# ISO 27001-Compliant Security and Privacy Monitoring Procedure Template

## Introduction

This Security and Privacy Monitoring Procedure aligns with ISO 27001 standards, providing a structured approach to monitoring and safeguarding sensitive information. Examples of sensitive information include personally identifiable information (PII), financial records, intellectual property, and confidential business data. It ensures the organization’s systems and data are continuously monitored to identify and respond to potential security and privacy incidents effectively.

## Purpose

The purpose of this procedure is to establish a comprehensive monitoring framework that safeguards the confidentiality, integrity, and availability of information assets while ensuring compliance with applicable legal, regulatory, and contractual obligations.

## Scope

This procedure applies to all information systems, applications, and users within the organization, including:

* Employees, contractors, and third-party service providers
* On-premises, cloud-based, and hybrid systems
* Data storage, processing, and transmission activities

## Policy Statement

The organization shall implement a robust security and privacy monitoring framework to:

* Continuously monitor systems, networks, and applications for suspicious activities.
* Identify potential vulnerabilities and threats proactively.
* Ensure timely response and mitigation of identified security and privacy incidents.

The procedure includes the following six steps:

1. Planning: Define monitoring objectives, scope, and resources.
2. Implementation: Deploy monitoring tools and configure them to capture relevant logs and alerts.
3. Monitoring: Continuously monitor activities using automated tools and manual oversight.
4. Analysis: Evaluate logs, alerts, and reports to identify trends and potential risks.
5. Response: Initiate incident response actions based on analysis findings.
6. Review and Optimization: Regularly review monitoring effectiveness and adjust processes as needed.

## Roles and Responsibilities

* Information Security Officer: Oversee the monitoring framework, ensuring alignment with ISO 27001 controls.
* IT Operations Team: Deploy and maintain monitoring tools and technologies.
* Incident Response Team: Analyze incidents and execute mitigation plans.
* Data Protection Officer: Ensure monitoring activities comply with data privacy regulations.
* Third-Party Vendors: Adhere to defined monitoring and incident reporting standards.

## Compliance and Monitoring

Compliance with this procedure will be ensured through:

* Periodic audits of monitoring tools and processes
* Regular reviews of incident logs and reports
* Implementation of key performance indicators (KPIs), such as:

- Number of detected and resolved incidents

- Average response time to incidents

- Percentage of systems with active monitoring enabled

The effectiveness of KPIs will be evaluated by analyzing trends over time, benchmarking against industry standards, and incorporating feedback from incident post-mortems. A change log or version control system will be used to track updates to the monitoring framework.

## Related Documentation

* Information Security Policy
* Incident Response Plan
* Data Protection Policy
* Risk Assessment Procedure

## Review and Revision

This procedure will be reviewed annually or when significant changes occur in the organizational environment, regulatory requirements, or technological landscape. The Information Security Officer will initiate the review process, and updates will be communicated to stakeholders through official channels such as email notifications or team meetings. Updates will be documented and approved through a formal review process.

## Narrative Guidance

This procedure emphasizes a proactive approach to security and privacy monitoring, integrating ISO 27001 principles of continuous improvement and risk management. Organizations are encouraged to customize this template to address specific risks, technological requirements, and operational needs.

## Instructions for Use

* Replace placeholders with organization-specific details.
* Tailor monitoring objectives and tools to your operational environment.
* Collaborate with stakeholders to ensure the procedure aligns with business and compliance goals.