# Audit and Accountability 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 and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. NIST 800-92: <https://csrc.nist.gov/pubs/sp/800/92/final>
2. NIST SP 800-100: <https://csrc.nist.gov/pubs/sp/800/100/r1/iprd>
3. NIST SP 800-115: <https://www.nist.gov/privacy-framework/nist-sp-800-115>
4. ISO/IEC: <https://www.iso.org/publication/PUB100484.html>
5. ISO/IEC 27007: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27007:ed-3:v1:en>
6. ISO/IEC TS 27008: <https://www.iso.org/standard/67397.html>
7. ISO/IEC 27001:2022: 4.4, 5.1.e, 6.1.1.a, 6.1.1.e, 7.5.3, 9.1, 9.2.1, 9.2.2, 9.3.1, 10.1, 10.2.d, 6.1.1.c, 6.1.1.e, 9.1, 9.2.1, A.5.31, A.5.33, A.5.35, A.5.36, A.8.15, A.8.34
8. NIST 800-53 rev. 5: AU-1, AU-4, AU-5, AU-9, AU-9(4), AU-11, CA-1, CA-2, CA-2(1), CA-2(3), CA-5, CA-7(1), CA-7(4), CA-8, CA-8(1), CA-8(2), PL-1, PL-2, PS-3(3), SI-2(3), SI-6, SI-12
9. AICPA SOC 2 TSC: C1.2, CC1.3, CC2.1, CC3.1, CC3.4, CC4.1, CC4.2, CC5.3, CC7.1, CC7.2, P3.1
10. CIS v8: 7.2, 7.7, 8.3, 8.10, 16.13, 18.1, 18.2, 18.3, 18.4, 18.5
11. PCI DSS 4.0: 1.2.7, 5.3.4, 9.3.1.1, 10.2.1.3, 10.3.1, 10.3.2, 10.3.3, 10.4.3, 10.5.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 12.3.4, 12.5.2, 12.5.2.1, 12.5.3

## 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 the Audit and Accountability Policy is to establish a framework for the management of audit and accountability functions within the organization. This policy aims to ensure the integrity, confidentiality, and availability of information systems by:

* Upholding legal and business obligations related to audit and accountability.
* Ensuring the quality and nature of formal reports and the protection of logs and records.
* Supporting the detection and investigation of unauthorized access and other security incidents.
* Promoting continuous improvement and compliance with applicable regulations and standards.

## Scope

This policy applies to all organizational information systems, personnel, and processes involved in audit and accountability functions. It encompasses the following key areas:

* Retention and protection of audit records and logs.
* Determination of the scope of systems and events to be audited.
* Establishment and maintenance of a Compliance Management Program.
* Conduct of internal audits by qualified and independent personnel.
* Engagement of external auditors and assessors for comprehensive evaluations.
* Execution of penetration testing, including both system and physical tests.
* Assessment of the effectiveness of security controls through continuous monitoring and corrective actions.

The policy is applicable to all departments, employees, contractors, and third-party service providers with access to organizational information systems. It mandates adherence to the defined procedures and controls to ensure robust audit and accountability practices across the organization.

## 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. Audit Information: Data collected about system activities, including logs of access, changes, and system operations, used to support audit functions and investigations.
  2. Audit Logging Tools: Software or hardware solutions designed to capture, store, and manage audit information.
  3. Audit Records: The documented logs and data generated by audit logging tools that provide evidence of system activities and events.
  4. Compliance Management Program: A structured approach to ensure that an organization adheres to legal, regulatory, and internal standards, including continuous monitoring and assessment.
  5. Continuous Monitoring: Ongoing evaluation of security controls and system activities to ensure effectiveness and compliance with policies and regulations.
  6. Corrective Action Plans: Strategies developed to address deficiencies identified during audits and assessments to improve system security and compliance.
  7. External Audit: An independent assessment conducted by third-party auditors to evaluate the security and compliance of an organization's information systems.
  8. Internal Audit: An assessment conducted by an organization's own qualified personnel to evaluate the security and compliance of its information systems.
  9. Penetration Testing: Simulated attacks on a system to identify vulnerabilities and assess the effectiveness of security measures, including red team (attackers) and blue team (defenders) exercises.
  10. Physical Penetration Tests: Assessments to evaluate the effectiveness of physical security controls by attempting to gain unauthorized physical access to facilities.
  11. Red Team: A group of security professionals who simulate adversarial attacks on a system to identify vulnerabilities.
  12. Blue Team: A group of security professionals responsible for defending an organization's information systems against attacks, often working in conjunction with red team exercises.
  13. Rules of Engagement: Formal agreements that outline the scope, objectives, and boundaries of penetration tests and security assessments.
  14. System Owner: The individual or entity responsible for the overall management and security of an information system.
  15. Information Security Officer: The person responsible for overseeing an organization's information security program, including audit and accountability functions.
  16. Unauthorized Access: Any attempt to access systems, data, or resources without permission, often detected through audit logs and addressed through security controls.
  17. Audit Processing Failures: Issues that arise when audit logs are not properly generated, captured, or stored, requiring immediate attention and corrective actions.
  18. Independence and Objectivity: The requirement that audit personnel must not have conflicts of interest or biases that could affect their judgment or findings.
  19. Scope of Audit: The specific systems, processes, and activities that are included in an audit, determined based on organizational needs and regulatory requirements.
  20. Qualified Personnel: Individuals with the necessary skills, knowledge, and experience to conduct audits and assessments effectively.
  21. Continuous Improvement: An ongoing effort to enhance security measures, processes, and controls based on findings from audits and assessments.
  22. Chain of Custody: The documented process of handling and storing audit records to ensure their integrity and reliability as evidence.
  23. Sanitization Mechanisms: Techniques used to remove sensitive data from media before disposal or reuse, ensuring that data cannot be recovered.
  24. Retention Period: The length of time audit records must be kept to meet regulatory and organizational requirements.
  25. Audit Reduction and Report Generation: The process of summarizing and analyzing audit records to produce actionable insights and reports without altering original data.
  26. Security Controls: Measures implemented to protect information systems and data from threats, including technical, administrative, and physical safeguards.

## Policy

#### Audit Logs

The [responsible party] shall:

* + 1. Ensure that the following events are to be logged within the information systems:
       1. successful and unsuccessful account logon events
       2. account management events
       3. object access
       4. policy change
       5. privilege functions
       6. process tracking
       7. system events.
    2. Ensure that audit records are retained off the originating system until they are no longer needed for administrative, legal, audit, or alternative purposes.
    3. Protect audit information and logging tools from unauthorized access, modification, and deletion.
    4. Upon detecting unauthorized access, modification, or deletion of audit information, alert the information security officer or system owner.
    5. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection of event criteria to be logged.

#### Establishment of a Compliance Management Program

The [responsible party] shall:

* + 1. Develop, document, and implement a comprehensive compliance management plan that includes identifying applicable regulations and standards and the mechanisms for continuous monitoring and assessment of compliance.
    2. Ensure the compliance management program is reviewed and updated annually or whenever the regulatory or threat environment changes.

#### Internal Audits by Qualified Personnel

The [responsible party] shall:

* + 1. Conduct internal audits of the information system at least annually, using qualified personnel with the necessary degree of independence and objectivity.
    2. Document findings and corrective actions from internal audits and report them to senior management and the Information Security Officer

.

#### External Audits and Assessments

The [responsible party] shall:

* + 1. Determine the type and scope of audits and assessments required to meet business objectives and regulatory requirements
    2. Engage qualified external auditors and assessors to conduct at least annually comprehensive audits and assessments of the information system.
    3. Ensure that external audit reports are reviewed and corrective actions are taken to address identified deficiencies.

#### Penetration Testing

The [responsible party] shall:

* + 1. Coordinate penetration testing of the system by qualified personnel.
    2. Establish rules of engagement and formal agreements on the scope and objectives of penetration tests.
    3. Conduct at least annual system penetration tests, including red team and blue team exercises.
    4. Perform physical penetration tests to evaluate the effectiveness of physical security controls.

#### Continuous Improvement

The [responsible party] shall:

* + 1. Establish a continuous monitoring program to evaluate security controls' effectiveness and identify areas for improvement.
    2. Implement corrective action plans to address any deficiencies identified during assessments.
    3. Commit to continuous improvement by regularly updating security policies and procedures based on assessment findings and changes in the threat landscape.

## 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** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |