

Logging and Monitoring Policy

Section 1: Policy Statement, Objectives, and Scope

- **1.1 Policy Statement** World Bank is committed to maintaining a comprehensive logging and monitoring program to ensure the security, integrity, and availability of its information systems and data. This program facilitates timely detection, investigation, and response to security incidents, supports operational stability, and ensures compliance with applicable legal, statutory, and regulatory requirements. Effective logging and monitoring are fundamental to understanding system behavior, identifying anomalous activities, and providing crucial evidence for forensic analysis.
- **1.2 Objectives** The primary objectives of this Logging and Monitoring Policy are to:
 - Establish standardized and consistent procedures for the generation, secure collection, centralized aggregation, analysis, retention, and disposal of log data across all relevant World Bank assets.
 - Enable the proactive and timely detection of security incidents, unauthorized access attempts, policy violations, system malfunctions, and anomalous activities that could indicate a threat to World Bank's assets or data.
 - Provide comprehensive and reliable audit trails to support forensic investigations in the event of a security incident and to demonstrate compliance with regulatory mandates (e.g., FFIEC, SOX, PCI DSS, AML regulations).
 - Support operational troubleshooting, performance analysis, and capacity planning for IT systems and applications.
 - Ensure the confidentiality, integrity, availability, and non-repudiation of log data throughout its lifecycle.
 - Define clear roles and responsibilities for all aspects of log management and security monitoring.
- **1.3 Scope**
 - This policy applies to all World Bank information systems, network devices (e.g., firewalls, routers, switches), servers, endpoints (workstations, mobile devices), applications (including core banking, online banking, payment systems), databases, and security appliances (e.g., IDS/IPS, WAF, PAM solutions) that generate or process logs.
 - This policy encompasses logs generated from both on-premise infrastructure and cloud-based services (IaaS, PaaS, SaaS) utilized by World Bank.

- This policy is binding upon all World Bank employees, contractors, consultants, and third-party vendors who manage, operate, access, or develop systems that fall within the scope of this policy.
- The successful implementation of this policy is not merely about collecting vast quantities of data, but about transforming that data into actionable intelligence. This necessitates careful planning regarding which events to log, how to correlate disparate events into meaningful security alerts, and defining what constitutes a significant alert that warrants investigation, thereby avoiding the common pitfall of "alert fatigue". A risk-based approach to identifying log sources and fine-tuning alert parameters is crucial, focusing on logs that provide genuine security value and directly support predefined detection use cases for threats relevant to the banking sector. This inherently requires skilled security analysts and a well-configured Security Information and Event Management (SIEM) system.

Section 2: Roles and Responsibilities

- **2.1 Security Operations Center (SOC) / Security Team:**

- Primary responsibility for the continuous monitoring of security alerts, analysis of log data, and identification of potential security incidents.
- Leads the initial investigation and triage of security events and alerts.
- Develops and maintains SIEM correlation rules, dashboards, and monitoring use cases.
- Manages and administers the central log management and SIEM infrastructure.
- Escalates confirmed incidents according to the Incident Response Plan.

- **2.2 System Administrators and System Owners:**

- Ensure that logging mechanisms are enabled, properly configured, and functioning correctly on all systems under their purview, in accordance with this policy and defined logging standards.
- Assist the SOC/Security Team in interpreting system-specific logs during investigations.
- Respond to operational alerts generated from logs related to system health and performance.
- Ensure logs are securely transmitted to the central logging facility.

- **2.3 Network Administrators:**

- Ensure comprehensive logging is enabled on all network devices, including firewalls, routers, switches, VPN concentrators, wireless access points, and IDS/IPS devices.
- Monitor network traffic logs for anomalies and security events.
- **2.4 Database Administrators (DBAs):**
 - Ensure robust logging of database activities, including user access, privileged operations, data definition language (DDL) changes, data manipulation language (DML) changes on sensitive tables, and security events.
 - Regularly review database audit logs for suspicious activities.
- **2.5 Application Owners and Developers:**
 - Ensure that applications developed or managed by them generate adequate security, transaction, and error logs to meet business, security, and compliance requirements.
 - Work with the Security Team to define application-specific logging standards.
 - Ensure application logs are in a parsable format and securely transmitted to the central logging facility.
- **2.6 Compliance and Audit Teams:**
 - Periodically review log management and monitoring practices to ensure adherence to this policy and relevant regulatory requirements.
 - Utilize logs as evidence during internal and external audits and investigations.
- **2.7 Privileged Access Management (PAM) Team:**
 - Ensure comprehensive logging of all privileged account creation, modification, usage, and session activities through the PAM solution.
 - Coordinate with SOC for monitoring privileged session logs and alerts.
- A successful logging and monitoring program hinges on a shared responsibility model. While the SOC is central to analysis and detection, the generation of high-quality, relevant log data originates at the source systems. This requires proactive engagement and collaboration from system, network, database, and application teams. This policy, therefore, mandates inter-departmental coordination to establish and maintain consistent logging standards, data formats, and definitions of "critical" loggable events tailored to different system types. This may also necessitate specific training for non-SOC personnel on their logging duties and the importance of their contribution to the overall security posture of the Bank.

Section 3: Log Management Lifecycle

- **3.1 Identification of Critical Log Sources:** A comprehensive inventory of log sources is maintained and regularly reviewed. Critical log sources for World Bank include, but are not limited to:
 - **Network Devices:** Firewalls (traffic, admin, VPN), routers (routing changes, errors), switches (port security, errors), IDS/IPS (alerts, blocked traffic), WAFs, VPN concentrators, DNS servers (queries, zone transfers), DHCP servers.
 - **Servers:** Operating System logs (Windows Event Logs: Security, System, Application; Linux: syslog, auth.log, kern.log), web server logs (access, error), application server logs, virtualization platform logs (hypervisor, VM management).
 - **Endpoints:** Workstation OS logs, mobile device management (MDM) logs, Endpoint Detection and Response (EDR) solution logs.
 - **Applications:** Core Banking System (transaction, admin, error logs), Online/Mobile Banking platforms (user activity, authentication, transaction attempts), Payment Systems (SWIFT, ACH, card processing logs), CRM systems, Loan Origination Systems, custom-developed financial applications.
 - **Databases:** Database Management System (DBMS) audit logs (logins, DDL/DML operations on critical tables, privilege changes), specific transaction logs.
 - **Security Systems:** Authentication servers (Active Directory, RADIUS, LDAP - successful/failed logins, account lockouts, group membership changes), Privileged Access Management (PAM) systems (privileged session recordings, credential access, policy changes), antivirus/anti-malware systems (detections, scans, updates), vulnerability scanners (scan reports), Data Loss Prevention (DLP) systems, physical access control systems.
 - **Cloud Services:** Cloud provider platform logs (e.g., AWS CloudTrail, Azure Activity Log, Google Cloud Audit Logs), logs from SaaS applications (e.g., Office 365 audit logs).
- **3.2 Log Collection, Aggregation, and Centralization (SIEM):**
 - World Bank mandates the use of a centralized Security Information and Event Management (SIEM) system for the collection, aggregation, correlation, and analysis of logs from all identified critical sources.
 - Standardized procedures are documented for onboarding new log sources into the SIEM, including configuration of log forwarding agents or listeners.

- Log data transmission from source systems to the SIEM must be secured using encryption (e.g., TLS/SSL) to protect confidentiality and integrity during transit.
- **3.3 Log Formatting, Parsing, and Normalization:**
 - Whenever possible, log sources shall be configured to generate logs in standardized, parsable formats such as Common Event Format (CEF), Log Event Extended Format (LEEF), JSON, or standardized Syslog formats.
 - The SOC team, in collaboration with system/application owners, is responsible for developing, testing, and maintaining parsers for any custom or non-standard log formats to ensure accurate data extraction.
 - Log data ingested into the SIEM will be normalized to a common schema. This involves mapping diverse log fields to a consistent set of fields within the SIEM (e.g., standardizing timestamp formats, user identifiers, IP addresses, event types) to facilitate effective cross-source correlation and analysis.
- **3.4 Log Storage, Retention, and Disposal:**
 - Log data will be stored securely and retained for periods defined by regulatory requirements, legal obligations, business needs, and forensic investigation purposes. The "World Bank Log Retention Schedule" table specifies these periods. The cost and complexity of storing and managing extensive log data demand a strategic, risk-based prioritization. Storing all logs indefinitely is neither practical nor cost-effective, while insufficient retention can lead to compliance violations or hinder incident investigations. This policy, therefore, mandates a balanced approach, as detailed in the retention schedule, supported by efficient storage solutions and data lifecycle management for logs.

TABLE: World Bank Log Retention Schedule (Illustrative Extract)

| Log Source Category | Specific Log Type | Minimum Retention (Online/Hot) | Minimum Retention (Archive/Cold) | Regulatory Driver(s) |
|------------------------------|---|--------------------------------|----------------------------------|-------------------------------------|
| Authentication (All Systems) | Successful/Failed Logins, Account Lockouts, PW Resets | 90 days | 7 years | SOX, PCI DSS, FFIEC, GLBA |
| Network Firewall/IDS/IPS | All Traffic (Allowed/Denied), Alerts, Signatures | 90 days | 1 year | PCI DSS, FFIEC |
| Core Banking Application | All Financial Transactions, Admin Activity, Errors | 180 days | 7+ years | SOX, FFIEC, AML, Local Banking Regs |
| Online/Mobile Banking | User Session Activity, Transactions, Auth Attempts | 90 days | 7 years | FFIEC, GLBA |
| SWIFT Payment System | Transaction Data, System Events, Operator Activity | 1 year | 5-10 years (per SWIFT/local reg) | SWIFT CSP, AML, FFIEC |

| | | | | |
|--|---|---------|-------------------------------------|--|
| Privileged Access Management (PAM) | Session Recordings, Credential Check-out/in, Policy Changes | 90 days | 3 years | FFIEC, SOX, Internal Audit |
| Database Activity (Critical DBs) | Privileged User Access, DDL/DML on Sensitive Data | 90 days | 1-7 years (as per data sensitivity) | SOX, PCI DSS, GLBA |
| Windows Security Event Logs (DCs) | Security Events (e.g., Kerberos, Account Mgt) | 90 days | 1 year | SOX, Internal Audit |
| DNS Server Logs | Queries, Responses, Zone Transfers | 30 days | 1 year | Security Best Practice, Forensics |
| Cloud Provider Audit Logs (e.g., AWS CloudTrail) | API Calls, Console Logins, Resource Changes | 90 days | 1-7 years (as per service) | Cloud Security Best Practice, Compliance |

* *This table is vital for demonstrating regulatory compliance regarding log retention. It provides clear guidance to IT staff on how long different types of logs must be kept, preventing premature deletion or excessive storage costs. It also aids auditors in verifying compliance. Different regulations (SOX: 7 years for financial records/audit [48, 63]; PCI DSS: 1 year for audit logs [63]) mandate different retention periods. A consolidated schedule ensures all requirements are met and provides a defensible position.*

* Secure and documented procedures for the disposal of log data will be followed once the defined retention period has expired, ensuring data is irrecoverably destroyed.

- **3.5 Log Protection, Integrity, and Access Control:**

- All log data, whether stored online or archived, must be protected from unauthorized access, modification, and deletion.
- Mechanisms such as cryptographic hashing (e.g., SHA-256) or digital signatures will be employed to ensure the integrity of log files and detect any tampering.
- Access to raw log data and log management systems (including the SIEM) will be strictly controlled through Role-Based Access Control (RBAC), adhering to the principle of least privilege. Only authorized personnel (e.g., SOC analysts, specific administrators) will have access necessary for their job functions.
- All access to log data and log management systems will itself be logged and audited regularly.

- **3.6 Clock Synchronization:**

- All systems, network devices, and applications generating logs must be synchronized to a common, authoritative time source, typically via Network Time Protocol (NTP), referencing World Bank's internal stratum 1 NTP servers, which are in turn synchronized with external authoritative time sources.

- Consistent and accurate timestamps across all logs are essential for effective event correlation, forensic analysis, and establishing a clear timeline of activities during an incident investigation.

Section 4: Security Monitoring

- **4.1 Continuous Monitoring Strategy:**

- World Bank mandates 24x7x365 security monitoring of its critical information systems, networks, and applications to detect and respond to threats in a timely manner.
- The SOC will leverage the SIEM platform, EDR solutions, network intrusion detection/prevention systems (NIDS/NIPS), and other security tools for continuous monitoring.
- Threat intelligence feeds (commercial, open-source, and industry-specific like FS-ISAC) will be integrated into the SIEM and other security tools to enhance detection capabilities with up-to-date indicators of compromise (IoCs) and threat actor tactics, techniques, and procedures (TTPs).

- **4.2 Key Monitoring Use Cases and Alerting Scenarios:** The SOC will actively monitor for and investigate alerts related to, but not limited to, the following scenarios. The effectiveness of this monitoring is directly tied to the quality of the log data ingested and the sophistication of the analytical capabilities (correlation rules, User and Entity Behavior Analytics - UEBA) within the SIEM. This means the policy supports not only the act of monitoring but also the continuous refinement of detection logic and ongoing training for analysts to recognize and appropriately respond to the evolving tactics of threat actors.

- **Unauthorized Access and Intrusion Attempts:**

- Multiple failed login attempts to critical systems, applications, or user accounts within a short timeframe.
- Successful logins from unusual or high-risk IP addresses, geolocations, or at anomalous times (e.g., outside standard business hours for a user).
- Use of default, shared, or compromised credentials.
- Attempts to bypass authentication mechanisms.
- Firewall/IDS/IPS alerts indicating blocked intrusion attempts or policy violations.

- **Malware and Malicious Code Activity:**

- Antivirus/anti-malware/EDR alerts for detected malware, ransomware, or suspicious executables.
- Detection of known malicious file hashes or C2 (Command and Control) server communication.
- Suspicious process creation or modification on endpoints or servers.
- Unauthorized outbound connections to known malicious domains or IP addresses.
- **Data Exfiltration and Leakage:**
 - Anomalous outbound network traffic patterns (e.g., large volumes of data to unknown external destinations, unusual protocols).
 - Access to large volumes of sensitive data followed by external data transfers.
 - DLP alerts indicating policy violations regarding sensitive data movement.
 - Unauthorized use of USB drives or other removable media on critical systems.
- **Insider Threat Indicators:**
 - Anomalous user behavior deviating from established baselines (UEBA alerts).
 - Unauthorized attempts to access sensitive files, systems, or applications not related to the user's job function.
 - Privilege escalation attempts or unauthorized changes to user permissions.
 - Unusual data aggregation, copying, or printing of sensitive information.
 - Activity during non-standard hours or from unapproved locations for specific users.
- **System and Application Anomalies:**
 - Unexpected system crashes, service failures, or critical errors reported in system logs.
 - Significant deviations in application performance or resource utilization (CPU, memory, network).
 - Unauthorized changes to critical system configurations, security policies, or application settings.

- **Privileged Account Activity Monitoring:**
 - All privileged account logins and logoffs.
 - Execution of privileged commands and utilities.
 - Creation, modification, or deletion of privileged accounts.
 - Alerts from PAM solution for policy violations or suspicious privileged sessions.
- **Payment System Anomalies:**
 - Suspicious transaction patterns in core banking, online banking, or SWIFT systems (e.g., unusually large transactions, transactions to high-risk countries without justification, rapid succession of transfers from a newly active account).
 - Multiple failed payment attempts.
 - Unauthorized changes to payment beneficiaries or limits.
- **Physical Security Alerts:**
 - Unauthorized access attempts to data centers or other secure areas, if logs are integrated.
- **4.3 Alerting Mechanisms and Thresholds:**
 - The SIEM and other monitoring tools will be configured to generate real-time alerts for high-severity and critical security events.
 - Alerting thresholds will be carefully defined and regularly tuned for each use case to balance sensitivity with the need to minimize false positives and alert fatigue.
 - Alerts will be prioritized based on severity and potential impact, and clear escalation procedures will be documented and followed by the SOC team.
- **4.4 Security Event Correlation and Analysis:**
 - The SIEM platform will be utilized to correlate security events from diverse log sources to identify complex attack patterns, multi-stage intrusions, and subtle indicators of compromise that might be missed when analyzing logs in isolation.
 - Correlation rules will be continuously developed, tested, and refined by the SOC team based on emerging threats, new vulnerabilities, and lessons learned from past incidents.

Section 5: Log Review and Incident Investigation

- **5.1 Procedures for Regular Log Reviews:**

- **Automated Alerts Review:** The SOC team will review and investigate SIEM-generated alerts on a 24/7 basis, prioritizing based on severity.
- **Daily Log Reviews:** A daily review of critical security system logs (e.g., firewall, IDS/IPS, key authentication servers, PAM) and high-priority SIEM alert summaries will be conducted by SOC analysts.
- **Weekly/Monthly Log Reviews:** More comprehensive reviews of specific log types (e.g., privileged user activity, database access logs for sensitive tables, remote access logs) and overall security event trends will be performed to identify patterns or anomalies not caught by real-time alerts.
- All log review activities, findings, and actions taken will be documented in a log review register or the SIEM's case management system.

- **5.2 Forensic Readiness and Evidence Preservation:**

- Procedures are established to ensure that log data is collected and preserved in a manner that maintains its integrity and admissibility for forensic investigations and potential legal proceedings. This includes maintaining chain of custody for critical log evidence.
- The SOC team will work closely with the Incident Response Team (IRT) and, if necessary, external forensic investigators, providing them with access to relevant log data during an investigation.
- Log reviews themselves should be risk-driven and intelligence-led, rather than a mere compliance exercise. The focus of manual or semi-automated reviews should be on high-risk systems, accounts, and activity patterns that are known to be targeted by current threat actors specific to the financial sector. This proactive "threat hunting" within logs is more effective than generic, broad-stroke reviews of voluminous data. Automated alerts from the SIEM serve as the primary guide for reactive reviews, but threat intelligence can highlight specific IoCs or TTPs that analysts should actively search for within the log data.

Section 6: Policy Review and Exceptions

- **6.1 Review Cycle:** This Logging and Monitoring Policy will be reviewed and updated at least annually, or more frequently in response to significant changes in World Bank's IT environment, threat landscape, business operations, or regulatory requirements.
- **6.2 Exception Process:** Any requests for exceptions to this policy (e.g., disabling logging on a specific system temporarily for critical maintenance) must be formally documented, submitted to the Security Manager for approval, include a risk

assessment, and specify compensating controls. Approved exceptions will be logged and reviewed periodically.

Appendix A: Logging and Monitoring Simulation Items/Scenarios for World Bank

1. **Scenario Trigger:** SIEM alert indicates 50 failed login attempts within 5 minutes for a privileged administrator account on the Core Banking System.
 - **Action:** SOC analyst to investigate the source IP, time of attempts, and previous login patterns for this account. Escalate per IRP.
2. **Scenario Trigger:** Network monitoring tool flags an unusually large data transfer (e.g., >1GB) from an internal database server to an unknown external IP address during non-business hours.
 - **Action:** SOC analyst to identify the database, type of data potentially involved, and the destination. Correlate with any authorized data transfers.
3. **Scenario Trigger:** An employee reports receiving a highly convincing phishing email requesting their VPN credentials.
 - **Action:** SOC team to analyze email gateway logs for other recipients, check VPN logs for any suspicious login attempts related to reported users, and scan endpoint logs of the reporter for malware.
4. **Correlation Rule Test:** Simulate a sequence of events: multiple failed logins from IP A to Server X, followed by a successful login from IP A to Server X, followed by Server X attempting to connect to a known C2 IP address.
 - **Action:** Verify the SIEM generates a correlated high-severity alert.
5. **SWIFT System Log Review:** Review SWIFT Alliance Access event logs for any unauthorized login attempts or changes to message routing rules.
 - **Action:** Document findings from a 24-hour period of logs.
6. **Malware Detection Test:** A test malware (non-destructive) is "executed" on a sandboxed endpoint.
 - **Action:** Verify EDR and antivirus logs detect and report the malware. Check if SIEM receives these alerts.
7. **Log Retention Verification:** Attempt to retrieve authentication logs for a critical server from 100 days ago.

- **Metric:** Confirm logs are available in online/hot storage as per the retention schedule (90 days for this example). Attempt to retrieve logs from 13 months ago from archive.
8. **Clock Synchronization Audit:** Select 5 critical servers from different segments.
- **Action:** Verify their system clocks are synchronized with the authoritative NTP server and note any discrepancies greater than 1 second.
9. **Log Tampering Simulation:** On a non-production server, attempt to modify or delete a critical security event log file.
- **Action:** Verify if File Integrity Monitoring (FIM) or other controls detect and alert on this unauthorized modification.
10. **Lateral Movement Detection:** Analyze VPN logs, Active Directory logs, and endpoint logs to trace a simulated attacker's movement from a compromised workstation to a domain controller.
- **Action:** Document the sequence of log entries that would indicate this activity.
11. **PAM Session Log Review:** Review the session recording and command log for a specific administrator's privileged session on a database server during a simulated critical patch deployment.
- **Action:** Identify any commands executed that were outside the scope of the approved change request.
12. **Unauthorized Software Detection:** An unapproved P2P file-sharing application is "installed" on a test workstation.
- **Action:** Verify if application control logs or EDR logs detect and alert on the unauthorized software.
13. **Threat Intelligence IOC Search:** A new threat intelligence report lists 5 new malicious IP addresses targeting financial institutions.
- **Action:** SOC analyst to search historical firewall and IDS/IPS logs in SIEM for any communication with these IPs in the last 30 days.
14. **VPN Anomaly Detection:** VPN logs show a user simultaneously logged in from two geographically distant locations.
- **Action:** Investigate as a potential compromised account or policy violation.
15. **Web Application Attack Detection:** Simulate a basic SQL injection attempt against a non-production web application.
- **Action:** Verify if WAF logs or application server logs detect and record the attempt.

16. **Cloud Service Log Ingestion Check:** A new IaaS virtual machine is commissioned in Azure/AWS.
- **Action:** Verify within 24 hours that its OS and security logs are being successfully ingested into the central SIEM.
17. **SIEM Access Audit:** Generate a report of all users who accessed the SIEM platform in the last 7 days.
- **Action:** Review the list for any unauthorized or unexpected accounts.
18. **AML Transaction Monitoring Alert:** An AML system flags a series of transactions as potentially structured to avoid reporting thresholds.
- **Action:** Correlate AML system logs with customer account activity logs and KYC information in the SIEM to build a comprehensive case for review.
19. **Physical Access Log Correlation:** (If integrated) A data center door forced open alert from the physical access control system is received.
- **Action:** Correlate with internal network monitoring logs for any unusual activity originating from the data center segment around the time of the physical alert.
20. **DNS Query Anomaly:** DNS logs show internal clients repeatedly querying for a known malicious domain or a domain with a DGA (Domain Generation Algorithm) pattern.
- **Action:** Identify the affected clients and investigate for malware infection.