Cybersecurity Policy Templates

Log Management Policy

(Last Updated April 2025)

Purpose

Our Log Management Policy aims to establish a structured and systematic approach for collecting, monitoring, and analyzing log data generated by our organization's systems, applications, and network infrastructure. This policy aims to provide clear guidelines and procedures for collecting, retaining, protecting, and analyzing logs to support effective cybersecurity incident detection, response, and forensic investigations. By implementing robust log management practices, this policy seeks to enhance our visibility into security events, identify anomalous activities, and mitigate potential threats to our systems and data. Through implementing centralized logging, log retention periods, and log review processes, we strive to maintain the integrity, confidentiality, and availability of log data, enable timely incident response, and ensure compliance with applicable regulations and industry standards. By prioritizing log management, we strengthen our overall cybersecurity posture, enhance threat detection capabilities, and maintain the trust and confidence of our stakeholders.

Scope

The Log Management Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses collecting, storing, analyzing, and retaining log data generated by systems, applications, and network devices within our IT infrastructure. This policy covers all logs, including events, access, audit, and system logs. It sets forth guidelines for log generation, aggregation, and centralized management to ensure accurate and timely log data availability for security monitoring, incident detection, and forensic investigations. The policy defines procedures for log retention periods, access controls, and log review processes. It also outlines the responsibilities of individuals involved in log management activities, including system administrators, security analysts, and log administrators. Compliance with this policy is mandatory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for log management and cybersecurity governance.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

LOG-01	Maintain at least three enterprise-managed time sources that the organization's information systems can use to synchronize time.
LOG-02	Ensure the organization's operating system configuration benchmarks enable appropriate logging on all computing systems.
LOG-03	Ensure the organization's network device configuration benchmarks enable appropriate logging on all network devices.
LOG-04	Ensure the organization's business application configuration benchmarks enable appropriate logging on all business applications.
LOG-05	Ensure the organization's cloud configuration benchmarks enable appropriate logging on all Cloud Service Providers (CSPs) and Software-as-a-Service (SaaS) platforms.
LOG-06	Maintain a system to aggregate all appropriate logs from each organization's information system.
LOG-07	Ensure the organization's aggregated information system logs are only accessible to authorized workforce members.
LOG-08	Ensure the organization's aggregated information system logs and alerts when logs have not been received from an information system after a defined period.
LOG-09	Ensure the organization's aggregated information system is regularly tuned to ensure appropriate log events are alerted to the appropriate workforce members.
LOG-10	Define a process the organization shall use to regularly review the logs aggregated from the organization's information systems.

LOG-11	Ensure that the organization's regular log review process includes clear Service Level Agreements (SLAs) for who should monitor aggregated information system logs (such as a Security Operations Center (SOC)).
LOG-12	Define a process the organization shall use to automate the review of aggregated logs.
LOG-13	Define a process the organization will use to automate alerting on threats discovered by its aggregate log management system.
LOG-14	Define a process the organization shall use to retain information systems logs over time (including how long to retain logs of particular types).
LOG-15	Implement a log management system (such as a SIEM, SOAR, or service management platform) to track the status of alerts generated by the organization's log management system.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.