Overview

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

Scope

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

Policy

Password Creation

1. All user and admin passwords must be at least 12 (12) 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 installation passwords must be changed immediately after installation is complete.

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 “hints,” do not hint at the format of your password (e.g., “zip + middle name”)
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.
8. Many services used at Forward Edge either are required or have the ability to use Multi Factor Authentication (MFA). It is strongly recommended that employees use MFA as a further safeguard with any account in use. Forms of MFA include SMS text messages, cellular phone push notifications, or One Time Password (TOTP) authentication.

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 the Security Operations Center team and change the password.