# Security Incident Communications Policy Template

# How to Use This Policy Template

To use this policy 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 Title** | Name the formal title of the policy. |
| **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. |
| **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. |

# Supporting Documents

* Security Incident Communications Guidelines and Templates
* Information Security Incident Management Policy
* Incident Management Runbooks

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also, state the policy’s basic objectives.

This policy is to ensure that incident response communications, both internal and external, are drafted and delivered according to a formal process designed to maximize the efficiency and effectiveness of statements, memos, press releases, etc. made during the discovery and remediation of a security incident.

Security incidents are often chaotic, and they pose a significant risk to [Organization’s] reputation and client base. However, this policy is meant to provide stability by outlining regulatory obligations and their reporting procedure and by defining proper communications protocols for various groups, such as employees, external stakeholders, and the media.

# Scope

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

The Security Incident Response Team Policy applies to members of the Security Incident Response Team (SIRT). Because this policy contains sensitive information regarding incident handling and reporting, it shall not be distributed to all employees for review. Rather, this policy will be kept confidential and only shown to new persons or parties on a need-to-know basis.

# Audience

The SIRT shall contain the following members:

1. IT Advisor [e.g. CSO, CISO, or similar role]
2. IT Deputy [e.g. Senior IT professional]
3. Legal Counsel
4. HR Representative
5. Communications/PR Coordinator [e.g. Communications Director]
6. Communications/PR Deputy [e.g. Senior Communications Professional]

Roles can be added, subtracted, or modified as needed, but avoid having more than six to eight members to ensure decisions can be made in a timely fashion. The SIRT team should be assembled with an eye towards balancing senior leadership and people with hands-on experience – keep this information in mind when deciding who will be on your team. It is also a good idea to establish alternates for each role in case someone is unavailable during an incident or crisis.

# Definitions

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

**Information security event:** Identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, including false alarms.

**Information security incident:** Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Exactly what constitutes an event or incident will vary from organization to organization. Be sure to modify these definitions so that they agree with your organization’s threat escalation chart.

# 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 sub-sections may be required depending on the length or complexity of the policy.

**SIRT Communication Program**

* SIRT members shall provide primary and secondary contact information, so that they can be reached in the event that a security incident reaches [Tier-2] status, or stands to reach crisis status rapidly if not addressed immediately.
* If a primary SIRT member cannot be reached after [4] hours and the situation demands immediate attention that member’s alternate shall assume the required role for as long as necessary.
* SIRT members will report updates to each other via the interdepartmental communications template on an as-needed basis, but not less than once every [24 hours] until the incident is contained.
* SIRT members will establish a method of communication alternative to the primary method that is to be used in the event that the primary communication method is affected by, or is otherwise unavailable during, the security incident [e.g. alternate non-organizational email or instant messaging platform].
* All SIRT members will collaborate on all statements, memos, press releases, holding statements, etc. but the [IT Advisor] will have final authority to approve [Organization’s] message to ensure that providing such information will not further increase the severity or risk associated with the incident.
* In the event of a crisis with significant impact on external stakeholders, the SIRT will vote on whether [Organization’s] CEO needs to be included in decision making or needs to make a public statement.

**Communications Schedule and Sequence**

* As much as possible, incident response communications should be issued to affected stakeholders as the SIRT advances through the six remediation stages:
  + Detection
    - Communication 1 – holding statement
  + Analysis
    - Communication 2 – press release
  + Containment
    - Communication 3 – dark site
  + Eradication
    - Communication 4 – dark site update
  + Recovery
    - Communication 5 – press release or dark site update
  + Post-Incident Activities
    - Communication 6+ – appropriate statements, releases, or updates as needed.
* These communications should be modelled according to the examples provided in the Security Incident Communications Guidelines and Templates document.
* The above communication sequence is designed in the interest of transparency. However, the SIRT is permitted to alter this sequence if a majority of SIRT members agree that doing so is in the best interest of the remediation effort and/or [Organization].
* However, [Organization’s] Incident Management Runbooks prescribe communications at certain times during the remediation process, and the schedule contained therein is to be observed by the SIRT. Any deviations from the runbook’s communications schedule must be approved by both the Communications/PR Coordinator and the IT Advisor.

For more information on Incident Management Runbooks, see Info-Tech’s [*Develop and Implement a Security Incident Management Program*](https://www.infotech.com/research/ss/develop-and-implement-a-security-incident-management-program) blueprint.

**Internal and External Communications Protocol**

* In the interest of transparency and trust within the organization, affected parties (as necessary) will be provided with a memo outlining the basic details of each security incident (but not events) and its remediation once the incident is sufficiently contained. However, such memos will be released at the discretion of the SIRT, who may withhold such information if the incident is deemed insignificant, or if informing employees presents a **reasonable risk** to [Organization’s] security. If the risk level drops to a tolerable level, the SIRT will, if possible, issue a memo explaining the incident and why employees were not able to be immediately informed of the incident.
* External communications are to be supervised and coordinated by [Organization’s] spokesperson. The SIRT PR/Communications Coordinator will be responsible for this job unless another member is deemed more appropriate for a particular incident, such as a crisis requiring a public statement from the CEO.
* External communications are to be as honest and transparent as possible, but specific details will be issued on a need-to-know basis. External communications, such as press releases, holding statements, media interviews, etc., shall be crafted in a way that does not increase [Organization’s] security risks or legal exposure (e.g. statements shall not identify security vulnerabilities that have not yet been secured). **All SIRT members have a duty to ensure communications do not create additional security risks.**
* While investigation/remediation efforts are still on going, all written external communications shall include a date when the next update is expected. If an update cannot be released on the named date, the spokesperson will issue a revised timeline for the next update.
* SIRT members shall work to ensure that external communications contain only information that is known for certain in order to prevent having to change [Organization’s] message with each information update (i.e. external communications shall update the story as new information becomes available rather than change the story with each statement).

**Media Interactions**

* Unless otherwise stated, only the spokesperson will address the media.
* In the event that others need to speak to the media, guidelines for what can and cannot be stated must be provided not less than [72 hours] before the scheduled media interaction.
* In the interest of limiting the media’s requests to speak directly to general employees, the SIRT will work to ensure that a holding statement or press release is available to the public as soon as possible. Also, the spokesperson will make themselves available for interviews, etc. as a means to promote transparency and a positive corporate image. All statements shall be made with due diligence to honesty, transparency, respect, empathy, restoring public trust, and limiting reputational damage.

**Post-Incident Review**

* After all incidents requiring external communications, the SIRT will conduct a post-incident review in order to discuss what elements of the Security Incident Response Plan were well executed and what areas need to be improved or otherwise changed to promote the development of a more effective communications plan for future use.
* When appropriate, the SIRT will put together a report of the incident to be shared with industry peers as a means of increasing the all-around security within the industry and improving peer relations.

**Alignment of Communications and General Incident Response Policies**

* This incident response communications policy is to be used in conjunction with the Information Security Incident Management Policy, which outlines [Organization’s] incident-response procedures more generally.

# Exceptions

Define any exceptions to the above policy statements.

# Governing Laws and 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. Use this section to summarize the ways that each regulation or law may affect your organization’s communications effort.

[Organization] is required to comply with the following laws and regulations:

E.g. GDPR – supervisory agency must be notified of a data breach within 72 hours; stakeholders must also be informed in plain language without undue delay.

# Non-Compliance

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

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

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

### Relevant Procedures, Standards, Policies, and Processes

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is 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.

# 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 understood the Security Incident Response Team 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** | **Change** | **Author** | **Date of Change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

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.