# Security Incident Management Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

## Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to minimize the impact of security incidents by ensuring controls are in place for identification, management, and communication of security events and weaknesses through a formal process to ensure that [Company Name] information assets and information systems are protected.

The policy defines how [Company Name]’s identifies security incidents, analyzes, and determine the magnitude of the threat presented by these incidents, responds to the incident, and reports the incident to stakeholders.

## Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Security Incident Management Policy applies to all business processes and data, information systems and components, personnel, and physical areas of [Company Name].

## Definitions

Define any key terms, acronyms, or concepts that will be used in the policy or accompanying procedures. A standard glossary approach is sufficient.

## Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

|  |  |
| --- | --- |
| **Guidance** | **Section** |
|  |  |

## Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Dividing this section into subsections may be required depending on the length or complexity of the policy. Mapped regulations can be edited based on policy requirements.

|  |  |  |
| --- | --- | --- |
| # | Policy Statement | Mapped Regulations/Standards |
|  | Assign responsibilities for security incident management. | NISTCSF1: RS.CO-1  NISTCSF2: GV.SC-08  NIST800-171: 3.6.1  NIST800-53: IR-1, IR-4, IR-4(11), IR-7, IR-7(1), IR-8  CMMC: IR.L2-3.6.1  SOC2: CC2.2, CC7.3, CC7.4  ISO27002: 5.24  CIS: 17.1, 17.5  PCI: 12.10.1  HIPAA: §164.308(a)(6)(i) |
|  | Implement mechanisms for employees, customers, and third parties to report security vulnerabilities. | NISTCSF1: RS.CO-1, RS.AN-5  NISTCSF2: ID.RA-08  NIST800-171: 3.6.1, 3.14.1  NIST800-53: IR-6, IR-6(1)  CMMC: SI.L1-3.14.1, IR.L2-3.6.1  SOC2: CC2.2, CC7.3  ISO27002: 6.8  CIS: 16.2, 17.3 |
|  | Response capabilities must be maintained for required time frames (e.g. 24/7). | NIST800-171: 3.6.1  NIST800-53: IR-4, IR-4(1), IR-4(11)  CMMC: IR.L2-3.6.1  PCI: 12.10.3 |
|  | Security incidents must be documented and tracked. | NISTCSF1: RS.AN-4  NISTCSF2: RS.MA-02, RS.MA-03, RS.AN-06  NIST800-171: 3.6.2  NIST800-53: IR-4, IR-4(1), IR-5, IR-5(1), IR-8  CMMC: IR.L2-3.6.2  SOC2: CC7.3, CC7.4  ISO27002: 5.24  HIPAA: §164.308(a)(6)(ii) |
|  | Security incidents must be classified according to potential impact. | NISTCSF1: DE.AE-4, RS.AN-2, RS.AN-4  NISTCSF2: DE.AE-04, RS.MA-02, RS.MA-03, RS.AN-08  NIST800-171: 3.6.1  NIST800-53: IR-4, IR-4(1), IR-8  CMMC: IR.L2-3.6.1  SOC2: CC7.3, CC7.4  ISO27002: 5.25  CIS: 17.9 |
|  | Create a security incident management plan that includes specific procedures for high-impact incident types. | NISTCSF1: PR.IP-9, RS.RP-1, RS.CO-1, RS.MI-1, RS.MI-2, RC.RP-1  NISTCSF2: ID.IM-04, RS.MA-01, RS.MA-05, RS.AN-03, RS.MI-01, RS.MI-02, RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-05, RC.RP-06  NIST800-171: 3.6.1  NIST800-53: IR-4, IR-4(4), IR-4(11), IR-8  CMMC: IR.L2-3.6.1  SOC2: CC7.4  ISO27002: 5.26  CIS: 17.4, 17.6  PCI: 12.10.1, 12.10.7  HIPAA: §164.308(a)(6)(i), §164.308(a)(6)(ii) |
|  | Develop a learning process for the information gained from security incidents. | NISTCSF1: DE.AE-2, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2  NISTCSF2: ID.IM-03, ID.IM-04  NIST800-53: IR-4, IR-4(4), IR-8  SOC2: CC7.5  ISO27002: 5.27  CIS: 17.8  PCI: 12.10.6 |
|  | Incidents must be reported to internal and external stakeholders as required. | NISTCSF1: DE.DP-4, RS.CO-2, RS.CO-3, RS.CO-5, RC.CO-3  NISTCSF2: DE.AE-06, RS.MA-04, RS.CO-02, RS.CO-03, RC.CO-03, RC.CO-04  NIST800-171: 3.6.2  NIST800-53: IR-4, IR-4(4), IR-6, IR-6(1), IR-6(3)  CMMC: IR.L2-3.6.2  SOC2: CC2.2, CC2.3, CC7.5  ISO27002: 5.5  CIS: 17.2, 17.3 |
|  | Security incident response capabilities must be tested periodically. | NISTCSF1: ID.SC-5, PR.IP-10  NISTCSF2: ID.IM-02  NIST800-171: 3.6.3  NIST800-53: IR-3, IR-3(2)  CMMC: IR.L2-3.6.3  SOC2: CC7.5  CIS: 17.7  PCI: 12.10.2 |
|  | Integrate security incident response with enterprise crisis management processes. | NISTCSF1: RS.RP-1, RS.CO-2, RS.CO-4, RC.CO-1, RC.CO-2  NISTCSF2: RS.MA-01, RS.MA-04, RC.CO-04  NIST800-171: 3.6.2  NIST800-53: IR-4, IR-4(4), IR-4(11), IR-8  CMMC: IR.L2-3.6.2  SOC2: CC7.4, CC7.5 |
|  | **Security e-Discovery and Forensics** | |
|  | Forensic investigations must be performed as part of security incident management. | NISTCSF1: RS.AN-3  NISTCSF2: RS.AN-07  ISO27002: 5.28 |
|  | Forensic evidence and e-discovery data must be collected and preserved as required. | NISTCSF1: RS.AN-3  NISTCSF2: RS.AN-07  ISO27002: 5.28 |

## Relevant Procedures

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is a best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

## Noncompliance

Clearly describe consequences (legal and/or disciplinary) for employee noncompliance with the policy. It may be pertinent to describe the escalation process for repeated noncompliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for noncompliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies.
2. Termination of employment.
3. Legal action according to applicable laws and contractual agreements.

## Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [name of policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.