Type of Policy: Administrative

Effective Date: July 2016

Last Revised: July 2016

Review Date: April 2025

Next Review Date: April 2027

Policy Owner: ACME Corporation Cybersecurity

Contact Name: John Kaset

Contact Title: Governance Risk & Compliance Manager - Cyber Security

Contact Email: johnkaset@acmecorp.com

Reason for Policy

This policy establishes the minimum requirements for generating and managing ACME Corporation user passwords, or other authentication factors, used by operating systems, applications, databases, and network devices owned by or managed by ACME Corporation. The intent of this policy is to protect access to Sensitive Data and ACME Corporation systems and networks.

Policy Statement

Single factor authentication (i.e. password authentication) or multifactor authentication (i.e. password and token) must be used to authenticate to any system or application which requires unique logon as defined by the Data Access Policy and Data Protection Safeguards Standard. The standards for single factor password authentication and multifactor authentication are defined in the standards section below.

ACME Corporation account users must take all reasonable measures to protect their passwords and accounts. ACME Corporation users must never share their account passwords with anyone, including third-party service providers (e.g. Google). Each user is accountable and responsible for any action taken with that user's account and password. If there is a business that needs to share access to an account, such sharing should be accomplished through system permission delegation.

Exceptions to the requirements of this policy may be requested per the Policy Exceptions policy.

Standards: General Standards

- ACME Corporation user account passwords must never be transmitted over the network in a clear text format.
- Passwords must be protected at all times, and measures must be taken to prevent disclosure to any unauthorized person or entity.
- Passwords must be protected during distribution to the end user.
- Temporary passwords must be changed within 24 hours of creation.
- Default passwords for new servers, endpoints, and applications must be changed.
- Password must be securely stored using a strong hashing algorithm.
- After five failed login attempts, the account must be locked, and IT must be contacted to resolve the issue.
- Password reset requests require all employees to use multifactor authentication.

Single Factor Password Configuration Standards

Single-factor passwords must meet the following:

Password Length:

- Contain at least 14 characters

Password Complexity:

- Contain characters from the following four-character classes:
- Upper case alphabetic (e.g. A-Z)
- Lowercase alphabetic (e.g. a-z)
- Numeric (e.g. 0-9)
- Special characters (e.g. .,!@#$%~)
- Expire every 365 days
- Password selection must be different from the last five passwords used
- All passwords must be stored in an approved password manager

Multifactor Password Configuration Standards

When logging into systems or applications that require multifactor authentication, the associated password must:

Password Length:

- Contain at least 12 characters

Password Complexity:

- Contain characters from the following four-character classes:
- Upper case alphabetic (e.g. A-Z)
- Lowercase alphabetic (e.g. a-z)
- Numeric (e.g. 0-9)
- Special characters (e.g. .,!@#$%~)
- Passwords expire every 730 days
- Password selection must be different from the last five passwords used
- All passwords must be stored in an approved password manager

System and Administrator Password Standards

Password Length:

- Contain at least 16 characters

Password Complexity:

- Contain characters from the following four-character classes:
- Upper case alphabetic (e.g. A-Z)
- Lowercase alphabetic (e.g. a-z)
- Numeric (e.g. 0-9)
- Special characters (e.g. .,!@#$%~)
- Passwords expire every 6 months
- Password selection must be different from the last ten passwords used
- All passwords must be stored in an approved password manager

Mobile Device Pin/Password Configuration Standards

When using a mobile device, such as a smartphone or tablet, that requires authentication, the associated password/pin must:

Numeric Pin Password:

- Contain at least eight digits

Alphanumeric Password:

- Contain at least 14 characters
- Contain characters from the following four-character classes:
- Upper case alphabetic (e.g. A-Z)
- Lowercase alphabetic (e.g. a-z)
- Numeric (e.g. 0-9)
- Special characters (e.g. .,!@#$%~)

Biometrics Password:

- Must be used with a PIN or alphanumeric password

Password Manager Configuration Standards

To create strong credentials management and requires company approval for a password manager to meet the following standards:

Approve Processes

- IT-approved password managers only and personal versions are not allowed for keeping corporate credentials

Master Password Requirements

- Contain characters from the following four-character classes:
- Upper case alphabetic (e.g. A-Z)
- Lowercase alphabetic (e.g. a-z)
- Numeric (e.g. 0-9)
- Special characters (e.g. .,!@#$%~)
- No reused password from any system
- Change at least once every 6 months
- Must have multifactor authentication enabled for all password manager accounts; not doing so is prohibited
- If it is suspected that a password is compromised, it must be changed immediately

Credential Sharing:

- Credential sharing is strictly prohibited
- Each employee is responsible for making sure only they have access to their authorized system

Audits & Monitoring

- IT team is to conduct audits regularly to ensure the following:

- Password manager is following policy requirements
- Access permission is accurate, and no unapproved credential access has happened

Scope

- This Corporation-wide policy applies to any endpoint, mobile device, or application that requires a unique logon as defined by the Data Access Policy and Data Protection Safeguards Standard and all users of those systems.

Policy Terms

- *Endpoint* – Desktop computers, laptop computers, workstations, group access workstations, USB drives, small servers, cloud-hosted virtual machines, and personal Network Attached Storage (NAS)
- *Mobile Device* – Mobile devices at ACME Corporation include, but are not limited to:
- Cellular telephones
- Smartphones (e.g. iPhones, Android Phones, BlackBerrys)
- Tablet computers (e.g. iPad, Kindle, Kindle Fire, Android Tablets)
- Wearable Devices (e.g. Google Glass, watch devices)
- Personal Digital Assistants
- Any other mobile device containing ACME Corporation data (e.g, handheld scanning devices)
- *Multifactor Authentication* – A process for securing access to a given system, such as a network or website, that identifies the party requesting access through several categories of credentials (e.g. password and soft token or password and thumbprint).
- *Server* – Any computer system that hosts a campus unit or Corporation-wide service or acts as an authoritative data source for the Corporation or campus unit.

- *Single Factor Authentication* – A process for securing access to a given system, such as a network or website that identifies the party requesting access through only one category of credentials (e.g. password).
- *Password Manager* – A software approved by ACME corporation that allows users to store and manage their password through encryption securely

Enforcement

- Violations of this policy may result in loss of ACME Corporation system and network usage privileges, disciplinary action, up to and including termination or expulsion as outlined in applicable ACME Corporation Employment policies and the ACME Corporation Student Code of Conduct, as well as personal civil and/or criminal liability.

Justification

General Standards Update

"Password must be securely stored using a strong hashing algorithm."

- Since storing passwords in plaintext is a massive vulnerability, they would be secure if an event happened due to their strong hash. Also, it aligns with US standards. (NIST SP 800-63B)

Added "Account must be locked after 5 failed login attempts, and IT must be contacted to resolve the issue.

- Locking accounts after multiple attempts prevents any brute-force attacks that can comprise a password. Therefore, reducing risk is a recommended corporate system. (NIST SP 800-53 Rev.5)

Added "Password reset requests require all employees to use multifactor authentication

- Adding multifactor authentication creates a second layer of protection: identity verification. It is a recommended system for corporations, and it reduces risk. (CIS Control v8 – Control 5)

Single Factor Password Configuration Standards Update

Increasing the character length from 6 characters to 14 characters

- Increasing the password length decreases the chances of any brute-force attacks from getting access (NIST SP 800-63B).

Complexity of character from 2 of 4 to using all four characters

- Requiring all four characters increases the password entropy, meaning that it protects against dictionary or hybrid attacks (ISO/IEC 27002).

The reuse of passwords was changed from the last one to the previous five passwords.

- This limits the chances of someone's password being compromised or guessed correctly, reducing exposure to password replay attacks (NIST SP 800-53 Rev.5).

Added, "Stored in an approved password manager."

- Encrypting credential storage reduces the chances of any password being leaked compared to a sticky note or spreadsheet (CIS Control v8 – Control 5)

Multifactor Password Configuration Standards

Increasing the character length from 8 characters to 12 characters

- MFA still requires strong credentials, meaning increasing the password length only strengthens it against attacks (NIST SP 800-63B).

Complexity of character from 2 of 4 to using all four characters

- Password complexity is essential even in MFA environments as it prevents brute force attacks and ensures a layered defense (ISO/IEC 27002).

Expiration from 365 to 730 days

- Frequent changes in passwords can lead to users being fatigued and password predictability. Therefore, since it's a second layer, it aligns with the guidelines (NIST SP 800-63B).

Reuse in passwords change from 2 to 5 passwords.

- Increasing the reuse of passwords aligns more with the standard as it offers identity protection, especially in places where it's an authentication environment (NIST SP 800-53 Rev.5).

System and Administrator Password Standards (New Section)

Password length to be 16 characters

- System/Administrator accounts tend to pose a higher threat when compromised, so they must have a longer password length (CIS Control v8 – Control 5).

Complexity must have all four types of characters

- Ensure password entropy since it's a higher privilege account, which is a top target (ISO/IEC 27002).

The password must be changed every 6 months.

- They have a faster rotation cycle as it ensures any compromised access is less effective due to a password change (NIST SP 800-53 Rev.5).

The last 10 passwords can't be repeated and must be stored in a password manager.

- It prevents any password that might have been compromised from being reused for an extended period (ISO/IEC 27002) and prevents insecure storage of high-risk credentials (NIST SP 800-53 Rev.5).

Mobile Device Pin/Password Configuration Standards

Pin length changed to 6 to 8 numbers/ characters

- Longer PINs provide resistance against surfing and brute force attacks and, as known 6, digits PINs then be insufficient against automated unlock tools (NIST SP 800- 124 Rev. 2)

Pattern/Swipe

- They have been completely removed as they are vulnerable against smudge attacks and observational compromises, which taking them out creates better security (ISO/IEC 30107).

Biometrics

- Biometrics cannot be used alone and requires a PIN or password in case of failure. It needs to fall back to something that works (ISO/IEC 30107).

Password Manager Policy (New Section)

Requires the approval of IT password managers

- Ensure that good software is used to manage sensitive credentials, which prevents any data leakage (ISO/ IEC 27001).

Master Password that must have complexity, MFA, and rotation

- Since the master password acts as a key that stores all the credentials, it must have the best security, which is why it has a good complexity, MFA, and rotation (NIST SP 800-63B).

No Credential Sharing

- Preventing password sharing offers a system in place for anything to be compromised and makes it more secure (ISO/IEC 20002).

Audit and Monitoring

- Having audit and monitoring allows to see misuse and policy violations. Also, it helps with incident investigation and regular compliance (NIST SP 800-92).

Minor Update

Added a password definition and a review date to be every two years

- It ensures we are up to date with the correct policies and provides clarity when reading documents (ISO/IEC 27001).

Reference

National Institute of Standards and Technology. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). 67 pages. https://pages.nist.gov/800-63-3/sp800-63b.html

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Rev. 5). 492 pages. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

National Institute of Standards and Technology. (2020). *Guidelines for managing the security of mobile devices in the enterprise* (NIST Special Publication 800-124 Rev. 2). 60 pages. https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/final

National Institute of Standards and Technology. (2006). *Guide to computer security log management* (NIST Special Publication 800-92). 53 pages. https://csrc.nist.gov/publications/detail/sp/800-92/final

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization. (2022). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Code of practice for information security controls*. https://www.iso.org/standard/75652.html

International Organization for Standardization. (2019). *ISO/IEC 27018:2019 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. https://www.iso.org/standard/76559.html

International Organization for Standardization. (2016). *ISO/IEC 30107:2016 – Information technology – Biometric presentation attack detection – Part 1: Framework.* https://www.iso.org/standard/67381.html

Center for Internet Security. (2021). *CIS controls version 8: Critical security controls for effective cyber defense*. https://www.cisecurity.org/controls