INTERNAL PCI DSS PASSWORD POLICY AUDIT REPORT

Confidential – For Internal Use Only

Organization: [Your Company Name]

System Owner: [Name of System Owner or IT Lead]

Audit Performed By: [Your Name – Internal PCI Auditor]

Audit Date: June 2025

Target System: Windows 10 Standalone VM

# Executive Summary

This audit report presents the results of an internal assessment of the password authentication policies configured on a Windows 10 virtual machine used for PCI-related administrative functions.  
  
The goal was to validate compliance with PCI DSS v4.0.1 Requirement 8. The assessment revealed multiple deficiencies in system configuration — most notably in password length, complexity, expiration, lockout thresholds, and temporary password handling.  
  
This report outlines each finding, its associated risk, the relevant PCI DSS requirement, and a recommended remediation path. All issues must be addressed before the system can be considered compliant.

# System Design Description

The target system is a Windows 10 standalone VM simulating access to cardholder data. It is configured using local security policy (secpol.msc) and does not rely on domain-joined group policies. Local user accounts are used to validate enforcement of password and account lockout policies.  
  
System changes are applied manually and validated using PowerShell and command-line tools.

# Observations

During the audit, it was noted that several password-related controls were misconfigured. Key observations include:  
- Password length set below PCI minimum  
- Complexity settings disabled  
- Expiration and reuse policies misaligned with standards  
- Lockout thresholds too lenient  
- No enforcement for temp password reset  
  
No documented configuration standard or user password guidance was provided.

# Audit Findings

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Finding # | Finding Description | PCI DSS Requirement | Risk | Recommendation | Due Date |
| 8.01 | Password minimum length is set to 8 characters. | 8.3.6 | Susceptible to brute-force attacks. | Set password length to 12 characters. | 2025-06-20 |
| 8.02 | Password complexity is disabled. | 8.3.7 | Allows weak passwords with low entropy. | Enable complexity: uppercase, lowercase, number, special character. | 2025-06-20 |
| 8.03 | Password expiration set to 180 days. | 8.3.8 | Extended expiration increases exposure time of stolen credentials. | Reduce to 90-day expiration per PCI DSS. | 2025-06-20 |
| 8.04 | Only 1 password remembered. | 8.3.9 | Allows users to cycle recent passwords repeatedly. | Increase password history to remember last 4. | 2025-06-20 |
| 8.05 | Lockout threshold is set to 20 failed attempts. | 8.3.11 | Greater risk of successful brute-force attacks. | Lower threshold to 10 or fewer failed attempts. | 2025-06-20 |
| 8.06 | Lockout duration is only 5 minutes. | 8.3.12 | Lockout resets too quickly, enabling continued attack attempts. | Set lockout duration to 30 minutes or until manual reset. | 2025-06-20 |
| 8.07 | Temporary passwords don’t expire and don’t require change at next login. | 8.3.13 | Long-lived temp accounts increase risk of misuse. | Enforce 24-hour expiry and force reset on next login for temp passwords. | 2025-06-20 |

# Remediation Plan

The System Owner is responsible for applying the above recommendations by June 20, 2025. Changes can be made via secpol.msc or GPO.  
  
A follow-up validation audit will be performed after the deadline. All remediated controls must be evidenced with screenshots and timestamped confirmation.

# Conclusion

This internal audit has identified multiple deviations from PCI DSS Requirement 8. A formal remediation effort is required to address the gaps before the system can be marked compliant.  
  
Once changes are implemented, a compliance verification walkthrough will confirm closure of each finding.