30 January 2024

CYBER ASSURANCE

PASSWORD POLICY

LADI RACHAEL MABELA

TABLE OF CONTENTS

CYBER ASSURANCE

REVISION HISTORY

Version	Date	Comment	Updated by
0.1	30/02/2024	Document created.	Rachael Mabela

EXECUTIVE SUMMARY

This Password Policy is designed to establish comprehensive guidelines for creating, managing, and securing passwords within our organization. Our goal is to strengthen our digital defenses against potential security threats and illegal access by instituting strong and unique password policies.

GUIDELINES

1. Strong Passwords:

Create robust passwords by incorporating a combination of uppercase and lowercase letters, digits, and special characters.

2. Minimum Password Length:

Passwords must consist of a minimum of 14 characters. Longer passwords provide enhanced security against unauthorized access.

3. Avoid Dictionary Terms:

Refrain from using easily guessable terms such as "password," "qwerty," "abc123," etc., as these can be swiftly compromised with the right tools.

4. Minimum Password Age:

Users are required to update their passwords every 90 days. Regular password updates reduce the likelihood of successful password cracking.

5. Stronger Authentication Technique:

For logging in on new devices, employ a stronger authentication technique, such as enabling the one-time password option provided by services like Gmail.

6. Distinct Passwords:

Use unique passwords for different websites or devices to mitigate the impact of potential security breaches.

7. Password Sharing:

If a password is shared, change it immediately. Avoid sharing passwords under normal circumstances and disclose them only when absolutely necessary.

8. Password Storage:

Avoid storing passwords on desktop computers or mobile devices, as unauthorized access to these devices may compromise sensitive credentials. Utilize a secure password manager as a safer alternative.

9. Personal Information:

Refrain from using personal details, such as birthdates, car numbers, or information about pets, in passwords. Social engineering attacks can exploit such information, making it easier for attackers to guess passwords.

PENALTIES

Adhering to our password policy is essential to preserving the security and integrity of our company's digital assets. Discipline may follow non-compliance with these principles; the type and frequency of violations will determine the severity of consequences. Penalties for disregarding the rules could be:

1. Warning:

A formal written warning may be issued for the first instance of non-compliance, providing an opportunity for individuals to rectify their behavior.

2. Account Lockout:

Persistent violations may lead to temporary account lockout, restricting access to organizational resources until the issue is addressed.

3. Training Requirements:

Individuals found in violation may be required to undergo additional cybersecurity training to reinforce awareness and understanding of the Password Policy.

4. Loss of Privileges:

Continued non-compliance may result in the loss of certain privileges, limiting access to specific systems or sensitive information.

5. Account Suspension:

In cases of serious or repeated violations, temporary suspension of account privileges may be implemented, preventing access to all organizational systems.

6. Termination of Employment or Contract:

Failure to adhere to the Password Policy, particularly in instances of intentional or gross negligence, may lead to the termination of employment or contractual agreements.

CONCLUSION

In conclusion, the implementation of this Password Policy reflects our unwavering commitment to fostering a robust cybersecurity posture within our organization. By prioritizing user education on secure password practices, advocating for the adoption of multi-factor authentication, and conducting regular security awareness training, we empower our workforce to be vigilant guardians of our digital assets.

Our approach recognizes the evolving landscape of cyber threats and the necessity for proactive measures against social engineering attacks. Through continuous education and reinforcement of security best practices, we not only fortify our password infrastructure but also cultivate a culture of heightened awareness and responsibility among our personnel.

The emphasis on prompt reporting of suspicious activities or security concerns to the IT department serves as a crucial component of our defense strategy. This collaborative approach ensures that potential threats are identified and addressed expediently, contributing to the overall resilience of our digital ecosystem.

By adhering to these guidelines, every member of our organization becomes an active participant in the ongoing effort to safeguard sensitive information and maintain the integrity of our digital operations. Together, we reinforce a collective commitment to security excellence, demonstrating our dedication to protecting our valuable assets from potential threats now and in the future.