Policy Memo

Toan Tran

CPSC 253

Prof. Franklin

December 13, 2024

To: Governance Risk & Compliance Manager, John Kasket

From: A Security Analyst

Date: December 13, 2024

Subject: Urgent Update and Remeasurements Policy

This memo will modify and clear unnecessary policies to follow modernized security trends and resolve existing organizational system issues. This memo delivers a better way to detect and prevent threats and develop methods to deal with or mitigate threats and risks.

The first change we should consider enhancing our organization's security system is the password policy. We should eliminate a single-factor password because this configuration setup is unsuitable and easily compromised via pattern recognition. Within this situation, encryption and MFA are recommended. Here, we should make a few adjustments so that passwords prioritize length over complexity. With randomized combinations, paraphrasing, and lengthy password techniques, it will take forever to guess all combinations with brute force, like John the Ripper. Also, modifying passwords should be limited and only occur when corrupt or in emergencies. The password manager tool is a reasonable option for saving time and securing sensitive passwords by matching combinations with unused ones. We do not have to stress about losing track of passwords and reusing mistakes ever again. (How to Implement a Robust Password Policy, 2024; Ferreira, 2024).  SSO should be executed in our system and set to expire every 2 months, so sign-on with a password manager or backup access is essential; accomplishing that can prevent unauthorized personnel from accessing documents to on-vacation or sick employees on business computers (Yip, 2024). For instance, new employees should change the organization's default password on the new endpoints and applications due to likely exposure to insider threats. Adding three trials of unsuccessful attempt lock mechanisms on the

backup prevents break-ins and signal alerts for IT to investigate. We should stop password distribution and never share them, as they have a high potential for leaks in the transmitted process and increase attack surfaces that damage our reputation and end-users.

Not only does the password policy need to change, but the private data policy must also be updated due to a lack of protection and privacy management. For instance, the old policy must provide a specific way to deal with vulnerabilities and risks. So, employees may need help with the next steps. With the new policy, we can give mandatory awareness training every 6 months about modern threats and ongoing risks with detailed procedures and techniques to respond quickly, like turning off the internet network if it is a network unauthorized access. With this training, our employees can first-aid the network and application before IT can mitigate damage. Also, our IT department should improve our outdated incident response plan with detailed steps to provide a secure place to transmit data and prevent unauthenticated access to data and breaches (Data Privacy Best Practices: Ensure Compliance & Security, 2024). For instance, to mitigate data in the cloud, we must have safe and backup response plans for internet vulnerability. That is why we need to train our IT team with new tools and use them in our work, like constant monitoring AI algorithms, which can analyze and detect data corruption where personnel oversee. Also, AI might audit and suggest some old data we have not used within 5 years, which is not mentioned in the old policy; we should delete them to prevent that old piece from becoming a weak spot in our storage resources. We should apply role-based access control and least privilege to prevent unrelated and unauthorized employees from accidentally misusing critical data and software that can lead to vulnerability, application corruption, and adverse effects on time and organization data, strengthening the overall reputation and protection system (Koneru, 2024)

The Cyber Security Policy should also include access control and the least privilege, which must be updated in our outdated policy. Regarding cyber policy, access control is essential because it limits threats to unrestricted user access and helps us prevent unnecessary malicious attacks on network systems. We should add a bring your device policy so that personal devices can be a reason for breaches and vulnerabilities. Our employees may lack knowledge of performing security and may be unaware of those risks, opening the door to attackers. As a second barrier, MFA, antivirus, should be set on all business devices and servers to ensure data and sensitive data are in secure containers. This is important because it can exclude unintentional incidents against malware and provide secure transmission with AI monitoring and encryption. Also, we should add patching management to our new policy because this ensures that no authorized access or integrity attacks happen due to outdated applications and software. For instance, Windows releases major updates on significant issues, and our organization does not mention anything on policy; our employees are more likely to ignore Windows updates, and attackers can dive in and exploit our assets and resources (Creating Your Cyber Security Policy: Ultimate 2024 Guide, 2024).

To ensure employees can enforce and notice this policy, we should set precise expectations for all employees and managers to monitor and check for violations, discipline, and consequences, which will be implemented based on severity while ensuring fairness in the working environment. The transparent policy communicates all employees via group meetings, and the remainder messages, work emails and other platforms. For instance, our IT department needs to notify our employees about all changes to policies whether minor or critical. We should repeat that during every 6 months of training to ensure we know the essential and critical purposes behind each new upgrade policy. We should provide policy updates at least once yearly

to follow modern security trends, annual reports from all employees and customers, and CVE vulnerability reports. Those security threats explain why passwords, data privacy, and cyber security changes are urgently needed with defense mechanisms and audit details.

**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