BLOOMSBURY INSTITUTE LONDON

Password Policy

Index

Document Version Control

Document Version	Committee	Committee Action	Date
	SMLT	Approved	June 2020
		Date in force	**1 September 2020**

The Password Policy will be reviewed annually by our Senior Management and Leadership Team (SMLT). Any amendments require the approval of our Senior Management and Leadership Team.

1. Introduction

Passwords are broadly used to authenticate users to access IT resources, and to provide the front line of defence against unauthorised access. Good password management will minimise the likelihood of user accounts being easily compromised and mitigate risks to information and IT systems.

This policy will define our expectations in terms of the use and management of passwords to ensure the security of devices, IT systems and services. It includes appropriate technical and procedural controls to reduce risk and meet the requirements of other IT security policies.

The purpose of this policy is to set the standard for creating strong passwords and keeping them safe.

This policy applies to all users of our computing facilities and/or systems. It is the user's responsibility to choose strong passwords and protect them.

2. Password usage and management

2.1 Secrecy and divulgence of passwords

Individual users are personally responsible for maintaining the secrecy of their passwords and for controlling access to their user accounts through password security.

Passwords are not to be divulged by users to anyone except a member of IT Services (ITS) whilst in their presence and only when there is a fault with the user's computer or the user's network access. In such circumstances the password must be changed as soon as the ITS member has resolved the issue. Passwords must never be divulged over the telephone or in an email.

2.2 Password storage

It is the responsibility of systems administrators to ensure that only hashed/encoded forms of password are stored in their respective systems.

It is the responsibility of individual users to ensure they do not store the password anywhere in the computer/browsers.

2.3 Password complexity and choice

2.3.1 Password complexity

We will not necessarily configure our systems to enforce password complexity, but users are required to choose strong passwords.

2.3.2 Password choice

Users are always required to choose sensible strong passwords in order to protect their 'electronic identity', prevent unauthorised access to systems, and preserve the availability and integrity of data.

Guidelines for choosing strong passwords can be found in Appendix A. All passwords used must be unique i.e. you are not allowed to recycle passwords or use the same one for more than one system.

2.4 Password ageing and forced password change

2.4.1 Password ageing

ITS enforces password ageing for all users. All passwords will expire 12 months after they have been issued except passwords that provide access to certain financial and other sensitive applications.

Password ageing is enforced for financial and sensitive applications, system-forced changes will occur at least every 180 days.

In exceptional circumstances, ITS can enforce a password change across the institution.

2.4.2 Forced password change

ITS staff, who operate their own systems (independent of Active Directory) are required to implement a process to force-change the password of newly created accounts at first log-on, where this is technically possible.

2.5 Unforced password change

2.5.1 Users at initial logon

All user logins must be configured to force-change their initial default passwords at first logon, and the users are required to change them themselves at the first logon.

2.5.2 Default passwords

ITS staff, who configure new systems and set up services are to ensure that all password settings are changed from their default settings before moving platforms into production.

Default passwords must be changed as soon as possible after a new system is acquired, or after any database or operating system upgrades that re-instate default accounts and passwords.

Peripherals with embedded software, such as printers, plotters and webcams, often have default or no passwords which must be reset/set.

2.5.3 System-level passwords

All system-level passwords (e.g. root, enable, application administration accounts, etc.) must be changed on at least an annual basis. All the systems will automatically prompt the password change 1 month before the due date and will force to change the password after the due date.

2.5.4 User passwords

It is recommended that user passwords are changed at least every six months. They must be changed immediately on any occasion that a user believes that someone else may be aware of their password and on all occasions when an incident of malpractice is discovered or suspected.

2.6 Systems-level (administrator and super-user) passwords

Staff may only have access to system-level passwords on a need-to-know operational basis, not because they may possibly need them at some time.

Shared administrator and super-user (global) passwords are not to be used on production systems except where passwords are hard-coded into applications.

On Windows systems passwords for privileged accounts must be 15 characters or more.

ITS staff are to be allocated secondary accounts which have the appropriate rights and privileges to enable them to support the systems and services for which they are responsible. This should be done in all cases where hard-coded passwords are not required.

Linux users are to use their own user accounts to SU to Root.

2.6.1 Hard-coded and service account passwords

Hard-coded and service account passwords must never be used to log on to servers.

Where practical, hard-coded and service account passwords are to be changed on a quarterly basis and the change is to be performed in a synchronised manner to avoid operational problems. Where password changes are due on a Friday, they are to be deferred until the next working day.

2.7 Shared passwords

Passwords are not to be shared by users, except in the case of ITS staff who are responsible for the maintenance of systems and services that utilise hard-coded passwords.

Where there is a need for several users to have access to common data and mailboxes, such as those working collaboratively, access must be controlled in accordance with the User Management and Access Control Policy.

All activities carried out on IT systems using an individual's username and password can only be traced to the individual, and these activities are logged, and audit trails can be generated to analyse them. Furthermore, generic usernames and passwords make it arduous to trace an activity to an individual due to the login information being used by various people. Consequently, it is important that passwords are not shared. Sharing of passwords may result in an individual being held responsible for someone else's actions.

2.8 Compliance monitoring

Password cracking tools may be operated by ITS staff on a random or periodic basis in a bid to identify weak passwords. Before doing this, authority must first be obtained from the Head of IT Services.

2.9 Password resets

2.9.1 Staff passwords

The identity and association of a person with a particular account must be verified by ITS staff prior to resetting their password.

Passwords must generally only be reset when the person requesting a password reset is present and has been properly identified and verified against held documentation as being the account holder. However, ITS may reset the passwords of staff by telephone using agreed shared personal information.

Only line managers and heads of divisions/departments may request the password reset of their members' accounts, where the user has forgotten their password and is unable to attend the Help Desk. Passwords must not be reset on the basis of any other third-party request, regardless of the status of the individual making the request.

However, ITS may request a reset of a user's password in order to identify or fix a fault, and a line manager can request a user's password be re-set when it is necessary to migrate services in the user's absence. In both cases, the user is to be informed of the new password at the first opportunity by the person who has requested the reset and is to change this at the next logon.

2.9.2 Student passwords

A password self-service re-set facility is provided to all enrolled students at the time of account creation, the use of which is mandatory. All students are required to register with the service when they log in to the Office 365 portal and provide answers to security questions. To re-set their password, students will need to answer a selection of the questions for which they have provided answers. All students' passwords must:

- comprise a minimum of eight characters

- contain at least one number
- not have been used before;
- contain at least one upper case letter
- contain at least one lower case letter
- contain one special character

2.9.3 Help and assistance

Users who forget their password may use the password re-set facility in order to establish details. In order to use this facility, users must first register. Any questions regarding the use and management of passwords should be directed to the ITS Help Desk (at Dilke House) which operates Monday to Friday from 09:00 hours to 17:00 hours (except bank holidays).

3. Protecting your passwords

In order to ensure that both our data and user's information are protected, system users are held responsible for safeguarding passwords and access identities. Passwords and identities must not be shared. System users are responsible for all use of information systems and technology and for any information stored or communicated using their identity or password.

All usernames issued are unique and are not reused. Although usernames are not secret, they should be treated as personal. Details are not published, and they should not be divulged to others.

Passwords on the other hand are secret and users are responsible for protecting their own.

A computer that is left unattended and logged on gives anyone access to information that should only be accessible to the authorised user. If a computer is left unattended, it should be shut down or locked using a password access 'hot-key' (Windows + "L") or password protected screen saver.

4. Related regulations, policies and procedures

- User Management and Access Control Policy
- Network Policy
- Information Security and Management Policy

5. Review of Password Policy

The Password Policy will be reviewed annually by our Senior Management and Leadership Team (SMLT). Any amendments require the approval of our Senior Management and Leadership Team.

Appendix A

Selecting a strong password

- When you choose a password, you should make it personally and easily memorable but difficult for others to guess:
    - Make sure that your password comprises at least 8 characters, which should contain at least one number, one upper case letter, one lower case letter and one special character;
    - Never use your username in any form as your password;
    - Never use your surname or given name in any form as your password;
    - Don't use any information about you that is easily obtainable, such as your car registration number, your birthday, your child or pet's name, your favourite holiday destination or your favourite sports team or hobby;
    - Don't use word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.;
    - Avoid the use of an ordinary word preceded or followed by a digit (e.g., secret1, 1secret);
    - Don't change your password by simply adding a number every time you have to change it;
    - Don't reuse or recycle your password;
    - If someone demands a password, refer them to this Policy or have them contact the Head of IT Services.
- In addition, make sure that your password is:
    - Private. It should be used and known by you only. You wouldn't like it if your identity was stolen, so why give it away?
    - Not shared, even with your colleagues. If you have a member of staff who has a need to access your data, this can be facilitated through file permissions for both Exchange and File Store;
    - Secret. It does not appear in clear text in any file or programme in any medium.
    - Never write your password down;
    - Don't use the 'Remember Password' feature of applications;
    - Immediately change your password if you think that it has been revealed to anyone else or compromised;
- Use one of the following methods to create a memorable but strong password:
    - Use the first letter of each word in a memorable phrase, saying, nursery rhyme or song title. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. Please do not use this example.
    - Substitute one or more letters with a numeric character (e.g. I = 1, A = 4, S = 5, L = 7 or O = 0);

- Take two words and splice them together with one or more non-alphanumeric character(s), or;

- Take an ordinary word or phrase and change, delete or add characters so that it becomes nonsensical.