Policy Administration

Toan Tran

CPSC 253

Prof. Franklin

December 13, 2024

**Password Policy**

Effective Date December 2, 2024

Review Date December 2, 2024

Policy Owner ACME Corporation CyberSecurity

Contact name: John Kaset

Contact Title: Governance Risk & Compliance Manager

Reason for Policy

* This policy is essential to protect employees, end-users, accounts, and passwords with safe network services, software applications, and other sensitive information and assets.

Policy General Standard

* Users must not share their work account and password with others or third-party providers. They must use their business accounts carefully and be responsible for their actions.
* The IT department, managers, or the boss must maintain communication and account sharing across computers and cooperation networks.
* User account passwords should be transmitted over the network with a strong encrypted format and secure distribution, such as password manager generators and second-layer MFA
* Passwords must be monitored and protected to prevent breaches and unauthorized access by personnel.
* New employees must change the organization's initial password on the new servers, endpoints, and applications.

Multifactor Password Configuration Standards (MFA)

According to Robyn Ferreira, Compliance Success Manager, “2024 NIST Password Guidelines: Enhancing Security Practices:”

* Contain at least 16+ characters (length over complexity)
  + Must include all characteristics from the following categories below:
  + Uppercase alphabetic (A- Z), recommend starting with.
  + Lowercase alphabetic (a-z)
  + Numeric (0 - 9)
  + Special characters (e.g. .,!@#$%~)
  + Each category must go beyond 1
  + Randomize combinations, paraphrase
* I recommend implementing emojis (strengthen passwords but limit them).
* Only cycle passwords once something goes wrong (no expiration date).
* Restriction:
  + Don’t reuse passwords.
  + There are no hints, no dictionary words.
  + No duplicate repeated words.
* The verification screen expires within 3 minutes and is locked after 3rd trial.

(Ferreira, 2024)

SSO (Single Sign-on)

According to Joanna Yip, “Best practices for creating a corporate password policy,”

* Applied to across accounts through SSO to access the electronic devices and their application
* It must be set up with MFA; refer to the password length and complexity requirement above.
* SSO will expire within a month.
* The SSO account must be locked after 3rd trial; contact IT for back-up.

(Yip, 2024)

Password Manager

Inspired by Robyn Ferreira, Compliance Success Manager, “2024 NIST Password Guidelines: Enhancing Security Practices:”

* Recommend this approach if fitting the budget
* Must pick the one with strong encryption and build-in MFA
* All Cooperation users should use a password manager to create, store, and retrieve passwords.

(Ferreira, 2024)

Mobile Device Pin / Password Configuration Standards

* Authentication forms contain:
  + Biometrics (recommend FaceID, TouchID).

Back-up plan

* If we fail to verify after three trials, accounts will lock, and we report to the IT department to regain access; we must change the password afterward and further info (both SSO and MFA)

Scope

* This policy applies to all endpoints, mobile devices, and applications that require verified and management processes for all users' systems.

Enforcement

* Any employees who violate the above policies may face consequences from pay cuts to job termination, depending on the severity of the information infringement. The contractors' contracts shall terminate with the following consequences. A lawsuit may apply if the loss exceeds the Cooperation acceptance limit

**Data Privacy Policy**

Effective Date December 2, 2024

Review Date December 2, 2024

Policy Owner: ACME Corporation CyberSecurity

Contact Name: John Kaset

Contact Title: Governance Risk & Compliance Manager

Reason for Policy

* The Data Privacy Policy provides a standard that restricts communication and information collection and limits access to personal files. More information should be needed to enhance services and achieve goals to follow the company's legacy.
* The Corporation promises a private space for customers, employees, and contractors and shall not violate nor touch upon their physical and virtual confidential information and data.

Policy Statement

According to the insights “Data Privacy Best Practices: Ensure Compliance & Security” and “The Evolving World of Data Privacy: Trends and Strategies” from Gagan Koneru, CISA:

* Securely dispose of all electronic devices and related documentation on research private data when employees leave the company. Adjustments depend on status changes (sick, deceased, etc.
* Regularly monitor and maintain network and application and update regulations if needed.
* Provide mandatory awareness and training every 6 months
* IT department assists and handles emergencies and provides safety practices
* Transparent data collection plans for contractors and end-users
* Implement incident response plans to data breaches and unauthorized access to private assets.
* Provide encryption privacy data protection
* Constant monitoring and record audits, AI helps, involves also recommend
* Restriction on access control level to all employees who can only access necessary data and information for work.

(Data Privacy Best Practices: Ensure Compliance & Security, 2024; Koneru, 2024)

Scope

* All data files and communications shall regulate received and transmitted services and stored resource maintenance.

Enforcement

* Investigate any violations of sensitive info during customers' and employees' contracts period, according to US cyber law and ACME Corporation data policy.
* Employees who violate the above policies face consequences ranging from pay cuts to job termination; depending on the severe data breaches, lawsuits may apply when damage goes beyond the Cooperation acceptance boundaries.

**Cyber Security Policy**

Effective Date December 2, 2024

Review Date December 2, 2024

Policy Owner ACME Corporation CyberSecurity

Contact Name John Kaset

Contact Title Governance Risk & Compliance Manager

Reason for Policy

* This Cyber Security Policy delivers guidance and regulations on IT management, security endpoints, and personal belongings control.
* This policy provides some techniques and rules to change while maintaining a balanced user experience.

Policy Statement

According to the article inspired by Cynet, “Creating Your Cyber Security Policy: Ultimate 2024 Guide:”

1. IT Security management

* Implement firewalls on all electronic devices to monitor and block unwanted incoming and outgoing traffic and unauthorized access to protect the network and the system.
* Set up an intrusion detection and prevention system on the central server to track unusual activities.
* Specify detailed guidance and requirements on which software can be used in the organization and procedures to install, update, and patch management.
* Set up and link encrypted VPNs to sensitive resources and secure IP address connections between personal devices and virtual servers.

(Creating Your Cyber Security Policy: Ultimate 2024 Guide, 2024)

1. Endpoint security management

* Apply the role-based control restriction to all employees.
* Set up MFA on all computers, mobile phones, and other electronic devices to retain sensitive environment of data and info from unauthorized access.
* All employees must upgrade their business electronic devices when the server or software releases update patches to protect against vulnerabilities.

(Creating Your Cyber Security Policy: Ultimate 2024 Guide, 2024)

1. Bring your own device management.

* Ensure secure measurement of all personal devices by embedding strong encryption techniques, MFA, antivirus, and modernized lengthy passwords so as not to cause corruption in the organization.
* All employees must practice and be responsible for staying alert to security and report to IT immediately when corruption or violation cases happen to mitigate risks. In addition, AI automatically goes unnoticed by manual checks.
* Follow the incident response procedures: preparation, detection, analysis, containment and recovery, and log incidents.
* Provide audits and inform all employees to prevent and prepare for future compromised situations (virus, malware infection, unauthorized access, etc.)

(Creating Your Cyber Security Policy: Ultimate 2024 Guide, 2024)

Scope

* All authorized users authorized third parties, and IT resources usage shall stay under and follow this policy.

Enforcement

* Any violations will be finalized with consequences and enforced rigorously to ensure fairness in the working environment. Terminate, and lawsuits may be applied if severe.

**References**

*Creating your cyber security policy: Ultimate 2024 guide - all-in-one cybersecurity platform*. Cynet. (2024, November 27).

https://www.cynet.com/cybersecurity/creating-your-cyber-security-policy-ultimate-2024-guide/

Data Privacy Best Practices: Ensure Compliance & Security. (2024, July 30). *Digitalguardian*.

https://www.digitalguardian.com/blog/data-privacy-best-practices-ensure-compliance-security

Ferreira, R. (2024, September 23). 2024 NIST Password Guidelines: Enhancing Security Practices. *scytale.ai*.

https://scytale.ai/resources/2024-nist-password-guidelines-enhancing-security-practices

Hewitt, N. (2024, April 23). *How to implement a robust password policy • truefort*. TrueFort.

https://truefort.com/password-policy/

Koneru, G. (2024, October 14). *The Evolving World of Data Privacy: Trends and Strategies*. ISACA.

https://www.isaca.org/resources/news-and-trends/industry-news/2024/the-evolving-world-of-data-privacy-trends-and-strategies

Yip, J. (2024, August 1). Best practices for creating a corporate password policy. *Smartdeploy*.

https://www.smartdeploy.com/blog/best-practices-for-creating-corporate-password-policy