Chameleon
Security

Network Security Policy

Purpose:

The purpose of this Network Security Policy is to establish guidelines, procedures, and responsibilities to ensure the confidentiality, integrity, and availability of Chameleon Company's network infrastructure and information assets. This policy aims to align with ISO/IEC 27001:2022 standards, specifically focusing on A.13.1 - Network Security Management.

Scope:

This Network Security Policy applies to all employees, contractors, and third-party users who have access to Chameleon's network resources and information systems. It encompasses all network devices, including but not limited to routers, switches, firewalls, servers, endpoints, wireless access points, and associated software and services.

Roles and Responsibilities:

1. **Network Security Administrator:**
    - Responsible for the implementation and enforcement of network security policies, procedures, and controls.
    - Conduct regular security assessments and audits of the network infrastructure to identify vulnerabilities and compliance gaps.
    - Coordinate with IT teams to deploy and configure security tools and technologies such as firewalls, IDS/IPS, and encryption protocols.
    - Monitor security alerts and incidents, respond promptly to mitigate security threats and breaches.
2. **System Administrators:**
    - Responsible for configuring and maintaining network devices and systems in accordance with security best practices and standards.
    - Ensure that software patches and updates are applied promptly to address known vulnerabilities and mitigate security risks.
    - Collaborate with the Network Security Administrator to implement access controls, encryption mechanisms, and network segmentation.
3. **Security Awareness Trainer:**
    - Develop and deliver security awareness training programs and materials to educate employees on network security risks and best practices.

- Promote a culture of security awareness within the organisation through interactive workshops, newsletters, and online resources.
- Monitor and assess the effectiveness of security awareness initiatives and adjust training content as needed based on feedback and evaluation.

4. **Incident Response Team:**
    - Formulate and maintain incident response plans and procedures to address network security incidents effectively.
    - Coordinate with relevant stakeholders to contain and mitigate security breaches, minimise impact, and restore normal operations.
    - Conduct post-incident analysis and document lessons learned to improve incident response processes and enhance overall network security posture.

Network Access Control:

- **Access Control Policy:** Implement measures to control and manage access to the network infrastructure based on the principle of least privilege. Access to network resources should be granted based on job roles and responsibilities.
- **Authentication Mechanisms:** Enforce strong authentication mechanisms such as passwords, multi-factor authentication (MFA), and biometrics to verify the identity of users accessing the network.
- **Access Review:** Regularly review and update access control lists (ACLs) and user permissions to reflect changes in roles or responsibilities. Access privileges should be revoked promptly upon termination of employment or contract.

Network Monitoring and Logging:

- **Continuous Monitoring:** Deploy monitoring tools to continuously monitor network traffic, activities, and anomalies. Network monitoring should encompass both inbound and outbound traffic.
- **Log Management:** Maintain comprehensive logs of network events, including access attempts, security incidents, and configuration changes. Logs should be stored securely and retained according to legal and regulatory requirements.
- **Log Analysis:** Periodically review and analyse network logs to identify potential security threats and vulnerabilities. Suspicious activities should be investigated promptly, and appropriate action taken to mitigate risks.

Encryption and Data Protection:

- **Data Encryption:** Utilise encryption protocols (e.g., SSL/TLS) to secure data transmission over the network, especially for sensitive information such as customer data, financial records, and intellectual property.
- **Data-at-Rest Encryption:** Implement encryption mechanisms for sensitive data stored on network devices and systems. Encryption keys should be managed securely to prevent unauthorised access.
- **Data Classification:** Enforce data classification policies to ensure appropriate encryption levels based on data sensitivity. Classify data into categories such as public, internal, confidential, and restricted, and apply encryption accordingly.

Firewall and Intrusion Detection Systems (IDS):

- **Firewall Deployment:** Deploy firewalls at network entry and exit points to monitor and filter incoming and outgoing traffic. Configure firewall rules to allow only authorised traffic and block known malicious activities.
- **Intrusion Detection Systems (IDS):** Implement IDS/IPS systems to detect and prevent unauthorised access and malicious activities. Configure intrusion detection signatures to identify and respond to known attack patterns.
- **Regular Updates:** Regularly update firewall and IDS/IPS configurations to address emerging threats and vulnerabilities. Patch management should be conducted promptly to ensure the security of network devices and systems.

Network Segmentation:

- **Segmentation Policy:** Implement network segmentation to isolate sensitive systems and data from less secure areas of the network. Define and enforce access controls between network segments to prevent unauthorised lateral movement and data breaches.
- **Access Controls:** Configure network segmentation policies to restrict access between network segments based on business requirements and risk assessments. Only authorised users should be granted access to specific network segments.
- **Review and Update:** Regularly review and update network segmentation policies based on changes in business requirements, security threats, and risk assessments. Ensure that network segmentation remains effective in mitigating potential risks.

Incident Response and Contingency Planning:

- **Incident Response Procedures:** Establish incident response procedures to promptly detect, respond to, and mitigate network security incidents. Designate incident response teams and define their roles and responsibilities in handling security breaches.
- **Response Coordination:** Coordinate with relevant stakeholders, including IT personnel, legal counsel, and law enforcement agencies, to manage and contain security incidents effectively. Communication channels and escalation procedures should be clearly defined.
- **Post-Incident Analysis:** Conduct post-incident analysis and lessons learned sessions to identify weaknesses in network security controls and procedures. Implement corrective actions and preventive measures to enhance the organisation's resilience to future incidents.

Employee Awareness and Training:

- **Training Programs:** Provide regular training and awareness programs to educate employees on network security best practices, policies, and procedures. Training topics should include password hygiene, phishing awareness, and incident reporting.
- **Security Awareness Campaigns:** Conduct security awareness campaigns to reinforce key security messages and promote a culture of security awareness within the organisation. Utilise various communication channels such as emails, posters, and workshops.
- **Assessment and Feedback:** Conduct periodic security awareness assessments to evaluate the effectiveness of training programs. Solicit feedback from employees to identify areas for improvement and tailor training initiatives accordingly.

Compliance and Legal Requirements Section:

Chameleon is committed to adhering to all relevant Australian laws, regulations, and industry standards concerning network security and data protection. In addition to Australian laws and regulations, we will also align our practices with international standards,

including ISO/IEC 27001:2022, to ensure a robust and comprehensive approach to network security management.

Specific areas of compliance include, but are not limited to:

1. **Privacy Act 1988 (Cth):** Compliance with the Privacy Act, including the Australian Privacy Principles (APPs), to safeguard the privacy and security of personal information collected, used, and stored by the organisation. This includes implementing appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, and misuse.
2. **Australian Cyber Security Centre (ACSC) Guidelines:** Adherence to the guidance provided by the ACSC, including the Essential Eight strategies for mitigating cyber security incidents. This includes measures such as application whitelisting, patching applications, and restricting administrative privileges to enhance network security posture.
3. **Data Breach Notification Laws:** Compliance with the Notifiable Data Breaches (NDB) scheme, which mandates the notification of individuals and the Office of the Australian Information Commissioner (OAIC) in the event of eligible data breaches. Our organisation will have procedures in place to detect, assess, and respond to data breaches promptly, in accordance with NDB requirements.
4. **Australian Signals Directorate (ASD) Strategies:** Alignment with the ASD's cybersecurity strategies, including the Information Security Manual (ISM) and the Strategies to Mitigate Cyber Security Incidents. This includes implementing controls and measures outlined in the ISM to protect sensitive information and critical assets from cyber threats.
5. **ISO/IEC 27001:2022 Standards:** Integration of ISO/IEC 27001:2022 standards into our network security practices to establish a systematic approach to managing information security risks. This includes implementing controls and procedures outlined in ISO 27001, such as risk assessment and treatment, security awareness training, and incident response planning.

Our organisation will regularly review and update our network security policies, procedures, and controls to ensure ongoing compliance with Australian laws and regulations, as well as international standards such as ISO/IEC 27001:2022. Compliance assessments, internal audits, and external reviews will be conducted periodically to verify adherence to legal requirements and industry standards.

Policy Enforcement and Review Section:

Chameleon is committed to ensuring the effective enforcement and regular review of our Network Security Policy to uphold compliance with Australian laws, regulations, and

international standards, including ISO/IEC 27001:2022. This section outlines the enforcement mechanisms and review processes that will be implemented:

1. **Policy Enforcement:**
    - **Monitoring and Auditing:** Regular monitoring and auditing of network security controls will be conducted to assess compliance with the Network Security Policy, Australian laws, and ISO standards. This includes periodic assessments of access controls, encryption mechanisms, firewall configurations, and incident response procedures.
    - **Incident Response:** In the event of a network security incident or breach, our organisation will follow established incident response procedures outlined in the policy. A designated incident response team will be responsible for promptly detecting, assessing, and mitigating security incidents, in accordance with Australian laws and ISO/IEC 27001:2022 standards.
    - **Disciplinary Action:** Any violations of the Network Security Policy, Australian laws, or ISO standards will be subject to disciplinary action as per organisational policies and procedures. Depending on the severity of the violation, disciplinary actions may include verbal warnings, written warnings, suspension, termination of employment, or legal action.
2. **Policy Review:**
    - **Annual Review:** The Network Security Policy will be reviewed annually or more frequently as needed to ensure its continued effectiveness and alignment with Australian laws, regulations, and ISO standards. The review will be conducted by a designated review committee comprising representatives from relevant departments, including IT, legal, and compliance.
    - **Compliance Assessments:** Regular compliance assessments will be conducted to verify adherence to Australian laws, regulations, and ISO standards. These assessments may include internal audits, external audits conducted by third-party auditors, and compliance checks against established benchmarks and frameworks.
    - **Feedback Mechanisms:** Feedback from stakeholders, incident reports, and compliance assessments will be used to identify areas for improvement and update the Network Security Policy accordingly. Employees will be encouraged to report any concerns or suggestions for enhancing network security practices through designated channels, such as IT helpdesk or compliance reporting systems.
    - **Legal and Regulatory Updates:** Changes to Australian laws, regulations, and ISO standards related to network security will be monitored regularly, and the Network Security Policy will be updated accordingly to ensure ongoing

compliance. Legal counsel will be consulted to interpret and implement changes effectively within the organisation.

Our organisation is committed to fostering a culture of continuous improvement and compliance with network security requirements outlined in Australian laws, regulations, and ISO standards. By enforcing the Network Security Policy and conducting regular reviews, we aim to mitigate risks and maintain the confidentiality, integrity, and availability of our network infrastructure and information assets.