Logging and Monitoring Policy Template

Document Control Information

- **Document Title:** Logging and Monitoring Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Logging and Monitoring Policy establishes [ORGANIZATION NAME]'s requirements for the collection, storage, protection, and analysis of logs and the monitoring of information systems in accordance with ISO 27001:2022 requirements. It provides a framework for detecting security events, supporting investigations, and maintaining evidence of system activities.

1.2 Scope

This policy applies to: - All information systems, applications, networks, and devices owned or managed by [ORGANIZATION NAME] - All system and security logs generated by these systems - All monitoring activities performed on these systems - All employees, contractors, and third parties responsible for managing logs and monitoring systems - All environments, including production, development, test, and disaster recovery

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing comprehensive logging and monitoring of information systems - Collecting and retaining logs necessary for security, operational, and compliance purposes - Protecting logs from unauthorized access, modification, or deletion - Analyzing logs to detect security events and anomalies - Responding appropriately to identified security events - Complying with relevant legal, regulatory, and contractual requirements - Continuously improving logging and monitoring capabilities

2. Logging Requirements

2.1 Events to be Logged

The following events shall be logged:

2.1.1 System Events

- System startup and shutdown
- Service startup and shutdown
- System errors and failures
- Hardware failures
- Configuration changes
- Backup and recovery operations
- System maintenance activities

2.1.2 Security Events

- User authentication attempts (successful and failed)
- Account lockouts
- Privilege changes
- Security policy changes
- Firewall and network device events
- Intrusion detection/prevention alerts
- Anti-malware alerts
- Physical access events

2.1.3 User Activities

- Login and logout events
- Access to sensitive data
- Administrative actions
- Remote access sessions
- Data export or download
- Changes to user accounts
- Privileged operations

2.1.4 Application Events

- Application startup and shutdown
- Application errors and exceptions
- Authentication and authorization decisions
- Data modifications

- Configuration changes
- API calls and responses
- Transaction logs

2.2 Log Content

Logs shall include, where applicable: - Date and time of the event - Source of the event (system, application, device) - User or system identity - Description of the event - Success or failure indication - Origination of request (e.g., IP address) - Affected data, system components, or resources - Severity level

2.3 Log Sources

Logging shall be implemented for: - Operating systems - Applications and databases - Network devices and firewalls - Security systems (IDS/IPS, anti-malware, etc.) - Authentication systems - Cloud services - Physical access control systems - Virtualization platforms - IoT devices and operational technology

3. Log Management

3.1 Log Collection

- Logs shall be collected from all relevant sources
- Collection methods shall be reliable and secure
- Collection shall minimize impact on system performance
- Collection failures shall be detected and alerted
- Collection mechanisms shall be regularly tested
- Time synchronization shall be implemented across all systems

3.2 Log Storage

- Logs shall be stored in a secure, centralized location
- Storage capacity shall be sufficient for required retention periods
- Storage shall be protected from unauthorized access
- Storage shall be protected from modification or deletion
- Storage shall be backed up regularly
- Storage performance shall be monitored
- Storage redundancy shall be implemented for critical logs

3.3 Log Retention

- Logs shall be retained according to defined retention periods
- Retention periods shall be based on:
    - Legal and regulatory requirements

    - Contractual obligations
    - Business needs
    - Security requirements
- Minimum retention periods shall be defined for each log type
- Logs shall be securely deleted at the end of retention periods
- Retention compliance shall be regularly verified

3.4 Log Protection

- Logs shall be protected from unauthorized access
- Logs shall be protected from unauthorized modification
- Access to logs shall be restricted to authorized personnel
- Log integrity shall be maintained
- Log access shall be logged (meta-logging)
- Log transmission shall be secured
- Log backup and archiving shall be secured

3.5 Log Normalization and Indexing

- Logs shall be normalized to a common format where possible
- Logs shall be time-stamped using synchronized time sources
- Logs shall be indexed for efficient searching
- Log metadata shall be standardized
- Log categorization shall be implemented
- Log correlation capabilities shall be enabled

4. Monitoring Requirements

4.1 Monitoring Scope

Monitoring shall include: - Network traffic and behavior - System performance and availability - Security events and alerts - User activities and behavior - Application performance and errors - Database activities - Cloud service usage - Physical security systems - Environmental conditions in data centers

4.2 Monitoring Methods

Monitoring methods shall include: - Real-time monitoring - Automated alerts and notifications - Threshold-based monitoring - Anomaly detection - Behavioral analysis - Trend analysis - Compliance monitoring - Performance monitoring

4.3 Monitoring Tools

- Appropriate monitoring tools shall be implemented

- Tools shall be properly configured and maintained
- Tools shall be secured against unauthorized access
- Tool performance shall be regularly assessed
- Tool coverage shall be regularly reviewed
- Tool integration shall be implemented where appropriate
- Tool updates shall be applied promptly

5. Log Analysis and Alerting

5.1 Log Review

- Logs shall be regularly reviewed for security events
- Automated log analysis shall be implemented
- Critical logs shall be prioritized for review
- Review procedures shall be documented
- Review findings shall be documented
- Review responsibilities shall be assigned
- Review effectiveness shall be assessed

5.2 Alert Configuration

- Alerts shall be configured for significant events
- Alert thresholds shall be defined and documented
- Alert priorities shall be established
- Alert notifications shall be sent to appropriate personnel
- Alert fatigue shall be minimized through tuning
- False positives shall be identified and reduced
- Alert configurations shall be regularly reviewed

5.3 Correlation and Analysis

- Log correlation shall be implemented
- Correlation rules shall be developed and maintained
- Security information and event management (SIEM) capabilities shall be utilized
- Behavioral analysis shall be implemented where appropriate
- Threat intelligence shall be incorporated into analysis
- Analysis procedures shall be documented
- Analysis capabilities shall be regularly assessed

5.4 Incident Detection

- Logs shall be analyzed to detect security incidents
- Detection criteria shall be defined and documented

- Detection shall be timely and accurate
- Detection capabilities shall cover known attack patterns
- Detection shall include anomaly identification
- Detection procedures shall be regularly tested
- Detection effectiveness shall be measured and improved

6. Monitoring Operations

6.1 Operational Procedures

- Monitoring procedures shall be documented
- Procedures shall include:
  - Routine monitoring activities
  - Alert response procedures
  - Escalation procedures
  - Reporting requirements
  - Maintenance activities
- Procedures shall be regularly reviewed and updated
- Staff shall be trained on procedures
- Procedure effectiveness shall be assessed

6.2 Monitoring Schedule

- Continuous monitoring shall be implemented for critical systems
- Regular monitoring shall be scheduled for all systems
- Monitoring frequency shall be based on risk
- Monitoring schedules shall be documented
- Schedule compliance shall be verified
- Schedule effectiveness shall be assessed
- Schedule adjustments shall be made as needed

6.3 Performance Monitoring

- System performance shall be monitored
- Performance baselines shall be established
- Performance thresholds shall be defined
- Performance degradation shall be alerted
- Performance trends shall be analyzed
- Capacity issues shall be identified proactively
- Performance reports shall be provided to management

6.4 Availability Monitoring

- System availability shall be monitored
- Availability targets shall be defined
- Outages shall be detected and alerted
- Outage duration shall be measured
- Availability reports shall be generated
- Availability trends shall be analyzed
- Availability improvements shall be implemented

7. Security Monitoring

7.1 Threat Detection

- Security monitoring shall detect potential threats
- Threat detection shall include:
  - Malware detection
  - Intrusion attempts
  - Policy violations
  - Suspicious activities
  - Data exfiltration attempts
- Detection capabilities shall be regularly updated
- Detection effectiveness shall be tested
- Detection coverage shall be assessed

7.2 Vulnerability Monitoring

- Systems shall be monitored for vulnerabilities
- Vulnerability scanning shall be regularly performed
- Vulnerability management shall be integrated with monitoring
- Exploitation attempts shall be detected
- Vulnerability remediation shall be tracked
- Vulnerability trends shall be analyzed
- Vulnerability reports shall be provided to management

7.3 User Activity Monitoring

- User activities shall be monitored for security purposes
- Privileged user activities shall receive enhanced monitoring
- Unusual user behaviors shall be detected
- Unauthorized access attempts shall be identified
- Policy violations shall be detected
- Privacy requirements shall be respected

- User activity monitoring shall be documented and communicated

7.4 Data Loss Prevention

- Data loss prevention monitoring shall be implemented
- Sensitive data flows shall be monitored
- Data exfiltration attempts shall be detected
- Policy violations shall be alerted
- False positives shall be minimized
- DLP effectiveness shall be regularly assessed
- DLP coverage shall be regularly reviewed

8. Response and Reporting

8.1 Alert Response

- Procedures shall be established for responding to alerts
- Response shall be timely and appropriate
- Response shall be based on alert priority
- Response actions shall be documented
- Response effectiveness shall be measured
- Response procedures shall be regularly reviewed
- Response capabilities shall be regularly tested

8.2 Escalation Procedures

- Escalation procedures shall be defined
- Escalation shall be based on:
  - Severity of the event
  - Impact on business
  - Response requirements
  - Time sensitivity
- Escalation paths shall be documented
- Escalation contacts shall be maintained
- Escalation effectiveness shall be assessed

8.3 Reporting

- Regular reports shall be generated from monitoring data
- Reports shall include:
  - Security events and incidents
  - System performance and availability
  - Compliance status

    - Trend analysis
    - Recommendations for improvement
- Reports shall be provided to appropriate stakeholders
- Report formats shall be appropriate for the audience
- Reporting effectiveness shall be assessed

8.4 Forensic Support

- Logs shall support forensic investigations
- Forensic requirements shall be considered in log configuration
- Log integrity shall be maintained for evidential purposes
- Chain of custody shall be maintained for log evidence
- Log access for investigations shall be controlled and documented
- Forensic analysis capabilities shall be available
- Staff shall be trained in forensic procedures

9. Compliance and Privacy

9.1 Regulatory Compliance

- Logging and monitoring shall comply with relevant regulations
- Compliance requirements shall be documented
- Compliance shall be regularly assessed
- Non-compliance shall be addressed
- Compliance reports shall be provided to management
- Regulatory changes shall be monitored
- Logging and monitoring shall be adjusted to maintain compliance

9.2 Privacy Considerations

- Privacy requirements shall be considered in logging and monitoring
- Personal data in logs shall be identified
- Personal data collection shall be minimized
- Personal data retention shall be limited
- Access to logs containing personal data shall be restricted
- Privacy impact assessments shall be conducted
- Privacy compliance shall be regularly verified

9.3 Legal Hold

- Procedures shall be established for legal hold of logs
- Legal hold shall override normal retention periods
- Legal hold implementation shall be documented

- Legal hold shall be properly scoped
- Legal hold shall be properly terminated
- Legal hold compliance shall be verified
- Legal department shall be consulted for legal hold matters

10. Roles and Responsibilities

10.1 IT Operations Team

- Implement and maintain logging infrastructure
- Configure logging on systems and applications
- Monitor system performance and availability
- Respond to operational alerts
- Maintain log storage and backup
- Ensure log collection is functioning
- Report logging issues to management

10.2 Security Team

- Define logging and monitoring requirements
- Configure security monitoring tools
- Review security logs and alerts
- Investigate security events
- Recommend security improvements
- Report security issues to management
- Coordinate security incident response

10.3 Compliance Team

- Define compliance logging requirements
- Review logs for compliance purposes
- Prepare compliance reports
- Coordinate regulatory audits
- Advise on retention requirements
- Monitor regulatory changes
- Report compliance issues to management

10.4 System and Application Owners

- Ensure logging is enabled for their systems
- Define logging requirements for their systems
- Review logs related to their systems
- Respond to issues identified in logs

- Approve log access for their systems
- Support log analysis for their systems
- Report logging issues to IT operations

11. Training and Awareness

11.1 Staff Training

- Staff responsible for logging and monitoring shall receive training
- Training shall cover:
  - Logging and monitoring tools
  - Alert response procedures
  - Log analysis techniques
  - Security event identification
  - Incident response procedures
- Training shall be refreshed regularly
- Training effectiveness shall be assessed
- Training records shall be maintained

11.2 Awareness

- All staff shall be aware of monitoring activities
- Monitoring purposes shall be communicated
- Acceptable use policies shall reference monitoring
- Privacy notices shall include monitoring information
- Monitoring signage shall be displayed where appropriate
- Awareness materials shall be regularly updated
- Awareness effectiveness shall be assessed

12. Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

13. Related Documents

- Information Security Policy
- Incident Management Policy
- Data Protection Policy
- Acceptable Use Policy
- Retention Policy

- Forensic Readiness Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

14. Approval

This Logging and Monitoring Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____