Chameleon
Security

Password Management Policy

Purpose

The purpose of this Password Management Policy is to establish guidelines and requirements for the creation, use, and management of passwords within the Chameleon to ensure the security of information systems and data. This policy aims to protect sensitive information from unauthorised access by enforcing robust password practices, in alignment with industry standards and regulatory requirements. By implementing this policy, Chameleon seeks to mitigate the risks associated with weak or compromised passwords and enhance overall information security.

Scope

This policy applies to all employees, contractors, vendors, and any other individuals who have access to Chameleon's systems, networks, and data. It encompasses all systems and applications, including but not limited to internal and external systems, on-premises and cloud-based services, and remote access environments. The scope of this policy covers the entire lifecycle of password management, from creation and storage to usage and change requirements, and applies to all types of user and administrative accounts.

Policy Statement

Chameleon is committed to maintaining the highest standards of information security by implementing stringent password management practices. All users are required to create and maintain strong, unique passwords in accordance with the guidelines outlined in this policy. Passwords must be managed securely to prevent unauthorised access to company resources. The company will provide the necessary tools and training to support users in adhering to these practices. Compliance with this policy is mandatory, and violations may result in disciplinary actions. This policy is designed to align with relevant ISO, NIST, and IEEE standards and to comply with Australian laws and regulations.

Definitions

Password: A string of characters used to verify the identity of a user during the authentication process.

Passphrase: A longer sequence of words or text used to enhance security, typically easier to remember than a complex password.

Multi-Factor Authentication (MFA): An authentication method that requires two or more verification factors to gain access to a resource.

Authentication: The process of verifying the identity of a user, device, or other entity in a computer system.

Password Creation Requirements

- Passwords must be at least 12 characters long and include a mix of upper and lower case letters, numbers, and special characters.
- Passphrases must be at least 16 characters long and can include spaces for ease of use.
- Passwords must not contain easily guessable information such as user names, birthdates, or common words.
- Users must not reuse passwords across different systems and applications.
- Passwords must not be identical to previously used passwords.
- Passwords must be significantly different from previous passwords, altering at least four characters.
- Users must follow additional complexity requirements, such as avoiding consecutive identical characters.
- Passwords should avoid common patterns like "1234" or "abcd".
- Temporary passwords issued for account creation or recovery must be unique and comply with the above requirements.

Password Change Requirements

- Passwords must be changed every 90 days.
- Users must not reuse any of their last 5 passwords.
- Passwords must be changed immediately if there is any suspicion that they have been compromised.
- Password change prompts must be configured to remind users ahead of the expiration date.
- Systems should force password changes at the next login if the password has expired.
- Users should be guided through a secure password change process, avoiding exposure to shoulder surfing.
- Password change requests must be authenticated by verifying the user's identity.
- Temporary passwords must be changed upon first use.
- Password change processes should be tested regularly for security vulnerabilities.

Password Storage and Transmission

- Passwords must be stored using secure, salted hashing algorithms (e.g., SHA-256 with salt).
- Passwords must never be transmitted in plain text; encrypted channels (e.g., TLS/SSL) must be used for all password transmission.
- Passwords must not be written down or stored in easily accessible locations.
- Passwords must not be stored in scripts or macros.
- Stored passwords must be protected by access controls to prevent unauthorised access.
- Password recovery mechanisms must not reveal passwords; they should reset them.
- Passwords in backups must be encrypted and protected.
- Password storage systems must be regularly audited for compliance.

- Password management systems must log and alert on any suspicious activities related to password access.

Multi-Factor Authentication

- MFA must be enabled for all access to sensitive systems and data.
- Acceptable methods for MFA include hardware tokens, mobile app-based authentication, and biometric verification.
- MFA must be required for remote access to the company's network.
- MFA should be implemented for administrative access to critical systems.
- Users must be educated on the importance and use of MFA.
- MFA tokens and devices must be securely managed and regularly reviewed.
- Lost or compromised MFA devices must be reported and deactivated immediately.
- MFA policies should be reviewed and updated regularly to adapt to new threats.
- The company must support a variety of MFA methods to accommodate different user needs.
- MFA systems must be resilient and provide fallback mechanisms for legitimate users without compromising security.

Administrative Passwords

- Administrative accounts must use unique, strong passwords that are different from user account passwords.
- Access to administrative accounts must be restricted to authorised personnel only.
- Administrative passwords must be changed more frequently (e.g., every 60 days) and immediately after any staff turnover.
- Shared administrative accounts must be avoided; each administrator should have a unique account.
- Administrative accounts must be monitored for unusual activity.

- Passwords for administrative accounts must follow all creation and storage guidelines outlined in this policy.
- Administrative accounts must use MFA wherever possible.
- Administrative account credentials must be reviewed regularly to ensure they comply with current policies.
- Emergency access procedures for administrative accounts must be documented and securely stored.
- Administrative passwords must not be used for any non-administrative purposes.

Password Management Tools

- The use of password management tools (e.g., password managers) is encouraged to help users generate, store, and manage complex passwords.
- Approved password management tools must be vetted and endorsed by the company's IT security team.
- Password managers must be configured to automatically generate strong, unique passwords for each service.
- Users must be trained on the proper use of password management tools.
- Password managers must use strong encryption to protect stored passwords.
- Access to password managers must be protected with strong authentication, preferably MFA.
- Password managers should provide secure sharing options for credentials when necessary.
- The company must regularly review and update the list of approved password management tools.
- Password management tools must be tested for vulnerabilities before approval.
- The use of password management tools must comply with all other password policies outlined in this document.

User Training and Awareness

- Regular training sessions on password security best practices must be conducted for all employees.
- Awareness programs must highlight the importance of strong password management and the risks associated with weak passwords.
- Users must be informed about the latest threats and how to protect against them.
- Training must cover the use of password management tools and MFA.
- Employees must acknowledge their understanding and adherence to the password policy.
- Training materials must be updated regularly to reflect current security trends and practices.
- Simulated phishing attacks may be used to test and reinforce password security awareness.
- Feedback from training sessions should be used to improve future training.
- Password security tips and reminders should be regularly communicated.
- Employees must be encouraged to report any password-related security concerns immediately.

Monitoring and Auditing

- Regular audits must be conducted to ensure compliance with this policy.
- Automated tools should be used to monitor for potential password breaches and policy violations.
- Audit logs must be maintained and reviewed for any unusual activities.
- Password policies and practices must be reviewed and updated based on audit findings.
- Unauthorised attempts to access accounts must be investigated promptly.
- Auditing procedures must comply with relevant legal and regulatory requirements.

- Reports on password security status must be provided to senior management regularly.
- Audit tools and processes must be tested and validated regularly.
- Audit logs must be protected from unauthorised access and tampering.
- Audit findings must be documented, and remediation actions tracked until completion.

Incident Response

- Any suspected or confirmed password compromise must be reported immediately to the IT security team.
- Affected passwords must be changed, and appropriate incident response measures must be initiated.
- Incident response plans must include specific steps for addressing password-related breaches.
- Users must be informed about the steps they need to take in case of a password compromise.
- Incident response activities must be documented and reviewed to identify lessons learned.
- Passwords involved in security incidents must not be reused.
- Incident response teams must have access to tools and resources for rapid password reset and account recovery.
- Communication plans must be in place to inform affected parties and stakeholders.
- The effectiveness of incident response measures must be regularly evaluated and improved.
- Coordination with legal and compliance teams must ensure that all actions align with regulatory requirements.

Compliance and Legal Considerations

- his policy is aligned with relevant Australian laws and regulations, including the Privacy Act 1988 and the Australian Signals Directorate's Information Security Manual (ISM).
- Compliance with ISO 27001, ISO 27002, NIST SP 800-63B, and IEEE 802 standards must be maintained.
- Regular reviews must ensure that the policy continues to meet legal and regulatory requirements.
- Legal and compliance teams must be involved in the development and review of password policies.
- Non-compliance must be addressed with appropriate disciplinary actions.
- Records of compliance reviews and audits must be maintained.
- Compliance training must include password management as a key component.
- Updates to laws and regulations must trigger a review of the password policy.
- Legal advice must be sought when implementing significant changes to the policy.
- The policy must be available to all stakeholders to ensure transparency and accountability.

Policy Review and Maintenance

- This policy must be reviewed annually or whenever significant changes occur in applicable laws, regulations, or best practices.
- The IT security team is responsible for maintaining and updating this policy.
- Feedback from users must be considered in policy updates.
- Changes to the policy must be communicated to all employees and stakeholders.
- Historical versions of the policy must be archived for reference.
- The effectiveness of the policy must be regularly assessed.
- Reviews must include input from legal, compliance, and operational teams.
- Policy updates must include implementation plans and timelines.

- The review process must be documented and transparent.
- Continuous improvement principles must guide the policy maintenance process.

Enforcement

- Violations of this policy may result in disciplinary action, up to and including termination of employment.
- Consistent enforcement is critical to the success of this policy; all violations must be documented and addressed promptly.
- Enforcement measures must be clearly communicated to all employees.
- Managers and supervisors must ensure compliance within their teams.
- Incident reports must include details of enforcement actions taken.
- Repeated violations must lead to escalating disciplinary measures.
- Enforcement actions must comply with legal and regulatory requirements.
- Support mechanisms must be in place to help users comply with the policy.
- Enforcement must be fair, impartial, and consistent across the company.
- Records of enforcement actions must be maintained and reviewed to ensure policy effectiveness.