Password Policy Audit Report

# 1. Introduction

This report documents the findings of a password policy audit conducted on a test login page of a sample application. The audit compares the current password practices of the system against the NIST SP 800-63B Digital Identity Guidelines to identify gaps and provide recommendations for improvement.

# 2. Methodology

The audit was performed by creating a test user account and attempting different password scenarios. Each scenario was compared against the NIST SP 800-63B guidelines for password length, complexity, expiration, dictionary checks, copy-paste restrictions, and support for multi-factor authentication (MFA).

# 3. Findings

|  |  |  |  |
| --- | --- | --- | --- |
| Test | Expected (NIST SP 800-63B) | Actual (System) | Pass/Fail |
| Minimum length | ≥ 8 characters | 6 characters allowed | Fail |
| Maximum length | ≥ 64 characters allowed | 16 characters max | Fail |
| Complexity rules | Not enforced (user choice) | Requires uppercase + special character | Fail |
| Common/compromised password check | Blocked (must check against breached/common lists) | Allowed 'password123' | Fail |
| Password expiration | Not required unless breach suspected | Forced every 30 days | Fail |
| Copy-Paste allowed | Allowed (should not block password managers) | Blocked | Fail |
| Multi-Factor Authentication (MFA) | Available & strongly recommended | Supported (SMS OTP available) | Pass |

# 4. Recommendations

Based on the findings of the audit, the following recommendations are made to align the system’s password policy with NIST SP 800-63B Digital Identity Guidelines:

1. 1. Increase minimum password length to at least 8 characters.
2. 2. Allow users to set longer passwords, up to 64 characters.
3. 3. Remove forced complexity rules and instead encourage longer passphrases.
4. 4. Implement a check against commonly used and breached passwords.
5. 5. Remove forced periodic password expiration; only require reset in case of compromise.
6. 6. Allow copy-paste functionality to support password managers.
7. 7. Continue supporting Multi-Factor Authentication (MFA) and consider adding more secure options like authenticator apps or hardware tokens.

# 5. Conclusion

The audit revealed significant gaps between the application’s current password policy and NIST SP 800-63B recommendations. By addressing these issues, the system can greatly enhance security while also improving usability for end-users.