# Information Security Monitoring Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. NIST SP 800-137: <https://csrc.nist.gov/pubs/sp/800/137/final>
2. NIST 800-92: <https://csrc.nist.gov/pubs/sp/800/92/final>
3. NIST SP 800-12: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter15.html
4. ISO/IEC 27001:2022: A.7.4, A.7.5, A.8.12, A.8.15, A.8.16, A.8.21
5. NIST 800-53 rev. 5: AC-2(4), AC-2(12), AC-4, AC-17(1), AC-21, AU-2, AU-3, AU-3(1), AU-4, AU-5, AU-6, AU-6(1), AU-6(3), AU-7, AU-7(1), AU-9, AU-9(4), AU-11, AU-12, CA-1, CA-3, CA-7, CA-8(3), CM-5(1), CP-2, IR-9, PE-6, PE-6(1), PE-13, PE-14, PE-15, SC-4, SC-5, SC-7, SC-7(12), SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(16), SI-4(18), SI-4(23), SI-5, SI-7, SI-7(1), SI-7(7), SI-12
6. CIS v8: 3.13, 3.14, 8.2, 8.3, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.11, 10.5, 13.1, 13.2, 13.3, 13.6, 13.7, 13.8, 13.11
7. PCI DSS 4.0: 1.4.3, 3.1.1, 3.4.2, 5.3.4, 6.4.2, 7.2.3, 9.2.1.1, 9.4.3, 10.1.1, 10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7, 10.2.2, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.4.1, 10.4.1.1, 10.4.2, 10.4.2.1, 10.5.1, 10.7.1, 10.7.2, 10.7.3, 11.5.1, 11.5.2, 11.5.1.1, 12.10.5
8. AICPA SOC 2 TSC: A1.1, A1.2, C1.1, C1.2, CC4.1, CC6.1, CC6.4, CC6.7, CC6.8, CC7.1, CC7.2, P6.1, PI1.5

## Document ownership

<(Choose from)>

* 1. Policy Owner:
     1. [Owner name] ([Owner email]), [Owner title]
  2. Information Security Officer:
     1. [Information officer name], ([Information officer email]), [Information officer title]
  3. System Owner(s):
     1. [System owner name], ([System owner email]), [System owner title]
  4. Process and Operational Owner(s)
     1. [process owner], ([process owner email]), [process owner title]
  5. System Administrator(s):
     1. [System admin name], ([System admin email]), [System admin title]
  6. Required Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT
  7. Optional Dissemination: <(Choose from)>
     1. IT Administrator
     2. Engineering
     3. Product Management
     4. Support
     5. Information Security Team
     6. [Organization name] Leadership Team
     7. Contractors
     8. Vendors
     9. Company Wide
     10. [Organization name] SIRT

## Purpose

The purpose of this Information Security Monitoring Policy is to establish guidelines and procedures for monitoring various systems and activities within the organization to detect, prevent, and respond to unauthorized access, data breaches, system anomalies, and other security threats. This policy aims to ensure the integrity, availability, and confidentiality of the organization's information systems and data by implementing comprehensive monitoring practices. By doing so, the organization can proactively identify and mitigate potential security risks, ensure compliance with regulatory requirements, and maintain the trust of stakeholders.

## Scope

This policy applies to all employees, contractors, vendors, and any other individuals or entities with access to the organization's information systems. It covers the monitoring of:

* System Activity and Security Events: Detecting unusual behavior, unauthorized access, and analyzing security incidents.
* Access and Integrity of Critical Systems and Files: Ensuring only authorized access and protecting against unauthorized modifications.
* Data Transfers and Loss Prevention: Monitoring communications for threats, especially transfers of sensitive information, and preventing data leakage.
* Physical Access: Securing physical access to facilities and systems.
* Environmental Conditions: Monitoring critical infrastructure conditions
* Alert Management: aggregating logs, and managing alerts effectively.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], [owner title] | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | Executive Team | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | Executive Team | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], [Information officer title] | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner],  Operational owner title] |  |
| Information Systems Administrators | System Administrators | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], [HR title] | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users | End Users | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | [provider type] | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
  2. Management has reviewed and approved this policy.
  3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
  4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
  2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. System Activity Monitoring: The continuous observation and analysis of system operations to detect unusual or malicious behavior.
  2. Security Event Monitoring: The process of reviewing and analyzing security-related events to identify potential threats or vulnerabilities.
  3. Access Monitoring: The practice of tracking and recording access to highly critical systems and files to ensure only authorized individuals have entry.
  4. Integrity Checks: Procedures used to verify that critical or risky systems and files remain unaltered and secure from unauthorized modifications.
  5. Data Transfer Monitoring: The surveillance of data transfers, particularly those involving highly sensitive protected data, to prevent unauthorized access or leaks.
  6. Data Loss Prevention (DLP): Strategies and tools designed to prevent the unauthorized transmission of sensitive information outside the organization.
  7. Storage and Processing Capacity Monitoring: The regular assessment of system storage and processing capabilities to ensure adequate availability and performance.
  8. Network Traffic Monitoring: The continuous inspection of inbound and outbound network traffic to detect unauthorized access, data leakage, or malicious activity.
  9. Physical Access Monitoring: The surveillance of physical entry to facilities and systems, including the use of video surveillance and access control systems.
  10. Humidity and Temperature Monitoring: The measurement and regulation of environmental conditions (humidity and temperature) in areas housing critical IT infrastructure.
  11. Log Aggregation: The collection and centralization of log data from various sources for easier analysis and monitoring.
  12. Security Information and Event Management (SIEM): A system that aggregates and analyzes log data from different sources to provide real-time analysis of security alerts.
  13. Intrusion Detection and Prevention Systems (IDS/IDP): Tools used to detect and prevent unauthorized access or attacks on a network or system.
  14. Audit Logs: Records of system activities that provide a trail of security-relevant events and actions for review and analysis.
  15. Backup: The process of creating copies of data to ensure its availability and integrity in the event of data loss or corruption.
  16. Alert Management: The processes and procedures for handling alerts generated by monitoring systems, including prioritization, response, and resolution.
  17. Unauthorized Access: Any access to a system or data that is not granted or allowed by the system's owner or security policies.
  18. Anomalous Behavior: Activities or patterns of behavior that deviate from the norm and may indicate potential security threats.
  19. Intrusion Detection: The process of monitoring and analyzing network or system activities to identify possible security breaches.
  20. Intrusion Prevention: Measures taken to block or prevent detected security breaches from causing harm or unauthorized access.
  21. Environmental Conditions: The physical factors, such as humidity and temperature, that can affect the performance and safety of IT infrastructure.
  22. Anomaly Detection: The process of identifying unusual patterns or discrepancies in log data that may indicate security issues.

## Policy

#### System Activity Monitoring

The [responsible party] shall:

* + 1. Monitor system activity to detect attacks, unauthorized access, and anomalous behavior.
    2. Utilize tools such as intrusion detection systems, log anomaly detection, and continuous vulnerability monitoring.
    3. Analyze detected events and anomalies, adjusting monitoring levels based on risk changes.
    4. Correlate data from monitoring tools to identify covert exfiltration of information.
    5. Alert the Information Security Team upon detection of compromise indicators.
    6. Employ automated mechanisms to integrate audit review, analysis, and reporting processes.
    7. Ensure audit records include event type, timing, location, source, outcome, and involved identities.

#### System Integrity

The [responsible party] shall:

* + 1. Use integrity verification tools to detect unauthorized changes to critical system components.
    2. Perform integrity checks at startup, security-relevant events, and monthly.
    3. Alert relevant teams upon detection of unauthorized changes.

#### Data Loss Prevention Strategy

The [responsible party] shall:

* + 1. Continuously monitor communications traffic for unauthorized access and data leakage.
    2. Analyze outbound communications to detect covert information exfiltration.
    3. Implement host-based monitoring mechanisms as approved.
    4. Implement mechanisms to monitor data transfers for unusual size or destinations.
    5. Alert upon detection of potential data leakage.
    6. Employ automated tools for real-time analysis of data loss prevention events.

#### Storage and Processing Capacity and Availability

The [responsible party] shall:

* + 1. Continuously monitor system metrics as part of the continuous monitoring strategy.
    2. Report the security and privacy status of the system quarterly.
    3. Include effectiveness, compliance, and change monitoring in risk assessments.

#### Physical Access

The [responsible party] shall:

* + 1. Record all entries to secure areas using CCTV and access control systems.
    2. Alert the Security team upon detection of abnormal or unauthorized physical access events

#### Humidity and Temperature

The [responsible party] shall:

* + 1. Implement monitoring systems for critical IT infrastructure areas.
    2. Alert upon detection of abnormal environmental conditions.

#### Protection of Logs from Being Altered or Deleted

The [responsible party] shall:

* + 1. Protect audit logs from unauthorized access, modification, and deletion.
    2. Authorize access to log management functions only to approved personnel.
    3. Monitor for unauthorized access or modification attempts and alert accordingly.
    4. Ensure daily backups of audit logs to a separate, secure location.
    5. Regularly verify the integrity and availability of backup logs.

#### Alerts

The [responsible party] shall:

* + 1. Generate and disseminate internal security alerts, advisories, and directives.
    2. Monitor and respond to system-generated alerts related to security and quality issues.
    3. Establish procedures for alert management, including prioritization criteria and response protocols.
    4. Assign roles and responsibilities for managing alerts to appropriate personnel.
    5. Regularly review and update alert management procedures for effectiveness.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
  2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
  3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
     1. Policies
     2. Procedures
     3. Standards
     4. Documentation
     5. Regulations
     6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
  2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
     1. The Information Security Officer
     2. Officer of the [Organization name] Leadership Team
  3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |