Chameleon
Security

# Monitoring and Logging Policy

# Purpose

The purpose of this policy is to define the requirements for monitoring and logging of information systems to detect and respond to potential security incidents, ensure compliance with regulatory requirements, and protect organisational assets. This policy aims to provide a structured approach to capturing, storing, and analysing log data to support security operations and incident response.

# Scope

This policy applies to all information systems, networks, applications, and data owned or managed by Chameleon. It includes all employees, contractors, vendors, and any other individuals who have access to the company's systems. The policy covers the entire lifecycle of monitoring and logging, including the generation, collection, analysis, storage, and disposal of log data.

# Policy Statement

Chameleon is committed to maintaining a robust monitoring and logging infrastructure to detect security threats and ensure compliance with industry standards and regulations. All systems must be configured to generate appropriate logs, and these logs must be monitored, analysed, and stored securely. The company will implement tools and processes to ensure the effectiveness of monitoring and logging activities. Compliance with this policy is mandatory, and violations may result in disciplinary actions.

# Definitions

**Monitoring:** The continuous process of collecting and analysing information to detect potential security incidents.

**Logging:** The act of recording events, transactions, or activities in an information system.

**Log Data:** Information recorded by systems and applications about activities and transactions.

**Security Information and Event Management (SIEM):** A system that collects, correlates, and analyses log data from multiple sources to provide real-time analysis of security alerts.

**Incident Response:** The process of identifying, managing, and mitigating security incidents.

# Logging Requirements

- **Log Generation:**
  - Systems must generate logs for all significant activities, including access attempts, administrative actions, system errors, and security events.
  - Logs should be generated for both successful and unsuccessful login attempts.
  - Applications should log critical activities, such as data access and modifications.
  - Network devices should log connection attempts and configuration changes.
  - Database systems should log queries, updates, and access control changes.
- **Log Content:**
  - Logs must include sufficient information to support forensic analysis, such as timestamps, user IDs, IP addresses, and details of the activity.
  - Ensure logs capture the who, what, when, where, and how of each logged event.
  - Include session identifiers for tracking user activities across sessions.

    - Ensure logs are time-synchronised across systems.
    - Maintain detailed logs for privileged access and administrative activities.
- **Log Retention:**
    - Logs must be retained for a minimum of 12 months or as required by regulatory requirements and company needs.
    - Implement automated log rotation and archival processes.
    - Ensure retained logs are accessible for audit and investigation purposes.
    - Comply with legal and regulatory requirements for log retention.
    - Archive old logs securely and ensure they are protected from unauthorised access.
- **Log Storage:**
    - Logs must be stored securely to prevent unauthorised access and tampering. Encryption should be used for sensitive log data.
    - Use centralised log storage to streamline access and analysis.
    - Implement redundancy and backup mechanisms for log storage.
    - Restrict access to log storage systems to authorised personnel only.
    - Ensure log storage solutions support scalability for growing log data volumes.
- **Log Integrity:**
    - Mechanisms must be in place to ensure the integrity of log data, including checksums and digital signatures.
    - Regularly verify log integrity to detect tampering or corruption.
    - Implement access controls to prevent unauthorised modifications to logs.
    - Use cryptographic methods to ensure log data authenticity.
    - Conduct periodic audits of log integrity and access controls.

# Monitoring Requirements

- **Continuous Monitoring:**
    - Systems must be monitored continuously to detect potential security incidents in real-time.
    - Implement 24/7 monitoring for critical systems and networks.
    - Utilise automated tools to streamline monitoring processes.
    - Ensure monitoring covers all network segments and devices.
    - Integrate monitoring systems with SIEM for centralised analysis.
- **Anomaly Detection:**
    - Tools must be implemented to detect anomalies and deviations from normal behaviour.
    - Use machine learning and behaviour analysis to identify unusual activities.
    - Establish baselines for normal system behaviour and track deviations.
    - Implement real-time anomaly detection for high-risk systems.
    - Continuously update and refine anomaly detection algorithms.
- **Alerting:**
    - The monitoring system must generate alerts for potential security incidents and notify the appropriate personnel.
    - Prioritise alerts based on severity and potential impact.
    - Ensure alert notifications reach relevant stakeholders promptly.
    - Implement escalation procedures for critical alerts.
    - Regularly test and validate the alerting mechanisms.
- **Correlation:**
    - Monitoring systems must correlate data from multiple sources to identify complex threats and patterns.
    - Use SIEM to aggregate and analyse log data from diverse systems.
    - Correlate network, application, and endpoint logs to detect advanced threats.

    - Implement correlation rules for known attack patterns and indicators of compromise.
    - Continuously update correlation rules based on emerging threats.
- **Performance Monitoring:**
    - The performance and availability of monitoring systems must be regularly assessed and optimised.
    - Ensure monitoring tools have minimal impact on system performance.
    - Conduct regular performance assessments and capacity planning.
    - Implement redundancy and failover mechanisms for monitoring systems.
    - Regularly review and update monitoring configurations for optimal performance.

# Incident Response and Analysis

- **Incident Detection:**
    - Logs and monitoring data must be analysed to detect security incidents promptly.
    - Implement automated incident detection mechanisms.
    - Ensure incident detection is integrated with threat intelligence feeds.
    - Conduct regular threat-hunting activities to identify undetected incidents.
    - Use advanced analytics to enhance incident detection capabilities.
- **Incident Reporting:**
    - Detected incidents must be reported to the appropriate incident response team immediately.
    - Establish clear incident reporting procedures and channels.
    - Ensure all incidents, regardless of severity, are reported.
    - Conduct regular training on incident reporting protocols.
    - Maintain an incident reporting log for accountability and review.
- **Forensic Analysis:**

    - Logs must be used to perform forensic analysis to understand the cause and impact of security incidents.
    - Ensure logs capture sufficient detail for forensic investigations.
    - Utilise forensic tools and methodologies for thorough analysis.
    - Preserve log data integrity during forensic analysis.
    - Document forensic findings and maintain a chain of custody.
- **Incident Documentation:**
    - All incidents must be documented, including the analysis, response actions, and lessons learned.
    - Maintain a detailed incident log with timestamps and actions taken.
    - Document root cause analysis and remediation steps.
    - Ensure incident documentation is accessible for audits and reviews.
    - Use incident documentation to improve future response strategies.

# Compliance and Legal Considerations

- **Regulatory Compliance:**
    - Monitoring and logging activities must comply with applicable Australian laws and regulations, including data protection and privacy laws.
    - Ensure compliance with the Australian Privacy Principles (APPs) and other relevant regulations.
    - Regularly review and update compliance practices to align with legal requirements.
    - Conduct compliance audits to verify adherence to laws and standards.
    - Implement data minimisation principles to protect privacy.
- **Audit Requirements:**
    - Logs must be available for audit purposes to demonstrate compliance with regulatory requirements and internal policies.
    - Facilitate regular internal and external audits of logging practices.
    - Ensure auditors have secure access to relevant logs and documentation.

    - Address audit findings and recommendations promptly.
    - Use audit results to enhance logging and monitoring controls.
- **Data Privacy:**
    - Monitoring and logging must respect the privacy of individuals and comply with data protection regulations.
    - Implement privacy-enhancing technologies to safeguard personal data.
    - Ensure log data is anonymised where possible to protect identities.
    - Conduct privacy impact assessments for logging activities.
    - Regularly review and update privacy policies to reflect changes in regulations.

# Policy Review and Maintenance

- **Regular Review:**
    - This policy must be reviewed at least annually or whenever significant changes occur in applicable laws, regulations, or best practices.
    - Establish a policy review committee to oversee the review process.
    - Solicit feedback from stakeholders during policy reviews.
    - Document review findings and update the policy as necessary.
    - Communicate policy changes to all relevant personnel.
- **Policy Updates:**
    - Updates to the policy must be communicated to all employees and stakeholders.
    - Use multiple communication channels to ensure broad awareness.
    - Provide training on policy updates and their implications.
    - Maintain a version history of policy changes for reference.
    - Ensure updated policies are easily accessible to all employees.
- **Continuous Improvement:**
    - Feedback from users and audit findings must be used to improve the policy and associated processes.

    - Implement a mechanism for employees to provide ongoing feedback.
    - Regularly assess the effectiveness of the policy in achieving its goals.
    - Use feedback to identify and address policy gaps and weaknesses.
    - Foster a culture of continuous improvement and compliance.

# Enforcement

- **Compliance Monitoring:**
    - Compliance with this policy must be monitored and violations must be addressed promptly.
    - Implement automated compliance monitoring tools.
    - Conduct regular compliance assessments and audits.
    - Address non-compliance through corrective actions.
    - Report compliance status to senior management regularly.
- **Disciplinary Actions:**
    - Violations of this policy may result in disciplinary actions, up to and including termination of employment.
    - Establish a clear disciplinary framework for policy violations.
    - Ensure disciplinary actions are consistent and fair.
    - Document all disciplinary actions and their outcomes.
    - Provide training to prevent future violations.
- **Responsibility:**
    - Managers and supervisors are responsible for ensuring compliance within their teams.
    - Assign clear roles and responsibilities for policy enforcement.
    - Provide resources and support for managers to enforce compliance.
    - Ensure accountability for compliance at all organisational levels.
    - Recognise and reward compliance efforts and achievements.