Password Policy

Overview

This policy is intended to establish guidelines for effectively creating, maintaining, and protecting passwords at Noter.

Scope

This policy shall apply to all employees, contractors, and affiliates of "Noter", and shall govern acceptable password use on all systems that connect to "Noter" network or access or store "Noter" data.

Policy

Password Protection

1. Passwords must not be shared with anyone (including coworkers and supervisors), and must not be revealed or sent electronically.
2. Passwords shall not be written down or physically stored anywhere in the office.
3. When configuring password, try not to use any words that can be found publicly about yourself.
4. User IDs and passwords must not be stored in an unencrypted format.
5. User IDs and passwords must not be scripted to enable automatic login.
6. “Remember Password” feature on websites and applications should not be used.
7. All mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

Password Aging

1. User passwords must be changed every [3] months. Previously used passwords may not be reused. (This applies to all your applications)
2. If you have any problem with the timeline you can contact a moderator

Password Creation

1. All user and admin passwords must be at least [8] characters in length. Longer passwords and passphrases are strongly encouraged.
2. Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
3. Passwords must be completely unique, and not used for any other system, application, or personal account.
4. Default user-password generated by the application is in the format of "username@site_name!" (This applies to all your applications)
5. Default installation passwords **must be changed immediately** after installation is complete.

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

If you believe your password may have been compromised, please **immediately** report the incident to "Noter Team" and change the password.