

**<Company Name>**

**Cyber Security Team Blue Team XX**

**Recipient**:

<Recipient Name>

<Orginization> , <Recipient Location>

**Date**: March X, 2025

**Subject:** Response to Request <Insert Request Title/Number>

Dear <Recipient/Team>,

Thank you for reaching out to our team. We have received the recent request # made to our team. We were asked to thoroughly review our current password policy and create a new policy that uses common industry and government standards. **We were also tasked with deploying this policy to the company infrastructure**. Below, you will see our report and recommended password policies.

Thank you,

Blue Team XX

Executive Summary

Our team observed that the current password policies used within the company infrastructure have default configurations. Although adequate for personal systems and use, this does not conform to the standards described by the National Institute of Standards and Technology (NIST), which are commonly used as the industry standard. These standards strike a balance between complexity to better defend against determined attackers and ease of use which can be an obstacle to users. If we use the default configurations, our customer’s data may be exposed to attackers as malicious actors could eventually guess simple passwords that would be allowed by the weak default policies. By using the standards defined by NIST, we will limit the risk to our systems and the customer data stored within by enforcing passwords that are complex and hard to guess in reasonable time frames. These standards also strike a balance between minimum complexity and ease of use, as if the password requirements are too strict, a user will likely store the password in an insecure manner or reuse passwords between company and personal services increasing the risk of compromise.

After determining the password complexity requirements, our team was able to deploy this policy on **X systems** on the company infrastructure. **Our team has also required each user to reset their password on the next successful login event.** **This is to enforce the new policy and prevent any weak passwords created under the previous policy from being guessed or leaked. As NIST no longer recommends enforcing regularly scheduled password resets unless a breach has occurred, we do not require frequent resets.**

Our team suggests users create passphrases instead of passwords. Passphrases are often easier to remember than passwords as they are various words combined together rather than a string of random letters and characters. Passphrases often use more characters and are equally complex, but easier for users to remember while maintaining security. Further we suggest critical systems be secured using passwordless authentication systems that take advantage of security keys that are even harder to guess and act like a home’s house key.

Password Policy

Our password policy is based on the [NIST SP 800-63B 2024](https://pages.nist.gov/800-63-4/sp800-63b.html) publication.

Each password must meet the following requirements:

- **At least 16 characters**: Length is the primary factor in increasing the complexity and entropy of the password

- A password **will not** be part of a blacklist of commonly used passwords.

- A user may **not** reuse the same old password.

Based on the [NIST SP 800-63B 2024](https://pages.nist.gov/800-63-4/sp800-63b.html) standard, we **do not require** the following:

- Use of special characters is **not required** but is still permitted.

- Use of uppercase characters is **not required** but is still permitted.

- Use of digits is **not required** but is still permitted.

We suggest users choose passwords that are *passphrases*, which consist of two or more words connected together. This can be something like “baby\_elephants\_are\_cool” or “theSchoolIsSchool”. This is only a suggestion, and as our only requirement is the length of a password, the user is free to construct them however best fits their use case.

Assets Affected

| Hostname | IP Address | Additional Notes |
| --- | --- | --- |
|  |  | **REMOVE IF NONE** |

Fulfilled Action Items

1. Our team analyzed the current password requirements for local accounts on Linux systems. We found that they **used the default requirements, as shown below, we can see they offer no additional configurations.** <Screenshots of defaults>

2. Our team analyzed the current password requirements for local accounts on Windows systems. We found that they **used the default requirements, as a result, we utilized Group Policy Objects to set preferences on Computers when creating a password as seen below.** <Screenshots of defaults>

3. Our team analyzed the current password requirements for domain-joined accounts on Windows systems. We found that they **used the default requirements, as shown below, we can see they offer no additional configurations.** <Screenshots of defaults>

4. Our team researched current industry and government standards and utilized the [NIST SP 800-63B 2024](https://pages.nist.gov/800-63-4/sp800-63b.html) which describes the current industry standards to implement the new password policies. <Screenshots of Linux and Windows system configurations>

5. Our team configured system policies to require password resets on the next successful login. <Screenshots of changes>

6. Our team tested the new password policies ensuring that complexity requirements were met, and that dictionary, weak or reused passwords were disallowed. <Screenshots of failures to set passwords>

\*Delete below before turning in

If inject also requires implementation, look towards windows AD and Identiy Management Services, such as KeyCloak. Don’t forget about supporting artifacts