jrhsupport

PASSWORD POLICY

PASSWORD POLICY

This policy outlines the requirements for creating and managing passwords for all employees of JRH Support. Strong passwords are a critical component of our security and help protect sensitive client and company data. Adhering to this policy is mandatory for all staff.

Password Complexity Requirements
All passwords for company systems and applications must meet the following criteria:

- Minimum Length: Passwords must be at least 12 characters long.
- Character Types: Passwords must include at least three of the following four character types:
    - Uppercase letters (A-Z)
    - Lowercase letters (a-z)
    - Numbers (0-9)
    - Special characters (e.g., !, @, #, $, %, ^, &, *)
- Uniqueness: Passwords cannot be easily guessable (e.g., "password," "123456," your name, company name).
- No Personal Information: Do not use personal information that can be easily found (e.g., birthdays, pet names, family names).

Password Security Best Practices
- Confidentiality: Never share your password with anyone, including colleagues, supervisors, or IT support. Your password is for your use only.
- Storage: Do not write down passwords on sticky notes, whiteboards, or in unencrypted digital files. If you need to store passwords, use an approved password manager. [Company Name] recommends [mention a specific password manager if applicable, or general advice like "a reputable password manager"].
- Phishing Awareness: Be suspicious of any unsolicited requests for your password, whether by email, phone, or text message. [Company Name] will never ask you for your password.
- Reporting Suspicious Activity: If you suspect your password has been compromised or notice any unusual activity on your accounts, report it immediately to your supervisor and/or IT support.
- Strong Passphrases: Consider using a passphrase – a series of random words – that is easy for you to remember but hard for others to guess (e.g., "correct horse battery staple").

Account Lockout Policy
Repeated failed login attempts may result in your account being locked out for a period of time to prevent brute-force attacks. If your account is locked, please contact IT support for assistance.

New Employees and Contractors
All new employees and contractors will be provided with temporary passwords upon onboarding, which must be changed immediately upon their first login to meet the above complexity requirements.

This policy will be reviewed annually and updated as necessary. Your cooperation in adhering to these guidelines is essential for maintaining the security of our data and the privacy of our clients. If you have any questions about this policy, please contact Paul Battershall, General Manager, paul@jrhsupport.co.uk or your line manager.

Paul Battershall
General manager