Password Policy

Design Magic Ltd

1. Purpose

This policy establishes requirements for the creation, maintenance, and protection of passwords at Design Magic ensuring the security and integrity of company systems and data. It aims to reduce the risk of unauthorised access and comply with UK data protection legislation, including the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).

2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and other individuals who access Design Magic systems, networks, cloud services, or sensitive information, regardless of location or device used.

3. Definitions

- Password: A secret string of characters used to authenticate a user's identity.
- Multi-Factor Authentication (MFA): An authentication method requiring two or more verification factors.
- Privileged Account: An account with elevated permissions, such as administrator rights.
- End User: Any person accessing company resources.

4. Password Creation Requirements

- Passwords must be unique and not reused across different systems.
- Passwords must contain at least twelve (12) characters.
- Passwords must include at least three of the following four categories:
- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters (e.g., !, @, #, $, %, ^, &, *)

Passwords must not contain the user's name, username, or easily guessed words (such as "password", "123456", "qwerty", or the company name).
Passwords must not be based on easily discoverable information such as birthdays, anniversaries, or favourite sports teams.

5. Password Management

- Passwords must be changed immediately if there is suspicion or evidence of compromise.
- Users should not change passwords more than once per day.
- Where technically feasible, users will be prompted to change passwords at least every ninety (90) days. Privileged accounts must change passwords every sixty (60) days.
- Users must not reuse any of their previous twelve (12) passwords.
- Password history must be maintained to prevent reuse.
- Password managers approved by IT may be used to generate and store passwords securely.
- Multi-factor authentication (MFA) must be enabled wherever possible, especially for remote access and privileged accounts.

6. Password Protection

- Passwords must never be shared with anyone, including colleagues, managers, or IT personnel, unless officially required and authorised by IT for troubleshooting or support purposes.
- Passwords must not be written down or stored in plain text.
- Passwords must not be sent via email, chat, or any other insecure method.
- When entering a password, ensure no one observes or records what is being typed.
- Default or vendor-supplied passwords must be changed before systems are put into production.
- Temporary passwords must be changed at first login.
- Any suspected password compromise must be reported to IT immediately.

7. Privileged Accounts

- Privileged account passwords must follow the same requirements as user accounts but must be at least sixteen (16) characters where technically possible.
- Privileged passwords should be changed whenever an administrator leaves the organisation or changes roles.
- Privileged accounts should not be used for day-to-day activities such as email or web browsing.
- Access to privileged accounts must be monitored and logged.

8. System and Application Passwords

- Service accounts and applications must use strong, randomly generated passwords that meet the requirements above.
- System and application passwords must be stored securely and access restricted to authorised personnel.
- All default passwords on new systems and devices must be changed before deployment.

9. Account Lockout and Recovery

- Accounts will be locked after five (5) consecutive failed login attempts.
- Locked accounts can only be re-enabled by IT support following identity verification.
- Account recovery procedures must require verification of the user's identity through secure means.

10. User Responsibilities

- All users must create and maintain passwords in accordance with this policy.
- Users are responsible for any activities performed using their credentials.
- Users must report suspected or confirmed security incidents, including password compromise, to IT immediately.
- Users must not attempt to circumvent or interfere with any security measures.

11. IT Department Responsibilities

- The IT department must enforce all technical measures required to implement this policy.
- The IT department must provide secure tools for password management and educate users about password security.
- Regular audits of password practices and system access must be conducted.
- IT must monitor for signs of unauthorised access or compromise and respond accordingly.

12. Training and Awareness

- All new staff must receive training on password policies and best practices as part of their induction.
- Annual refresher training will be provided to all staff.
- Awareness materials (e.g., posters, intranet posts) will be distributed regularly to reinforce good password habits.

13. Compliance

- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.
- Serious or repeated breaches may be reported to relevant authorities if required by law.
- This policy will be reviewed annually and updated as necessary to address new risks and technologies.

14. References

- Data Protection Act 2018
- UK GDPR
- National Cyber Security Centre (NCSC) Guidelines
- Design Magic IT Security Policy

15. Policy Acceptance

All users must confirm that they have read, understood, and agree to comply with this Password Policy as a condition of continued access to Design Magic systems.

Last Updated: 25th November 2026
Next Review: 25th November 2027