Logging and Monitoring Policy

Purpose

Logs only help if someone looks at them. This policy defines what Your Organization logs, how those logs are protected and kept, and how alerts are reviewed and escalated, so that suspicious or abnormal activity is detected quickly and handled through the incident response process.

Scope

This policy applies to all Your Organization production systems, cloud accounts, identity providers, endpoints, network and security devices, and to the people and teams responsible for operating and monitoring them. Detailed audit-record requirements for regulated environments are set out in the Audit and Accountability Policy.

What is logged

Every in-scope system logs, at minimum: authentication events (success and failure), privilege and permission changes, administrative and configuration changes, access to Confidential or Restricted data, security tool events (malware detections, firewall denials, agent failures), and failures of logging itself. Each entry carries a timestamp, the user or process identity, the event type and outcome, and the affected resource, where technically feasible.

Centralization and protection

Logs are sent to a central logging platform that is separate from the systems producing them, so that a compromised system cannot quietly erase its own history. Access to the logging platform is limited to named personnel, is itself logged, and log data cannot be modified by ordinary administrators. System clocks are synchronized to an authoritative time source.

Retention

Logs are retained for at least 90 days in searchable form and at least 12 months in archive, unless a contract, regulation, or legal hold requires longer. Retention periods are recorded in the data retention schedule, and logs are deleted at the end of their period.

Monitoring and alerting

Your Organization defines alert rules for the events that matter most: repeated failed sign-ins, sign-ins from unusual locations, new administrator accounts, disabled security tooling, unexpected data transfers, and changes to logging configuration. Each alert rule has an owner, a severity, and a documented first response. Alert rules are reviewed at least annually and after every significant incident.

Review and escalation

High-severity alerts are triaged within one business hour during staffed hours, with an on-call route outside them. Lower-severity alerts and a summary of log activity are reviewed at least weekly. Any alert confirmed as a possible security event is escalated under the Incident Response Plan. Reviewers record what they checked and what they found.

Gaps and failures

If a system cannot produce the required logs, or logging stops, the system owner records an exception with a compensating control and a remediation date. A silent logging failure on a Tier 1 system is treated as a security event until proven otherwise.

Roles and responsibilities

- **Security lead** owns this policy, the alert rules, and the review schedule.
- **System owners** make sure their systems log to the central platform and fix gaps.
- **Platform and operations teams** run the logging platform and keep it available and protected.
- **All personnel** report suspicious activity they notice, even if no alert fired.

Compliance and exceptions

Compliance is checked through periodic sampling of systems and alert handling records. Exceptions require written approval from the security lead and are reviewed on a fixed date. Violations of this policy may lead to disciplinary action.

Review

This policy is reviewed at least annually, and after any incident in which detection was late or missing.

Effective [the date this policy takes effect].