a password guideline is based on an individual's role(s) at the University and is not an automatic result of an affiliation or staff position.
c) Passwords may be required to change as per the password guideline matrix. This will be enforced at the operating system level i.e. Windows, and at the application level, where possible (this will be dependent on system capabilities).
d) Passwords must not be inserted or attached into email messages or other forms of electronic communication that retain knowledge of pasted or inserted data (e.g., SMS, Chat, emailed documents, etc)
e) Password guidelines and security roles, and the resulting association of password guidelines to a user, are managed by Information Technology Services.

### Password Protection Standards

All passwords are to be treated as sensitive, confidential Bond University information. The following password standards should be adhered to:

a) Do not reveal a password over the phone or electronic communication to anyone;
b) Do not hint at the format of a password (e.g., "my family name");
c) Do not reveal a password on questionnaires or security forms;
d) Do not share a password with family members;
e) Do not reveal a password to co-workers, including while on vacation or other leave;
f) Do not create a new account in ANY application or website using your Bond University password;
g) Do not use the "Remember Password" feature of applications or websites, as malicious software can retrieve these stored passwords;
h) Do not store passwords in a file on ANY computer system (including mobile devices) unless the system is a password management platform specifically designed for storing passwords;
i) Temporary passwords should be changed at first log on;

j) If a password has been compromised or there is a possibility it may have been compromised then users should change their password immediately and notify Information Technology Services.

**User Password Construction Guidelines**

Everyone is responsible for setting a **strong** password on their Bond University IT account. Strong passwords have the following characteristics:

a) Are at least twelve alphanumeric characters long and preferably a passphrase (Oh1stubbedmyt0e);
b) Are not a singular word or name in any language, slang, dialect, jargon, etc., even when combined with other numbers or symbols;
c) Are not based on personal information, names of family, etc.;
d) Are not based on information that is accessible via social media or known by family, friends or colleagues;
e) Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or choose unrelated words and string them together with spaces. For example, “cat car cloud”.

When setting or changing your password Bond University’s password protection system will automatically take the following actions, which may lead to the password being rejected:

a) Place a lower rating on passwords that contain weak or easily guessable words, such as password, qwerty, Bond, Gold Coast etc. even if these words include multiple character sets (e.g. p@55w0rd, g0ld c0@st);
b) Reject passwords that are the same as the examples mentioned in the aforementioned construction guidelines;
c) Reject passwords that contain your username.

**User Password Guideline Matrix**

| Description | Example |
|---|---|
| Standard | Authorised Users including students, Staff, Alumni, Contractors |
| High | Privileged access administrative accounts |

| Description | Standard | High |
|---|---|---|
| Minimum length of password | 12 | 15 |
| Maximum age of password (in days) | Indefinite | Indefinite |
| Password minimum age for reset (in days) | 0 | 0 |
| Password uniqueness/history | 5 | 5 |
| Failed attempts before lockout | 5 | 3 |
| Password Complexity | False | False |
| Multi-factor authentication | True | True |

**Application Development Standards**

Application developers must ensure their programs adhere to the following security guidelines:

a) Applications must not locally store individual user passwords but instead should support federated authentication (SAML, AAF) of individual users;
b) Applications should not store system passwords in clear text or in any easily reversible form;
c) Applications should provide role management capabilities, such that one user can take over the functions of another without having to know the other's password.

**Service Accounts, Shared Secret and API keys**

Non-user based service accounts, Shared secret keys and API keys must conform to the following security requirements:

a) Group managed service accounts (gMSA) with defined endpoints are preferred for Windows service accounts.
b) Password or key length of at least 32 characters for other services.
c) Password or keys must be generated via a random-generator using alphanumeric characters to increase the entropy.
d) Must be audited for which individual have knowledge of this password, secret or key access, and changed if there are personnel changes.
    - At least every 12 months.
    - When associated personnel have left the organisation or changed role

**Exclusions**

a) Infrequently there are certain circumstances whereby a particular vendor, technology or business process is unable to comply with this Policy.
b) Information Technology Services reserves the right to approve exceptions through a case-by-case review process, requiring final sign-off from either the Head of Information Security Services or Director or Deputy Director of ITS.

## 5. DEFINITIONS, TERMS, ACRONYMS

| | |
|---|---|
| **Authorised User** | A person who has been provided with an Authentication Credential by the University to access University ICT Services. |
| **Authentication Credential** | User identification and password, username and passcode, PINs or other secret means to gain access to University ICT Services |

## 6. RELATED DOCUMENTS

ICT Acceptable Use Policy

## 7. MODIFICATION HISTORY

| Date | Sections | Source | Details |
|---|---|---|---|
| 22 Aug 2022 | All | ITS | Reflect additional new procedures and standards around password management |
| 19 November 2019 | | ITS | |