Chameleon Account Security and Awareness Policy

Chameleon Security Team

CHAMELEON

FOR OUR SMARTER WORLD

Author(s):

Name:	Student ID:	Team:
Rewniz Patell	221267802	Chameleon Security

Table of Contents

Introduction

The account security and awareness policy highlights the importance of account security, and provides procedures that all Chameleon members must follow. This ensures that the accounts of employees are adequately protected, and that measures are in place to avoid security breaches, account compromise, or loss of data. It is required that all members of Chameleon are adequately trained to be aware of potential cyber security threats, and aware of how to mitigate these threats through employing preventive measures.

Purpose

The purpose of this policy is to ensure that members of Chameleon take adequate measures to ensure third-party application accounts are secure, and employees within Chameleon are aware of security threats. Ensuring account security standards are maintained, mitigates the chance of potential cyber-attacks, enhances security awareness throughout the organization, and ensures that confidential company information is secure.

Scope

The scope of this policy is all members within the Chameleon team, regardless of role or project. All members within Chameleon should be adequately trained to understand cyber security threats, the importance of taking preventative measures to mitigate threats, and understanding how to keep Chameleon accounts and infrastructure secure from potential threats. The applications for this policy include (but are not limited to), Microsoft Teams, Outlook, Github and Git.

Importance

With the Chameleon projects using multiple different third-party applications for communication, developing, and conducting projects, and collaborating with each other, the importance of account security is paramount. Employees should take adequate measures to ensure that all accounts are secure and monitored, and the Chameleon leadership should ensure that individuals are assisted with account security.

Chameleon Account Security Policies

During the onboarding process of new employees, Chameleon administrators and senior leaders should ensure that new employees follow these policies, to enhance the security of accounts for third-party applications.

Password Creation Policy

Password strength and complexity is extremely important to ensure account security. Passwords should meet the following criteria when created,

- Use unique passwords, that are not shared with any other company or personal accounts.
- Use complex and long passwords of at least 12 characters long, includes numbers, special characters, and a mix of lowercase and uppercase letters.
- Avoid personal information such as birthdate, names, common words.
- Should not contain a pattern or repetition.

Additionally, to ensure long-term password protection,

- Passwords should only be known by the relevant employee and not shared.
- Passwords should not be stored on any device, written down, or kept in a list.
- Passwords must be changed if there is unauthorized access, a potential breach of the account, and should be changed at regular set intervals of 1-3 months.

Password Manager Policy

To ensure that there is a good balance between accessibility of accounts and password security, a companywide password manager should be utilized. This ensures that there is one standard for password managers across all employees, administrators have access to all password manager accounts, and only safe and authorized password managers are used by employees. Password manager accounts should be set up by administrators, so that new employees have access to configured and set up password manager accounts.

Employees should

- Use the password manager to store, add and delete passwords.
- Use only the authorized password manager.
- Follow the password creation policy when creating a new password.
- Store passwords only related to work accounts, and not store any passwords related to private accounts.
- Not share their password manager account with anyone.
- Ensure only authorized devices (such as work on computers/mobiles) are logged in to the password manager.
- Ensure that no personal devices are used to log into the password manager account.

Two Factor Authentication (2FA) Policy

Chameleon should also ensure that a dedicated two-factor authentication (2FA) application is utilized as a standard within the company. This should be a single service, to avoid administrators having to monitor accounts across multiple different 2FA services. Mandatory 2FA should be enacted across all employees, and across all accounts. Additionally,

- All employees within Chameleon must enable 2FA for all accounts across all applications.
- 2FA must have biometric authentication enabled.
- Hardware tokens should be offered as an alternative if the 2FA service cannot be enacted by a certain employee. Reasons for this could include but are not limited to,
    - Incompatible mobile device
    - Unable to use 2FA application/service due to accessibility issues.
    - Required to use hardware tokens due to the employee not being able to have a reliable internet connection for online 2FA services.
    - Any other reason deemed satisfactory by the Chameleon Administrator(s). These exemptions must be approved by the Administrators.
- Employees should report if 2FA is logging unauthorized login attempts, or if there is a suspected breach or unauthorized access.

Work Devices Policy

This policy applies to all Chameleon employees within the organization. This policy ensures that,

- Employees should be provided with a work device if necessary for work-related tasks.
- The assigned device should only be used for work-related tasks.
- Work devices must be up-to-date and maintained through the employee or administrative team.
- Employees can request approval to use a personal device for work purposes.
    - These devices must comply with all Chameleon security policies and approved at the discretion of the administrator(s).
- Employees must not disable, circumvent, or attempt to remove security software, modify privileges, or protocols installed or set by the Chameleon administrative team.

Responsibility of policy standard and enforcement

Senior Leadership and Administrators

Security leadership and administrators are responsible for

- Ensuring that new employees are trained to understand the account security policy, and all policies and procedures included within this policy.
- Decide on what services to use and implement the standards for password managers and 2FA applications.
- All passwords, password managers, and work devices, 2FA application accounts are monitored to ensure that all policies are met by employees.
- Ensuring that all employees engage with the account security policy and have completed the training to understand the account security policy.
- Ensure that avenues are in place for reporting if any of these policies are not being met by employees.
- Ensure that employees can report if there are potential security breaches or unauthorized access of accounts/passwords to administrators.
- Maintaining and monitoring all company accounts for third party applications.
- Ensure that training is updated based on changes to procedure, policies or services being used.
- Monitor for suspicious or unauthorized login in attempts of employee accounts.

Employees

Employees are required to,

- Take training to ensure that they meet all account security policies including, but not limited to password creation policy, password manager policy, 2FA policy, and work devices policy.
- Employees are required to report any potential security breaches or unauthorized access to third party application accounts.
- Employees are required to adhere to the account security policy to maintain a security standard within Chameleon and mitigate any potential cyber-attacks.