US Solutions Pvt Ltd. - Logging and Monitoring Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-03-01
- **Author:** IT & Infosec Department - Anita Patel
- **Approved By:** Stephen Davies, Security Operations Manager
- **Effective Date:** 2024-04-01
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes that comprehensive logging and monitoring are crucial for detecting, investigating, and responding to security incidents and ensuring the integrity and availability of our systems and data. This Logging and Monitoring Policy establishes the guidelines and procedures for collecting, storing, analyzing, and retaining log data. All employees, contractors, and authorized users ("Users") are required to adhere to this policy.

2. Purpose

The purpose of this policy is to:

- Establish a standardized approach to logging and monitoring.
- Detect and respond to security incidents in a timely manner.
- Ensure the integrity and availability of Company systems and data.
- Facilitate compliance with applicable laws, regulations, and industry standards.
- Provide a foundation for forensic investigations and audits.

3. Scope

This policy applies to all systems, applications, and networks owned, managed, or accessed by US Solutions Pvt Ltd., including:

- Servers and workstations.
- Network devices (routers, firewalls, switches).
- Databases and applications.
- Cloud-based services.
- Security devices (IDS/IPS, SIEM).
- Remote access systems.
- Any system that processes, stores, or transmits company data.

4. Logging Requirements

- **Log Data:** Log data must include relevant information, such as timestamps, user IDs, IP addresses, event types, and system actions.
- **Log Sources:** Logs must be collected from all critical systems and applications.
- **Log Retention:** Log data must be retained for a minimum of [Insert Time Period, e.g., 12 months] to support investigations and audits.

- **Log Integrity:** Log data must be protected from unauthorized modification or deletion.
- **Log Storage:** Log data must be stored securely, using encryption and access controls.
- **Time Synchronization:** All systems must be synchronized with a reliable time source (e.g., NTP).

5. Monitoring Requirements

- **Real-Time Monitoring:** Critical systems and applications must be monitored in real-time for security events and performance issues.
- **Alerting:** Security alerts must be generated for suspicious or anomalous activity.
- **Thresholds:** Monitoring thresholds must be established to detect deviations from normal behavior.
- **Log Analysis:** Log data must be analyzed regularly to identify security trends and potential threats.
- **Security Information and Event Management (SIEM):** SIEM systems must be used to aggregate and analyze log data from multiple sources.
- **Network Monitoring:** Network traffic must be monitored for suspicious activity and performance issues.

6. Access Control

- Access to log data and monitoring tools must be restricted to authorized personnel.
- Access controls must be based on the principle of least privilege.
- Access logs must be maintained and audited regularly.

7. Incident Response

- Log data and monitoring tools must be used to support incident response activities.
- Security incidents identified through monitoring must be reported and investigated promptly.
- Log data must be preserved for forensic analysis.

8. Legal and Regulatory Compliance

- Logging and monitoring practices must comply with all applicable laws, regulations, and industry standards (e.g., GDPR, CCPA, PCI DSS, HIPAA).
- Log data may be used for legal or regulatory purposes.

9. User Responsibilities

- Users must not attempt to disable or circumvent logging and monitoring controls.
- Users must report any suspected security incidents or anomalies to the IT department ([email address removed]).
- Users must comply with all logging and monitoring procedures.

10. IT Department Responsibilities

- Implement and maintain logging and monitoring systems.

- Configure logging and monitoring parameters.
- Analyze log data and monitor security events.
- Investigate security incidents.
- Maintain log data integrity and availability.
- Provide training to authorized personnel on logging and monitoring tools.
- Ensure compliance with this policy.

11. Training and Awareness

- Authorized personnel will receive training on logging and monitoring tools and procedures.
- Regular security awareness training will be provided to all Users regarding logging and monitoring practices.

12. Policy Review and Updates

- This policy will be reviewed and updated annually or as needed to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

13. Monitoring and Enforcement

- The IT department will conduct regular audits to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

14. Acknowledgement

- By accessing Company systems, applications, and networks, Users acknowledge that they have read, understood, and agree to comply with this Logging and Monitoring Policy.

This Logging and Monitoring Policy is designed to ensure the security and integrity of US Solutions Pvt Ltd.'s information assets. By adhering to these guidelines, Users contribute to a secure and compliant work environment.