|  |
| --- |
| Password Policy Report |

|  |  |  |
| --- | --- | --- |
| Sam Bailey |  |  |
| 19/11/2025 |  | logo-placeholder |

## detail of persons hands with scissors, markers, working

## Introduction

This report looks at the updated CITEMS Password Policy and compares it to the NIST SP 800-63B guidelines, focusing on the rules for memorized passwords. The goal is to see which parts of the current policy follow NIST’s recommendations, which parts don’t, and what changes should be made to bring the policy up to modern security standards.

## Recent Changes to Policy

Recent updates to the CITEMS Password Policy include increasing the recommended password length to around 14–16 characters, adding multi-factor authentication (MFA) as a requirement, and changing the rule around password expiry so that passwords only need to be updated if they’ve been compromised. These changes help strengthen overall security and bring the policy more in line with modern authentication practices.

## Summary of NIST Requirements

NIST SP 800-63B recommends that user-created passwords should be at least 8 characters long, while system-generated passwords can be at least 6 characters and may be numeric. It also states that complexity rules, like forcing symbols or uppercase letters, shouldn’t be required.

Passwords should be checked against lists of weak or previously compromised passwords. The guidelines also say that all characters, including spaces, should be allowed so users can create longer passphrases. Passwords also shouldn’t expire regularly unless there is evidence that the password has been compromised.

## Alignment With Current Policy

**In line with NIST:**

* The policy encourages longer passwords and passphrases.
* It avoids strict complexity rules.
* It discourages weak, common, or predictable passwords.
* It includes proper handling of passwords (not storing or sending them in plain text).
* The use of multi-factor authentication also lines up with NIST’s overall approach.

**Not in line or missing:**

* The recommended minimum of 14–16 characters is stricter than NIST’s 8-character minimum.
* It doesn’t clearly state that mandatory regular password changes are avoided, which NIST states explicitly.

## Conclusion

The CITEMS Password Policy generally follows the main ideas in the NIST Digital Identity Guidelines. It supports longer passwords, removes strict complexity rules, and includes MFA, which are all in line with NIST. However, there are still a few areas that are missing or not fully explained, such as what characters are allowed, how minimum length is handled, and how passwords should be managed over time.

## Recommendations

To improve compliance and modernize the policy, the following changes are recommended:

* Clearly state that all characters, symbols, and even spaces are allowed in passwords.
* Adjust the recommended length to around 12–14 characters, with 8 being the minimum to stay in line with NIST’s requirements.
* Add a clear statement saying CITEMS does not require regular password changes unless there’s evidence the password has been compromised.
* Officially include a password blacklist to block common weak passwords and any known leaked passwords.

## Email

