www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

# Royal Borough Windsor & Maidenhead

# Password Policy

## October 2022

**“Building a borough for everyone – where residents and businesses grow, with opportunities for all”**

**Our vision is underpinned by six priorities:**

*Healthy, skilled and independent residents*
*Growing economy, affordable housing*
*Safe and vibrant communities*
*Attractive and well-connected borough*
*An excellent customer experience*
*Well-managed resources delivering value for money*

# Contents



Frequently used acronyms

| | |
|---|---|
| IT | Information Technology |
| RBWM | Royal Borough of Windsor & Maidenhead |
| 2FA | Two Factor Authentication |

# 1 PURPOSE

1.1 The purpose of this Password Policy is to ensure that the applicable and relevant security controls are set in place in line with the Royal Borough of Windsor and Maidenhead requirements.

1.2 This policy Passwords are an important aspect of computer security and a critical component of information security. A poorly constructed password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems and can compromise our entire infrastructure.

1.3 All staff, including contractors and vendors with access to the Royal Borough of Windsor and Maidenhead systems, are responsible for taking the appropriate steps, as outlined in this policy to select and secure their passwords and follow the guideline provided with best practices for creating secure passwords.

1.4 The purpose of this policy is to establish a standard for the use of usernames and passwords and the protection of those passwords.

# 2 SCOPE

2.1 This Password Policy aims to ensure that the integrity and security of the council's data and other resources remain protected.

2.2 It outlines a set of rules pertaining to password security standards.

2.3 The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any business system.

2.4 This policy applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

# 3 APPLICABILITY

3.1 This policy applies to all council employees and RBWM Councillors. This policy also applies to contractors, temporary, agency staff, partners and others working in a similar capacity that can access, manage, or process information assets of the council.

They are also accountable for understanding and adhering to the guidance contained in this policy and any applicable supporting policies and procedures. All applicable persons listed above are referred to as 'users' in this policy.

# 4 AUTHORISATION

4.1 Only authorised persons will have access to council assets and systems or accessing the council IT or mobile network. Any user that deliberately or inadvertently accesses the council IT or mobile network or systems unauthorised, will be in breach of this policy.

4.2 For any council business:

4.2.1. Users accessing council IT facilities must comply with all council policies and procedures.

4.2.2. Managers and Team Leaders must ensure their staff comply with this policy and provide advice to them.

4.2.3. Managers and Team Leaders must ensure security incidents are raised in response to IT access security concerns or security breaches as covered in the Reporting security incidents policy.

4.2.4. IT Services provide technical solutions to support different IT access security levels, depending on the sensitivity and value of the data accessed. Administer, control and monitor access to IT facilities and systems.

4.2.5. IT Services ensure that privileged and systems administrator access is strictly controlled based upon a valid business justification and specific job requirements as approved by the user's line managers.

# 5 POLICY COMPLIANCE

5.1 Compliance Measurement

5.1.1. All users must comply with this policy.

5.1.2. IT Services will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1.3. If you do not understand the implications of this policy, how it may apply to you, or your security responsibilities when working with the council, please seek advice in advance from your line-manager or contact the council's Data Protection Officer at dpo@rbwm.gov.uk.

5.2 Exceptions

5.2.1. Any exception to the policy must be approved by the IT Senior Management Team in advance.

5.3 Non-Compliance

5.3.1. Any breach of this policy may be subject to disciplinary action under the council's disciplinary procedures, up to and including dismissal. In circumstances where it is believed that a criminal offence has been committed the matter may be reported to the Police.

# 6 RESPONSIBILITIES AND RISK

6.1 The purpose of providing the internet service is primarily provided to give council employees and Councillors:

6.1.1. Access to information relevant to the council's business obligations.

# 7 PASSWORD CREATION

7.1 All passwords must conform to the Password Construction Guidelines.

7.2 All user-level passwords must consist of sixteen (16) or more characters.

7.3 All Administrator and Service Level passwords must consist of twenty-four (24) or more characters.

7.4 Users must use a separate, unique password for each of their work-related accounts.

7.5 Users may not use any work-related passwords for their own, personal accounts.

7.6 Users will not reveal their user credentials; usernames, IT access codes, passwords, or passphrases to anyone, unless requested by RBWM IT Service support. The password must be updated by the individual after the support has been completed.

7.7 User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges.

In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts

7.8 Passwords/Passphrases will be at least sixteen (16) characters.

7.9 Do not use any part of the username in the password.

7.10 Truncation of the secret (password) will not be performed when processed.

7.11 No password hints (password suggestions).

7.12 No knowledge-based authentication (e.g. who was your best friend in high school?).

7.13 No SMS for 2FA (for 2FA use a one-time password from an app - Microsoft or Google Authenticator).

# 8 MOBILE DEVICES

8.1 The Alphanumeric: Passcode must be a mix of numbers and letters.

8.2 Screen Lock passcode complexity requirements of at least six characters with an uppercase, lower case, number, and special character.

8.3 Minimum length of Screen Lock passcode: 6 (six) characters.

8.4 Number of sign-in failures before wiping device: 10 (ten) attempts.

8.5 Maximum minutes of inactivity until screen locks: 1 (one) minute.

8.6 Passcode expiration (days): 182 days (6 months).

8.7 Prevent the reuse of a previous passcode: 10 (ten) changes

8.8 Require passcode when device returns from idle state.

8.9 Simple passcode: Set to Block so users can't create simple passwords, such as 123456 or 000000.

# 9 PASSWORD CHANGE

9.1 Except Force a password change on first logon.
9.2 Password expiration (days): 365 days (12 months).

9.3 Passwords should not be changed unless there is reason to believe a password has been compromised or whenever the IT system prompts you to change it.

9.4 The same password cannot be reused within the last 10 (ten) changes.

9.5 Password cracking or guessing may be performed on a periodic or random basis by security professionals using known password dictionaries. If a password is guessed or cracked during one of these scans, the user will be required to change it to be compliant with this policy.

# 10 PASSWORD PROTECTION

10.1 When using external systems or visiting web sites not affiliated with the RBWM, users should create a password different from any of their RBWM passwords.

10.2 Multiple users should not share the same user account.

10.3 Never reveal your user credentials; usernames, IT access codes, passwords, or passphrases to anyone, unless requested by RBWM IT Service support. The password should be updated by the individual after the support has been completed.

10.4 Do not save passwords within an application (e.g. a tablet/cell phone or browser).

10.5 Never use a 'remember identifier or password' function because it makes access less secure.

10.6 Do not use any part of your user identifier within the password.

10.7 Avoid using the same password to access different RBWM systems.

10.8 Do not use the same password for systems access inside and outside of work.

10.9 Only store your passwords in an encrypted electronic file.

10.10 Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.

10.11 Avoid information that can be easily guessed (e.g. birthdays, children names, etc.). More samples of weak passwords that can easily be discovered include words picked out of a dictionary, names of children and pets, car registration numbers, simple patterns of letters from a computer keyboard, or any variation of the word ‘password’.

10.12 User identifiers and passwords must not be communicated via the same channel (i.e.. In-person, email, instant messaging, or phone).

10.13 Any user suspecting that their password may have been compromised must report the incident by email to security@rbwm.gov.uk and change all passwords.

# 11 APPLICATION DEVELOPMENT

11.1 Application developers must ensure that their programs contain the following security precautions:

11.1.1. Applications must support authentication of individual users, not groups.

11.1.2. Applications must not store passwords in clear text or in any easily reversible form.

11.1.3. Applications must not transmit passwords in clear text over the network.

11.1.4. Applications must provide for some sort of controlled role management, such that one user can take over the functions of another without having to know the other's password.

# 12 MULTI-FACTOR AUTHENTICATION

12.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

# 13 LOCK ACCOUNTS

13.1 To prevent brute-force attacks,

13.1.1. accounts will be locked after 6 (six) consecutive failed login attempts.

13.1.2. accounts must stay locked for 30 (thirty) minutes, or until a system administrator resets the account.

# 14 SYSTEM ACCOUNTS

14.1 Never use shared passwords between different systems (including local passwords).

14.2 Never use the same passwords between local and domain accounts.

14.3 Rename the Local Administrator Account on all systems.

14.4 Use unique local administrator usernames for each system.

14.5 Never leave Domain Administrator Accounts logged on to Servers (locked screen).

14.6 Never run local services and/or schedule tasks in the context of a Domain Administrator account.

14.7 Ensure that all default passwords/settings are changed before systems are put into production.

14.8 Limit the number of 'cached' tokens that are held locally on servers. Cached tokens are required for authentication if a Domain Controller isn't available. However, in most modern Windows Networks with multiple domain controllers and multiple redundant network paths the chance of a Domain Controller being unavailable is extremely unlikely. 10 (ten) 'cached' tokens are stored by default. See "Interactive logon: Number of previous logons to cache (in case domain controller is not available)" Group Policy, under "Computer Configuration > Windows Settings > Local Policies > Security Options".

14.9 Ensure that IT staff have separate 'User' and 'Admin' accounts and that Domain Admin privileges are only granted when necessary. Where Domain Admin privileges are granted, ensure that they are only used to login to Domain Controllers, with delegated authority to lower privileged accounts where applicable.

14.10 Strict operational controls shall be enforced as part of the device deployment for all devices that have no technical controls available to enforce password complexity.

14.11 Accounts that utilise SPNs (Service Principal Name) are set with a Passwords / Passphrases of more than 24 (twenty-four) characters.

# APPENDICES

## RELATED STANDARDS, POLICIES AND PROCEDURES

- Reporting Security Incidents Policy.
- Disciplinary procedure.
- Password Construction Guidelines.
- UK Data Protection Act 2018.
- Information Security Management Standard ISO/IEC 27001:2013.
- NIST SP800-63.3 standards.
- Terms and Conditions of Employment – this states that employees are required to follow the council’s policies, procedures, and guidelines, including those for security.

| | |
|---|---|
| **Document name** | Password policy |
| **Document author** | Infrastructure security manager |
| **Document owner** | **Head of HR, Corporate Projects and IT** |
| **Accessibility** | |
| **File location** | |
| **Date destruction** | |
| **Circulation restrictions** | |

**How this document was created**

| **Version** | **Date** | **Author** |
|---|---|---|
| Version 1 | 25/06/2020 | Infrastructure security manager |
| Version 2 | 23/10/2022 | Strategic Lead, IT Services |
| Version 3 | | |

Next review date: 22/10/2024