Chameleon
Security

Access Control Policy

Purpose:

The purpose of this Access Control Policy is to establish comprehensive measures for managing access to Chameleon's information systems and resources. This policy aligns with Annex A.9 of the ISO/IEC 27001:2022 standard and aims to ensure the confidentiality, integrity, and availability of data while mitigating the risks associated with unauthorised access.

Scope:

This Access Control Policy applies to all employees, contractors, third-party users, and systems within the Chameleon company's domain. It encompasses user access control, network access control, administrative access control, and application access control across all devices, networks, and information systems owned or operated by the organisation.

Access Control Principles:

- **Least Privilege:** Users shall be granted the minimum level of access necessary to perform their assigned tasks effectively.
- **Need-to-Know:** Access to sensitive information shall be restricted to individuals who require it to fulfill their duties.
- **Segregation of Duties:** Responsibilities shall be divided among multiple individuals to prevent conflicts of interest and reduce the risk of fraud or errors.
- **Defense-in-Depth:** Multiple layers of security controls shall be implemented to protect against unauthorised access, including physical, technical, and administrative measures.

User Access Control:

- **User Authentication:** Users shall authenticate their identities using strong authentication mechanisms such as passwords, tokens, or biometrics.
- **Password Policies:** Passwords shall adhere to complexity requirements, be regularly changed, and not shared among users.

- **Account Provisioning and Deprovisioning:** User accounts shall be provisioned based on job roles and responsibilities and promptly deprovisioned upon termination or change in employment status.

A.9.2.1 User Registration and Deregistration:

Procedures shall be established for registering new users and deregistering users who are no longer authorised to access the organisation's systems and resources.

A.9.2.2 User Access Provisioning:

User access rights shall be provisioned based on job roles and responsibilities, following the principle of least privilege.

A.9.2.3 Management of Privileged Access Rights:

Procedures shall be implemented for managing and controlling privileged access rights to critical systems and data.

A.9.2.4 Management of Secret Authentication Information of Users:

Secret authentication information, such as passwords and cryptographic keys, shall be securely managed and protected from unauthorised disclosure or access.

A.9.2.5 Review of User Access Rights:

User access rights shall be reviewed periodically to ensure compliance with policies and business requirements.

A.9.2.6 Removal or Adjustment of Access Rights:

Procedures shall be established for removing or adjusting user access rights promptly upon termination, change in employment status, or change in business requirements.

Administrative Access Control:

- **Privileged Account Management:** Administrative accounts shall be designated and managed separately from standard user accounts, with additional security measures implemented.
- **Access Controls for Privileged Accounts:** Access to administrative functions and sensitive systems shall be restricted and monitored to prevent unauthorised changes.
- **Audit Logging:** All administrative actions shall be logged and regularly reviewed to detect unauthorised activities.

Network Access Control:

- **Network Segmentation:** The network shall be segmented to control traffic flow and limit access to sensitive resources.
- **Access Control Lists (ACLs):** ACLs shall be configured on network devices to restrict access based on predefined rules and policies.
- **Virtual Private Networks (VPNs):** Secure VPN connections shall be used to provide remote access to the organisation's network resources.

Application Access Control:

- **Role-Based Access Control (RBAC):** Access to applications and data shall be based on users' roles and responsibilities within the organisation.
- **Access Control Lists (ACLs):** ACLs shall be implemented within applications to regulate user access to specific functions or data.
- **Application Whitelisting:** Only authorised applications shall be permitted to execute on organisation-owned devices, reducing the risk of malware infections.

User Responsibilities:

Users shall be responsible for safeguarding their authentication credentials and complying with access control policies and procedures. This includes:

- **Password Security:** Users shall create strong, unique passwords and safeguard them from unauthorised disclosure. Passwords shall not be shared with others and shall be changed periodically according to policy requirements.
- **Multi-Factor Authentication (MFA):** Users shall utilise multi-factor authentication where available to enhance the security of their accounts and prevent unauthorised access.
- **Access Control Awareness:** Users shall familiarise themselves with access control policies and procedures and understand their role in maintaining the security of the organisation's information systems. They shall promptly report any suspected security incidents or violations of access control policies to the appropriate authorities.

Secure Log-On Procedures:

Secure log-on procedures shall be implemented to authenticate users and prevent unauthorised access to information systems. This includes:

- **Strong Authentication Mechanisms:** Information systems shall employ strong authentication mechanisms such as passwords, tokens, biometrics, or a combination of these methods to verify the identity of users during the log-on process.
- **Session Management:** User sessions shall be managed securely to prevent unauthorised access, including mechanisms for session timeout, session locking, and automatic log-off after periods of inactivity.
- **Logging and Monitoring:** Log-on events shall be logged and monitored to detect and respond to unauthorised access attempts. Logs shall include details such as user identities, timestamps, and IP addresses for auditing and forensic purposes.

Access Control to Program Source Code:

Access to program source code shall be restricted to authorised personnel and protected against unauthorised modification or disclosure. This includes:

- **Access Controls:** Access to program source code repositories shall be restricted to authorised individuals based on the principle of least privilege. Access permissions shall be granted only to those individuals who require access to perform their job duties.
- **Version Control:** Program source code shall be managed using version control systems to track changes and revisions. Access controls shall be enforced within the version control system to ensure that only authorised changes are made to the codebase.
- **Code Review Processes:** Code changes shall undergo review by authorised personnel to ensure compliance with coding standards, security best practices, and regulatory requirements before being merged into the production environment. Code reviews shall be documented, and any identified vulnerabilities or issues shall be addressed promptly.

Password Management System:

A password management system shall be implemented to enforce password policies, such as complexity requirements, expiration, and history, and to securely store and manage passwords. This includes:

- **Password Complexity Requirements:** Passwords shall adhere to complexity requirements, including minimum length, character diversity, and inclusion of both alphanumeric and special characters.
- **Password Expiration and History:** Passwords shall be set to expire periodically, and users shall be prohibited from reusing previous passwords to prevent password recycling and enhance security.
- **Secure Storage:** Passwords shall be stored securely using encryption and hashing techniques to protect against unauthorised access in the event of a data breach. Access to password databases shall be restricted to authorised personnel only, and mechanisms shall be in place to monitor and audit access to sensitive password information.

Access Review and Monitoring:

- **Regular Access Reviews**: User access rights and permissions shall be reviewed periodically, at least annually, to ensure compliance with policies and detect unauthorised access. Reviews shall include verification of user roles and permissions against documented requirements and business needs.
- **Access Logs and Audit Trails:** Access activities shall be logged and retained for audit and forensic purposes. Logs shall include details such as user authentication, access attempts, changes to access permissions, and administrative actions. Audit trails shall be regularly monitored and analysed to detect and respond to unauthorised access attempts or suspicious activities.
- **Incident Response Procedures:** Security incidents involving unauthorised access shall be promptly investigated, contained, and remediated following established incident response procedures. Incident response team members shall be trained and equipped to respond to access-related incidents, including identifying the root cause, restoring affected systems and data, and implementing preventive measures to mitigate future risks.

Training and Awareness:

- **Employee Training:** All employees shall receive training on access control policies, procedures, and best practices as part of their onboarding process and regularly thereafter. Training shall cover topics such as password security, data classification, user responsibilities, and incident reporting.

- **Security Awareness Programs:** Ongoing awareness campaigns shall be conducted to educate employees about the importance of access control and their roles in maintaining security. Awareness programs may include newsletters, posters, emails, and interactive training sessions to reinforce key messages and promote a security-conscious culture.
- **Incident Reporting:** Employees shall be informed of reporting procedures for suspicious access attempts or potential security breaches. Reporting channels shall be clearly defined and accessible, and employees shall be encouraged to report any observed or suspected security incidents promptly.

Compliance and Legal Considerations:

- **Legal Compliance:** The Access Control Policy shall adhere to relevant Australian laws, regulations, and industry standards, including but not limited to the Privacy Act and ISO/IEC 27001. This includes ensuring that access control measures are implemented in accordance with legal requirements regarding data protection, privacy, and information security.
- **Data Protection Requirements:** Access control mechanisms shall be designed and implemented to protect sensitive data from unauthorised access, disclosure, alteration, or destruction, in compliance with data protection laws and regulations such as the Australian Privacy Principles (APPs).
- **Industry Standards Adherence:** The Access Control Policy shall align with industry-recognised standards and best practices for information security, including ISO/IEC 27002, NIST Cybersecurity Framework, and relevant sector-specific standards.

Policy Review and Maintenance:

- **Annual Review:** The Access Control Policy shall be reviewed at least annually or more frequently as needed to ensure its effectiveness, relevance, and alignment with changing business requirements and regulatory standards. The review process shall include an assessment of policy objectives, controls, and procedures, as well as feedback from stakeholders and lessons learned from security incidents or audits.
- **Change Management:** Procedures shall be established for implementing changes to the Access Control Policy, including approval, testing, and

communication to affected parties. Changes may include updates to access control mechanisms, policy revisions based on regulatory changes, or enhancements to address emerging security threats.

- **Documentation Updates:** Any changes or updates to the Access Control Policy shall be documented and communicated to relevant stakeholders, including employees, contractors, and third-party service providers. Updated policy documents shall be maintained in a centralised repository and made accessible to authorised personnel for reference and compliance purposes.

Enforcement and Compliance:

- **Enforcement Mechanisms:** Compliance with the Access Control Policy shall be enforced through monitoring, audits, and disciplinary actions for non-compliance. These enforcement measures will be conducted in accordance with relevant Australian laws and regulations, including but not limited to the Privacy Act 1988 (Cth) and the Australian Cyber Security Centre (ACSC) guidelines.
- **Consequences of Non-Compliance:** Violations of access control policies shall result in appropriate consequences, as outlined in organisational policies and procedures and in accordance with Australian laws. Depending on the severity and frequency of the violation, consequences may include verbal warnings, written warnings, suspension, termination of employment, or legal action.
- **Reporting Procedures:** Mechanisms shall be in place for users to report suspected violations of access control policies, ensuring timely investigation and resolution. Reports of non-compliance shall be handled confidentially and in accordance with established incident response procedures and reporting requirements under Australian laws and regulations.