Password Management Process

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	02/02/2017
V 0.2	Andrew Clarke	Approved CISA 03/02/2017	03/02/2017
V1.0	Andrew Clarke	Approved Info SubCommittee 27/04/2017 with amendment that the password should never be divulged with no exceptions	27/04/2017
V1.1	Andrew Clarke	Align with new Password Policy for 12 character minimum length passwords	16/07/2019
V 1.2	Andrew Clarke	Process encryption/hashing of stored passwords and transmitted passwords	18/07/2019

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Document Owner: Andrew Clarke	Document Approver: Mick Jenkins
Cyber & Information Security Manager	Chief Information Security Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Process establishes the area within Brunel University London covering Password Management.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Systems Manager	Is responsible for maintaining and managing password policies on IT systems and infrastructure.
Network Manager	Is responsible for maintaining and managing password policies on network systems.
Head of Development and Application Services	Is responsible for maintaining and managing password policies on application and web systems.
Application Owners	Is responsible for maintaining and managing password policies on applications.
Cyber & Information Security Manager	Is responsible for maintaining password policy best practice and ensuring compliance with legislative and regulatory requirements.
All Users	Are responsible for ensuring passwords are chosen that remain compliant with this Policy.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A9 – Access Control
ISO 27001:2013 Conformance Control	Information Classification Objective A.9.3.3 Password Management System

1.4 Scope

This document is valid for all University information systems (Desktops, laptops, servers, network equipment, virtual machines, SAN, OpenLDAP etc.) and all applications that are password protected. (SITS, eVision, Office365 etc.)
This excludes Third party systems that require University access.

This current Policy stands for a minimum baseline in terms of Security requirements. This policy applies to all Users (whether employees, contractors or temporary staff and third party users) and all owners of University information security assets or systems are required to be aware of and to follow this policy.

1.5 References

Brunel Acceptable Computer Use Policy – BACUP;
BUL Network Account Policy;
BUL Extended-privilege account Policies and Procedures;

2.0 Password Management Introduction

2.1 Process Summary

This Process defines the steps required to comply with the minimum set of requirements for strong passwords as defined by the BUL-POL-9.4.3 - Password Policy.

If for technical reasons it's not possible to comply with one or more of the requirements listed below, then the maximum feasible must be accomplished after the Cyber & information Security Manager's approval.

As the password is the first line of defence against unauthorised access, it is critical that this line of defence is made effective with a good password management policy. In addition, users should also be educated and aware of the best practices in choosing and handling passwords. The use of an insecure password may have a direct impact on the security of the whole system. As such, all users need to be responsible for taking appropriate steps to select and secure their passwords.

As authentication via the Identity and Access management system controls access to all resources, it is important that the authentication process is secure enough to protect these resources. This protection should satisfy the requirements of the most critical application. The single authentication process should not be weaker than the original authentication method used by the various applications, otherwise, the result is a downgrade in security level.

3.0 Password Management

3.1 Account password creation

Information Services will generate a *password* of an adequate level of complexity and security, and will issue this password to the account-holder as the account's secondary access key.

3.2 Password Confidentiality

This password must not be divulged to any other person and the continuing security of access is the responsibility of the account-holder, through the maintenance of a secret password of an adequate level of complexity and security. If the security of the password is known or suspected to be compromised (actually or potentially), it is the duty of the user to inform Information Services immediately. Information Services, on learning from any reputable source of any such actual, suspected or potential compromise, may act (without the necessity of prior notification of the accountholder) to retrieve any diminution in security by revoking the password associated with any account, substituting another password of an adequate level of complexity and security, and may take any further steps deemed necessary to maintain the integrity of Brunel University London data. Following any such action, the account-holder must attend Information Services Service Desk before access may be resumed. Information Services will not store a password *en clair*, in hardcopy or electronic form, beyond the initial issue to the account-holder: this means that a lost password cannot be re-issued, and that any succeeding access rights must be authenticated using a freshly generated Password. Since the disclosure or unauthorised discovery of any password compromises the security of the entire Brunel University London data network, any transgression may lead to disciplinary proceedings appropriate to a serious breach of Brunel University London regulations. The delegation of any access is a serious matter, and must be carried out in accordance with the rules and policies drawn up by Brunel University London, by JANET, and by other relevant parties. All users should note particularly that it is forbidden to disclose any password which might allow another person to gain access in a manner which could lead to personation of the account-holder.

3.3 Administrator accounts / Extended privileges (EP)

Information Services may provide a member of staff who requires elevated access privileges with an additional network account from which such actions may be carried out in a standard auditable way.
Examples of such an account would be a *technical administrator account* (or *ADM account*) or a database administrator account (or *DBA account*). Where this Process refers to an extended-privilege account in general, it will be called an *EP account*.

By this means, if an EP account-holder's standard network account becomes compromised, then these additional privileges are not also compromised. It also means that this additional access can be quickly stopped (by disabling the EP account) without disabling the standard account (which would result in the staff member being cut off from e-mail, etc.).

Owing to the privileged nature of EP account, and the elevated risk of compromise from such an account, password policy is different to the normal password policy.

- The EP account must have a stronger and more secure password. As for all accounts, this password must not be shared with anyone else. Failure to abide by this instruction will be considered a serious lapse of discipline;

- The EP account must be used only for the tasks approved at the time of the account's creation. Any abuse of this account may result in it being disabled with no warning to the account-holder, who may be subject to disciplinary proceedings;

- The use (or attempted use) of an EP account by anyone other than the account-holder (including the holder of another EP account) may result in disciplinary proceedings;

- The EP account should only be active during the time needed to carry out the required tasks. Leaving an EP account logged into a PC or server beyond such minimum time will be considered a serious lapse of discipline;

The use of an EP account is subject to all other policies, rules and regulations of the University:

3.4 Password selection

Examples of Bad Passwords

The following are examples of badly chosen passwords that can be easily guessed or cracked using password crackers freely available on the Internet.

- "password" - the most easily guessed password;
- "administrator" - a login name;
- "cisco" - a vendor‟s name;
- "John Smith" - a person‟s name;
- "aaaaaaaa" - repeating the same letter;
- "abcdefgh" - consecutive letters;
- "23456789" - consecutive numbers;
- "qwertyui" - adjacent keys on the keyboard;
- "computer" - a dictionary word "computer12" - simple variation of a dictionary word;
- "c0mput3r" - simple variation of a dictionary word with o substituted by 0 and e substituted by 3;
- “28/06/1986” – a date of birth or variant of a date;
- “football”
- “letmein”
- “money”

Do not use the following in password selection:

- Do not use your login name in any form (as-is, reversed, capitalised, doubled, etc);
- Do not use your first, middle or last name in any form;
- Do not use your spouse's or child's name;
- Do not use other information easily obtained about you. This includes Passport or ID card numbers, license numbers, telephone numbers, birth dates, the name of the street you live on, and so on;
- Do not use a password that contains all digits, or all the same letters;
- Do not use consecutive letters or numbers like "abcdefgh" or "23456789";
- Do not use adjacent keys on the keyboard like "qwertyui";
- Do not use a word that can be found in an English or foreign language dictionary;
- Do not use a word in reverse that can be found in an English or foreign language dictionary;
- Do not use a well-known abbreviation e.g. BUL, HMRC, RSVP, DOB;
- Do not use a simple variation of anything described in 1-10 above. Simple variations include appending or prepending digits or symbols, or substituting characters, like 3 for E, $ for S, and 0 for O;
- Do not reuse recently used passwords;
- Do not use the same password for everything; have one password for non-critical activities and another for sensitive or critical activities;

DOs

- Use a password with a mix of at least twelve mixed-case alphabetic characters, numerals and special characters;
- Use a password that is difficult to guess but easy for you to remember, so you do not have to write it down;
- Use a password that you can type quickly, without having to look at the keyboard, thereby preventing passers-by seeing what you are typing;
- Use a Passphrase, it is more secure as it is a sequence of words e.g. IgotontheU4bus!

Handling Passwords

Don't

- Do not write down your password, particularly anywhere near your computer or file it in a box file with the word 'password' written on it;
- Do not tell or give out your passwords to other people, even for a very good reason;
- Do not display your password on the monitor;
- Do not send your password unencrypted, especially via email;
- Avoid using the 'remember your password' feature associated with some websites, and disable this feature in your browser software;
- Do not store your password on any media unless it is protected from unauthorised access (e.g. encrypted with an approved encryption method);

Do

- Change the default or initial password the first time you login;

- Change your password immediately if you believe that it has been compromised. Once done, notify the system/security administrator for follow up action;

Administrator accounts / Extended privileges (EP)

Don't

- Do not send passwords to users unencrypted especially via email;
- Do not disclose or reset a password on a user's behalf unless his or her identity can be verified;
- Do not allow the password file to be readable publicly;

Do

- Choose good passwords as initial passwords for accounts;
- Use different passwords as initial passwords for different accounts;
- Request users change the initial password immediately upon receiving the new password.
- Change all system default passwords, including service accounts after installing a new system;

4.0 Secure Password storage and transmission

4.1 Encryption and Hashing

The University BUL-POL-9.3.3 - Password Policy states:

- Passwords MUST NEVER be stored in clear text in any application or on any system.
- Passwords MUST NOT be transmitted in clear text format over the network, and NEVER together with the User ID in the same message or email.

There are no reasons for storing or transmitting passwords in clear text for users or applications, this is an unambiguous policy.

To ensure that passwords are neither stored nor transmitted in clear text, Passwords MUST be stored as a HASHED[1] string using either SHA-1 or SHA-2 algorithms with SALT[2] for additional security.

If Hashing cannot be done, (i.e. when it is a necessity to recover the password) the password must be encrypted using FIPS 140-2 Compliant Algorithms (BUL-POL-10.1 - Cryptographic Policy) i.e. Asymmetric Key (public-key) DSA, RSA, ECDSA or Symmetric Key - AES, Triple-DES, Escrowed Encryption Standard and that the symmetric password is stored using PKI (asymmetric encryption).

The credibility of the third party should be ascertained with the exchange public keys to ratify identities before sending the encrypted passwords.

[1] Hashing is an ideal way to store passwords, as hashes are inherently one-way in their nature. By storing passwords in hash format, it's very difficult for someone with access to the raw data to reverse it (assuming a strong hashing algorithm and appropriate salt has been used to generate it).

[2] Salting is the randomising of the hashes by appending or prepending a random string