Password Policy

# Summary

This policy states [company name]’s password complexity, rotation, and retention policy. It is intended to be used on all services, both internal and external, as well as corporate and personal devices.

This is enforced on all devices in all contexts, company-owned or not.

# Length

Passwords must be between 5 and 8 characters in length. To ensure an attacker remains unaware of our maximum password length, any characters beyond the first eight are silently discarded by the login screen.

# Character Set

## Valid

* The alphabetic characters of A through Z, both upper- and lower-case
* The numbers 0-8, inclusive
* Any symbol found on a standard US keyboard that is not listed in the “Invalid” section below

## Invalid

* The space character
* Any file-delimiting character, such as / or \
* The @ and . (dot) caricatures

## Enforcement

To avoid undue pain to our users, Javascript within the login page will validate all characters and enforce all rules, simplifying backend operations by not requiring further validation and enforcement logic to be written.

# Complexity

Passwords must contain at least one character from each of these categories:

* Symbols
* Numbers
* Capital letters

Additionally, no grouping of more than three consecutive characters can be from the same category. For example, cat is accetable but cats is not. As another example, 123 is acceptable but 1234 is not.

# Rotation

Passwords must be updated every 30 days. To avoid attackers being aware of this security measure, users will be provided with no warning and locked out on the 31st day, requiring a “magic link” sent to their corporate email account to facilitate a reset. This will be clearly explained during an employee’s onboarding process.

# Retention

None of a user’s previous 10000 passwords can be reused.

# Other Requirements

To further enhance our security, all login sessions will be limited to 30 minutes of total time and five minutes of idle time.

After three failed login attempts, the user is locked out of all services and must use a “magic link” delivered to their corporate email account to reset their password, in full compliance with all the requirements listed above.

Due to business efficiency concerns, all field employees who use company-owned devices, such as power line technicians, substation employees, mobile repair trucks, and similar, are exempt from all of these requirements to ensure they can quickly and easily reach data critical to their safety.