

Computer Security Incident Response Plan Template – Short Version

A Guide for Developing an Incident Response Plan
and
Step-by-Step Instructions for Completing the Template
(Rev. 2016-May-03)

Disclaimer

The templates are not copyrighted and are to be made available free of charge to anyone who wants to use them, in their entirety or using any section or subsection, and without the need for any attribution as to the source. The templates are provided AS-IS, without any warranty of fitness for any particular purpose, business or industry, or of their applicability to any specific business circumstances. **Organizations are advised and strongly encouraged to consult and work with their legal counsel** (and Human Resources) on the completion of any policy or plan using the templates. **This template should not be taken or interpreted as providing any legal advice, and is no substitute for contacting appropriate legal counsel.** By using the template, you agree that the author/creator of the template shall not be held responsible for any damage or loss incurred as a result of reliance on the content of the template, and you agree to hold harmless and release from any liability the author/creator of the template.

Background and Purpose (1)

Ideally, a business should have a set of documents which define its purpose and mission, outline how it assesses and manages risks, and provide strategic goals and direction. Additional documents cover policies and procedures related to its business operations and should include technology and security. To maintain business functions during times of disasters or other emergencies, there should be a Disaster Recovery Plan (DRP) and a Business Continuity Plan (BCP), also called a Continuity of Operations Plan (COOP). These fall under the category of Operational Policies and Procedures.



© 2015 ABW Consulting Services. All Rights Reserved.

References (1)

- The following websites offer assistance for small businesses in creating a Business Plan and other start-up processes:
 - <https://www.sba.gov/category/navigation-structure/starting-managing-business/starting-business>
 - <https://www.sba.gov/offices/headquarters/oed>
 - <https://www.sba.gov/offices/headquarters/oeo>
 - <https://www.score.org/>
 - <https://www.ftc.gov/tips-advice/business-center>

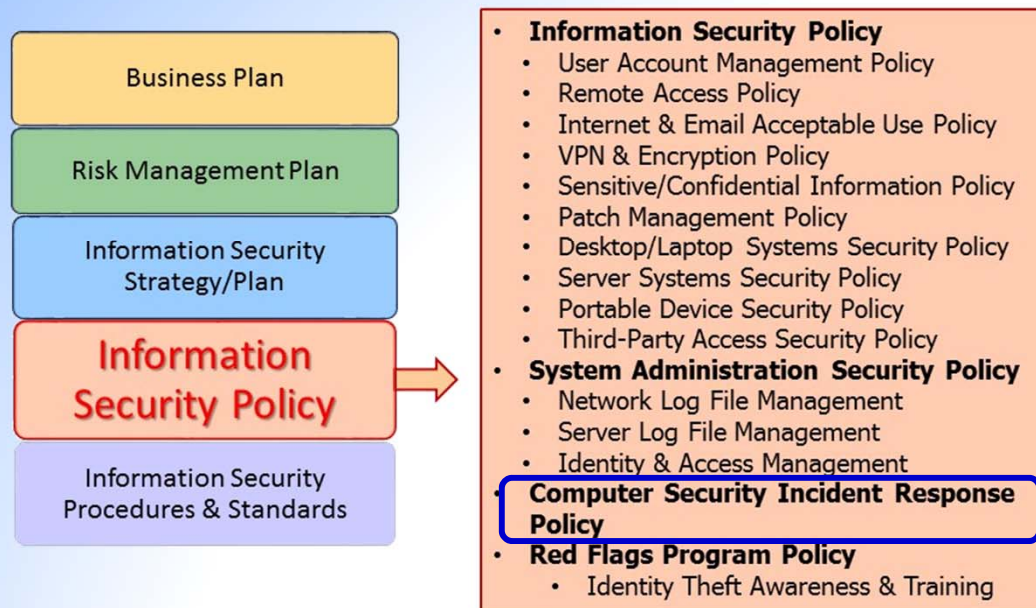
[Listing these resources is not an endorsement of their services or the information provided by them, these are simply free (government or government-sponsored) resources.]

Background and Purpose (2)

A Computer Security Incident Response Plan can be a separate document, often part of a larger Information Security Program, or it can be part of the Continuity of Operations Plan. For smaller businesses, it might be a simple reference document to be used when a computer security event has been discovered.

Regardless of how the plan fits into the business structure, its content and importance remain basically the same. The purpose is to help the business respond to and recover from a security incident, so it can return to normal business operations.

Typical Hierarchy of Documents
(Detail View - Policies)



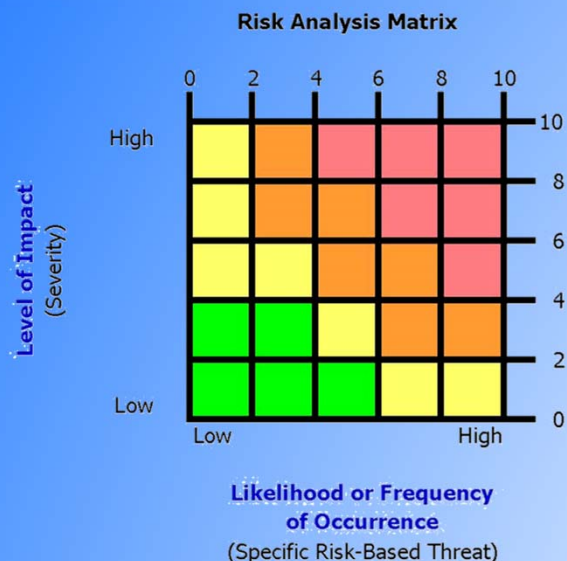
© 2015 ABW Consulting Services. All Rights Reserved.

References (2)

- The following websites offer information about information security for small/medium businesses, including some policies and procedures
 - <https://www.sba.gov/navigation-structure/cybersecurity>
 - <http://csrc.nist.gov/groups/SMA/sbc/>
 - <https://www.sans.org/security-resources/policies/>
 - <http://securingourecity.org/business>
 - <https://www.cisecurity.org/cyber-pledge/index.cfm>
 - <https://www.score.org/resources/how-choose-right-backup-system-your-small-business>
 - <http://www.bbb.org/council/for-businesses/cybersecurity/>
 - [http://securingourecity.org/wp-content/uploads/2015/12/Bringing IT Home Booklet 4th Edition web FINAL.pdf](http://securingourecity.org/wp-content/uploads/2015/12/Bringing_IT_Home_Booklet_4th_Edition_web_FINAL.pdf)

[Listing these resources is not an endorsement of their services or the information provided by them, these are simply free (government, government-sponsored or non-profit) resources.]

Background and Purpose (3)



Action Indicators:

1	Level 1 {High Risk} - requires immediate corrective action (security controls)
2	Level 2 {Med-High Risk} - requires corrective action with Management approval
3	Level 3 {Med-Low Risk} - requires Management review to accept or mitigate
4	Level 4 {Low Risk} - acceptable risk without further Management review

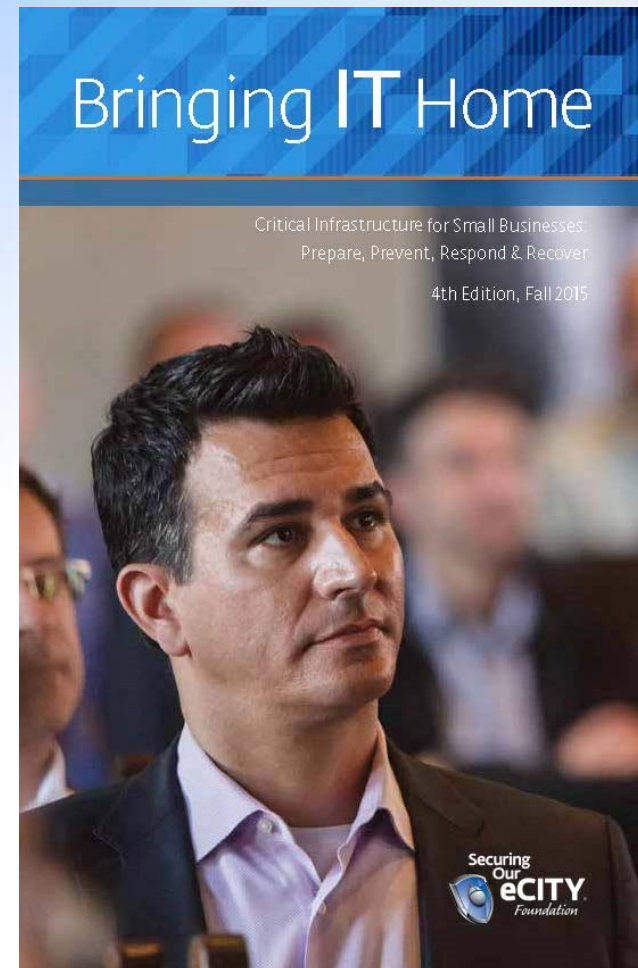
Part of the preparation steps, before creating a response or recovery plan, is to determine and document all of the business computer assets (don't forget your data) and then perform a business risk analysis for each asset (refer to pages 3-4 of the template). The business value of an asset is not only based on the cost of the hardware and software, it is mainly based on the importance of the data and information stored on the asset and the business impact of losing that asset. This chart is just an example risk matrix with four defined levels of risk (others use five levels). Depending on the risk tolerance of a business, the colored boxes may shift up/down or left/right, so that, for example, there are more High Risk boxes and fewer Low Risk, which would indicate lower risk tolerance. (Separate resources are available to guide you through a risk analysis process.)

Additional Considerations

- For both this Computer Security Incident Response Plan, and for a Disaster Recovery Plan or Business Continuity Plan, take into consideration:
 - Secondary and tertiary means of communications, when primary communications are not working
 - If the network is down, email won't work
 - Consider pagers, home & cell phones, text messaging, 2-way radios
 - Having the ability to notify employees to stay away from a worksite or to report to a worksite, as necessary
 - Procedures for checking on the safety and well-being of employees, and accounting for their location, during emergency situations
 - Create and post safety/security checklists covering different types of events – distribute to all employees
 - Emergency/Security team members could have a wallet-size card with contact positions (no names) and phone numbers
 - Plan for training employees on policies and procedures

Incident Planning - Prepare, Prevent, Respond, & Recover

This booklet is a free resource for small businesses. It covers the 16 critical infrastructure sectors; providing real-life scenarios related to cybersecurity incidents and how to prepare/prevent in advance, respond during, and recover afterward. There are lists of actions to take for each sector, as well as an overall checklist at the end for any business. Hard copies may be requested from Securing Our eCITY® Foundation by sending an email to Liz Fraumann at lfraumann@securingoureconomy.org; or you can access the online version at: <http://securingoureconomy.org/business> and scroll down to "Business Tips and Resources."



Background and Purpose (4)



Next, you can start preparing your Computer Security Incident Response Plan and Policy. The following instructions are for the “Condensed-Short Version” of the template, geared toward businesses with 25 or more employees, including some internal information technology (IT) support, and generally located in one facility/site. There is also a “Comprehensive Version” of the template for businesses with more than 250 employees.

Before starting on the template, you should have the following information available:

- IT staff by position/title with phone numbers and email addresses
- IT service providers with contact information (phone and email)
 - copy of service contract, especially any references to security incidents
- Company employees who will be on the incident response team (phone and email)
- Non-company representatives (e.g., service providers) to be on the response team
 - may require mutual Non-Disclosure Agreements (NDAs)

NOTE: The template was written for the San Diego (CA) region; other locations may need to change some of the references used in some sections in the template.

[YOUR COMPANY NAME]

> CONDENSED/SHORT VERSION - TEMPLATE <

<This version is more applicable to Small Organizations>

>> INSTRUCTIONS: Make modifications (additions, deletions or edits) to the template to fit your industry sector and to meet your specific business needs. Businesses are advised to consult with their legal counsel (and possibly Human Resources) when completing the information and before issuing a policy/plan. This template is not considered legal advice and should not be interpreted as such. Within the template, cyan-color highlighting indicates instructions; yellow-color highlighting indicates content that needs to be supplied by your company, in some places optional language/content is supplied and may need to be modified, in other places there is a 'placeholder' label. Delete any brackets where company content is added to replace the optional text or placeholders. Be sure to delete all the highlighted instructions before finalizing the document. <<

**COMPUTER SECURITY
INCIDENT RESPONSE PLAN**

Version # **[]**
[Current Revision Date]

Yellow highlighting indicates areas where you need to replace the 'placeholder' text with your own specific content (and remove the highlighting). You can perform a global "replace" text by finding "[Your Company Name]" (with the brackets, but without the quotation marks) and filling in your actual business name, to change it throughout the whole document.

Cyan (turquoise) highlighting indicates instructions, which should be deleted after completing the section where they apply.

You can also perform a global "replace" text for "#___" (using 3 underscores) and for "[Current Revision Date]" (without the quotation marks on both).

On this cover page, after removing the instructions, it is recommended that you align the title/heading a few lines below the company name, and align the version information near the bottom of the page/margin. (Refer to example on next slide.)

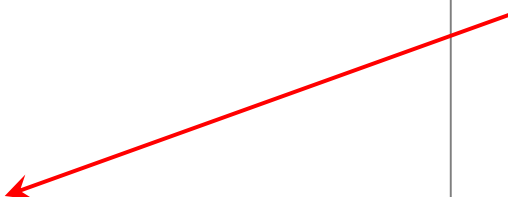
[YOUR COMPANY NAME]

**COMPUTER SECURITY
INCIDENT RESPONSE PLAN**

Version # **[]**
[Current Revision Date]

This is an example of the alignment for a completed cover page (of course, your own information would replace the yellow highlighted areas).

Add whatever additional information is relevant or typical for your business, such as a company logo (which could be placed in the center).



Document Revision History

Date	Version	Revision Comments	By
05/03/2016	0.6	Created Condensed/Shortened Template for Small & Medium Businesses	Author
mm/dd/yyyy	0.9	[Your Company Name] Issued Draft for Review	
mm/dd/yyyy	1.0	Approved Version Issued	

You can use a 'global replace' text for "[Current Version Date]" (with the brackets, but without the quotation marks) to change it throughout the whole document.

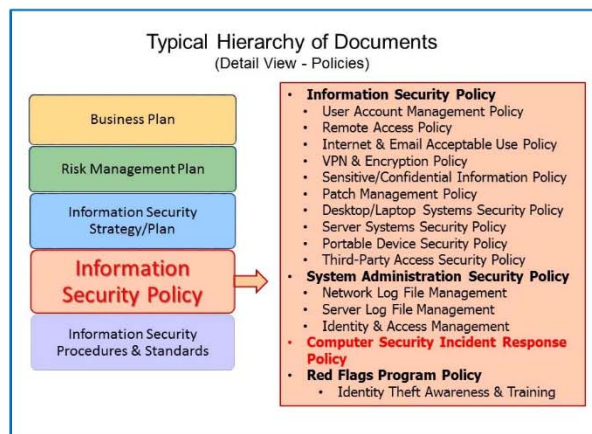
This "Document Revision History" table is intended to keep track of each version of the document and to briefly summarize changes that were made, the date, and by whom. The initial row (creation of the template) can be deleted, then you can start with your first draft version. Ideally, the first official version to be issued will be "1.0" (so prior draft versions would be 0.1, 0.2, 0.3, etc.).

The note (text box) at the bottom of the page can be deleted.

NOTE: This Computer Security Incident Response Policy & Plan template was created for the purpose of assisting Small/Medium Businesses (SMBs) in being better prepared for handling a cybersecurity incident, using current best practices. There are two templates – one comprehensive version for medium and larger businesses, and one short version for smaller businesses. The templates are a work-in-progress, and as changes are made, new versions of the templates will be released. The templates are not copyrighted and are to be made available free of charge to anyone who wants to use them, in their entirety or using any section or subsection, and without the need for any attribution as to the source. The templates are provided AS-IS, without any warranty of fitness for any particular purpose, business or industry, or of their applicability to any specific business circumstances. **Organizations are advised and strongly encouraged to consult and work with their legal counsel** (and Human Resources) **on the completion of any policy or plan using the templates. This template should not be taken or interpreted as providing any legal advice, and is no substitute for contacting appropriate legal counsel.**

PREFACE

While this document is being used as a stand-alone policy for [Your Company Name], larger organizations may consider this part of an overall Information Security Program, within a structure or hierarchy of business and information technology documents, as indicated below **for reference purposes only**.



This page is mostly informational and can be deleted, modified or moved to a different part of the document, as you see fit.

Table of Contents

Preface.....	ii
1. Statement of Management Commitment	1
1.1. Mission & Goals for Incident Response	1
1.2. Senior Management Approval of Plan	1
2. Policy	2
3. Purpose & Objectives of the Plan	2
4. Scope of the Plan.....	3
5. Definitions of Computer Security Incidents and Related Items	3
5.1. Category Definitions for Priority and Severity Ratings of Incidents.....	3
5.1.1. Business Risk Assessment of Information Assets	3
5.1.2. Incident Response Levels	4
6. Creation of Computer Security Incident Response Team.....	4
7. Roles & Responsibilities	6
8. CSIRT Communications	6
8.1. Reporting requirements.....	6
8.2. Guidelines for External Information Sharing.....	6
9. Incident Response and Incident Management Lifecycle Overview.....	8
9.1. Evidence Retention	8
10. References	9
Appendix A	A-1
Definitions of Terms, Abbreviations, and Acronyms.....	A-1
Appendix B	B-1
NIST Incident Handling Checklist.....	B-1
Appendix C	C-1
Sample - Detailed Incident Handling Form	C-1
Appendix D.....	D-1
CSIRT Points of Contact List.....	D-1

After finalizing the full document, come back to this page and re-generate the Table of Contents, so all of the section headings and page numbers show up correctly. If there are problems with section numbering, those will have to be corrected within the document first, then generate a new Table of Contents.

For the Appendices, they will all show as starting on page "1," and you will need to manually edit each one to insert the appropriate Appendix prefix with a hyphen ("A-", "B-", "C-", and "D-").

COMPUTER SECURITY INCIDENT RESPONSE PLAN

1. Statement of Management Commitment

By the approval and adoption of this Computer Security Incident Response Plan (the "Plan"), the [Your Company Name] management have declared their commitment to this critical policy and its importance in the protection of company Information Assets. This Plan is considered critical for the company's overall business risk management, to help mitigate risks where possible, and to quickly recover business operations after a computer security incident.

1.1. Mission & Goals for Incident Response

The mission of this Plan is to minimize business impacts caused by computer security incidents, by optimizing the incident response actions to be both effective and efficient.

The goals for this Plan are {{**Examples:** (1) to identify and train an adequate number of staff from different functional areas to allow for overlapping coverage (a primary and a backup) as members of the CSIRT, (2) to effectively utilize the procedures and processes in this Plan to mitigate business impacts during actual computer security incidents, (3) to assist with conducting drills or assessments to test company incident response capabilities, and (4) to provide valuable feedback into updating Information Security policies, procedures or mechanisms, as a result of the lessons learned after an incident.}}

1.2. Senior Management Approval of Plan

Through the standard process for approval of company operational policies, the [Chief Executive Officer / Company Management Team] has approved this Plan, effective on [Date], including the creation of a Computer Security Incident Response Team with its defined responsibilities.

Signed: _____

Name (Printed): _____

Title: _____

The purpose of this first section (#1) is to have management affirm their support and commitment to protecting the company's information assets (data) by implementing this Plan and to inform employees of the goals for this Plan.

Four example goals are provided in the yellow highlight, and can be used as-is or with minor changes to meet the business requirements, or they can serve as general reference while the company inserts your own specific goals for this Plan. You should keep the number of goals to four or less.

The last section should be filled in with the title of whoever is approving this Plan document and the date it is approved; then it should be signed. This person needs to be the top leader of the company (i.e., CEO, President or Owner).

2. Policy

It is the policy of [Your Company Name], that all computer security incidents be addressed, as promptly as possible, using consistent methods to minimize business impacts and potential damage to company Information Assets. As part of this policy, [Your Company Name] will implement a basic Computer Security Incident Response Program to help mitigate the risks from computer security incidents, by defining standard operating procedures for effectively and efficiently responding to incidents.

3. Purpose & Objectives of the Plan

This Plan not only establishes an incident response program, but a primary purpose of the document is defining procedures for detecting, analyzing, prioritizing, and handling computer security incidents to minimize business impacts.

This Plan is based on national standards issued by the National Institute of Standards & Technology (NIST), along with national best practices from the Software Engineering Institute (CERT Coordination Center) at Carnegie Mellon University, using the following published documents for guidance:

- NIST Information Technology Laboratory (ITL) Bulletin, September 2012, **Handling Security-Related Incidents** (overview of NIST Special Publication 800-61, Rev. 2)
 - http://csrc.nist.gov/publications/nistbul/itlbul2012_09.pdf
- NIST Special Publication SP-800-37, Rev. 1, **Guide for Applying the Risk Management Framework to Federal Information Systems**
 - <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>
- NIST Special Publication SP-800-61, Rev. 2, **Computer Security Incident Handling Guide**
 - <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- NIST Special Publication SP-800-83, Rev. 1, **Guide to Malware Incident Prevention and Handling for Desktops and Laptops**
 - <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf>
- NIST Special Publication SP-800-86, **Guide to Integrating Forensic Techniques into Incident Response**
 - <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
- NIST Special Publication SP-800-92, **Guide to Computer Security Log Management**
 - <http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>
- NIST Special Publication SP-800-94, **Guide to Intrusion Detection and Prevention Systems (IDS/IPS)**
 - <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

This section (#2) provides a brief policy statement. Although not highlighted, your company may want to change some of this content or add to it.

The next section (#3) states the general purpose of the Plan and provides a list of national standards from NIST (continued on the following page), which serve as background and supporting references with more specific details related to incident response and computer security. It is recommended that this section be left as-is.

- NIST Special Publication SP-800-128, **Guide for Security-Focused Configuration Management of Information Systems**
 - <http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf>
- NIST Special Publication SP-800-137, **Information Security Continuous Monitoring (ISCM)**
 - <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>
- NIST Special Publication SP-800-150 (Draft), **Guide to Cyber Threat Information Sharing (Draft)**
- Software Engineering Institute, CERT Program, Carnegie-Mellon University, **"Incident Management Capability Metrics Version 0.1"**, April 2007
 - <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8379>

These documents provide valuable resources for management to identify best practices for risk management and incident response, and for Incident Response Team members to learn about different aspects of security protective and responsive measures.

4. Scope of the Plan

This Plan applies to:

- All company IT Resources and Information Assets, regardless of whether they are located within company facilities or in third party service provider facilities, and whether they are managed by company staff or by third party service providers on behalf of [Your Company Name];
- All Individuals or Users who are authorized to access company IT Resources and Network Services; and
- All Computer Security Incidents (also referred to as "Cyber Security Incidents") which may occur, involving company IT Resources or Information Assets.

5. Definitions of Computer Security Incidents and Related Items

General definitions of terms, abbreviations, and acronyms used in this Plan are contained in Appendix A.

5.1. Category Definitions for Priority and Severity Ratings of Incidents

5.1.1. Business Risk Assessment of Information Assets

Generally, each Information Asset should be rated for its importance to the business and the impact that would result if the asset were compromised; for

This next section (#4) may be modified, as deemed necessary; however, it is recommended that the scope of the Plan cover all "Information Assets" (generally the hardware and, more importantly, the data), no matter where it is located, all "IT Resources" (generally the software and network infrastructure) which are owned by the company, and all users (whether employees, vendors, partners, or others) who have access to the company's Information Assets. To help ensure the success of the Plan, it needs to be coordinated with the company's ISP and any other IT service providers. This is one area where the company should consult with legal counsel.

The following section (#5) is intended to provide general direction for setting a risk value for Information Assets, in order to determine a proper response.

example, using a scale of “1” being low impact, up to “10” being very high impact. Examples of high business impacts include loss of revenue, customers’ inability to transact business, damage to company reputation or image, physical damage to property, and loss/theft of confidential or proprietary information.

5.1.2. Incident Response Levels

There are four (4) priority levels for security incidents, based on the degree of business criticality and importance to [Your Company Name] for the related information systems or data. These priority levels roughly coincide with the business risk ratings indicated above and are defined as follows:

- **Priority #1 - Emergency/Urgent:** An Incident has caused a complete and immediate work stoppage affecting at least one primary business process or a broad group of End Users (such as an entire department, building, floor, branch, line of business or external customer). No workaround is available.
- **Priority #2 - High:** An Incident has affected a business process in such a way that business functions (operations) are severely degraded, multiple End Users are impacted or key external customer is affected. A workaround may be available, but it is not easily sustainable.
- **Priority #3 - Medium:** An Incident has affected a business process in such a way that certain business functions are not available to End Users or external customers, or a system or service is degraded. A workaround may be available.
- **Priority #4 - Low:** An Incident has little or no effect on business processes or operations and can be handled on a scheduled basis (e.g., preventive maintenance). A workaround is available.

6. Creation of Computer Security Incident Response Team

It is the intent of [Your Company Name] executive leadership to use internal resources, as much as possible, in the creation of a Computer Security Incident Response Team (CSIRT). {{ **Optional, if applicable:** Leadership also took into account the company’s dependence on external IT contractors for several critical services which are integral parts of the company’s overall IT environment. As such, the CSIRT necessarily includes key members from external service providers to work alongside company staff, to create a hybrid CSIRT. }} If possible, one primary member and one alternate member will be identified from each functional business area, to allow for backup coverage on

After defining risk levels for each asset, this section (#5.1.2) provides the definitions for levels of response to a particular incident, based on business impacts. While these definitions may be modified as needed to meet a company’s particular requirements, it is strongly recommended to leave them as-is, since they are based on best practices and NIST standards.

The next section (#6) (continued on the next two pages) is where the company defines the composition of the Computer Security Incident Response Team (aka “CSIRT”). This should be based on staff **positions**, not by employee names (although the names will be part of the contact list). When including the company’s ISP or other IT service providers, you will want to include the optional sentences within the highlighted areas (modified, as needed).

the CSIRT in case one of the members is not available. Both the primary and alternate CSIRT members should receive the same level of training in Incident Response procedures. Because CSIRT members will potentially have access to system-level data and information, which may include Sensitive or Confidential Information (such as, handling a breach where personal information has been exposed), each CSIRT member must be cleared through a background check process that would permit them that level of access.

The CSIRT should consist of the following individuals or representatives from the functional business areas (which may include external IT service providers):

- [Chief Information Security Officer (CISO) or equivalent IT Security Manager]
- [Information Security Team]
- [Internet Services Provider (ISP) – point of contact]
- {{If applicable: Network Operations}}
- {{If applicable: Data Center Operations}}
- {{If applicable: Website Management}}
- {{If applicable: Database Administration}}
- {{If applicable: Managed Security Services Provider (MSSP)}}
- {{If applicable: Cloud Services Provider}}

The following functional contacts should be used to address issues or concerns related to employees or potential liability matters resulting from a security incident, and to facilitate proper legal processes if matters need to be referred to law enforcement.

- Executive Management
- Human Resources
- Legal Counsel (company attorneys)
- Cybersecurity Insurance Carrier/Provider

Once the CSIRT members have been identified, a contact list (refer to Appendix D) should be created and distributed to each team member, as well as to management. In addition, the CISO {{or equivalent position}} should also develop liaison contacts with local law enforcement agencies, such as the Law Enforcement Coordination Center (aka Fusion Center), especially their computer crime units, and/or with the nearest FBI field office's Cyber Squad.

To continue defining the CSIRT, this list should include the key positions who are responsible for operations or security of the company's computer systems and networks. The actual number of team members and their titles will depend on the size of the company and its IT staff. In many cases, for small businesses, there is no dedicated IT staff and services are provided either on an ad hoc basis by company employees (sometimes supervisors, managers or even the owner), or else by a contracted IT service provider. In this circumstance, the company should still have a Plan, but coordinate with the service providers – and make a contractual agreement on the Plan, with key emphasis on roles and responsibilities (refer to the next page). Whether the service providers participate in your Plan, the company should require the providers to disclose their plans and procedures for incident response.

7. Roles & Responsibilities

The CISO {{or equivalent position}} shall have the lead role in Computer Security Incident Management and Response for [Your Company Name], and shall manage the CSIRT. The CISO should develop the internal CSIRT operating procedures and should coordinate development of inter-organization procedures with the company's third party IT service providers {{, including the cybersecurity insurance provider}}.

Through the approval and adoption of this Plan, the CISO {{or equivalent position}} is granted the authority to take any necessary actions in regards to security incident response and recovery, to minimize impacts and damage to company IT Resources or Information Assets.

8. CSIRT Communications

8.1. Reporting requirements

[Your Company Name] must comply with all reporting and notification requirements pursuant to applicable state and federal laws, particularly involving breaches with the potential loss or exposure of confidential, personal information. The CISO or designee is responsible for ensuring proper reporting and notifications are accomplished. Examples of applicable regulations include California Civil Code §1798-§1798.78 (Information Practices Act of 1977), as amended (for example, by SB 1836 or the Security Breach Information Act of 2003), or the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended. The company shall maintain a list of all applicable state and federal regulations regarding the reporting (to a regulatory agency) and notification (to consumers or customers/clients) for discovered data breaches.

In addition to mandated reporting or notification requirements, the CSIRT (either through the CISO or another designated CSIRT member) should be providing information regarding an active incident to appropriate internal stakeholders, including third party IT service providers who support and maintain company's IT infrastructure and systems, as applicable and appropriate. At a minimum, the CISO should provide regular status updates to company management during the incident handling phases, as well as providing a final incident report.

8.2. Guidelines for External Information Sharing

[Your Company Name] may decide to proactively share relevant incident indicator information with peers to improve detection and analysis of incidents. This may occur through the IT-ISAC or some other security group, such as the FBI-sponsored InfraGard Members Alliance or an industry-specific professional association. Before an incident occurs, the CSIRT should discuss information sharing parameters with

This section (#7) should be modified and even expanded to include all of the relevant CSIRT positions; although, they may be contained in a separate procedural document. The intent is to also cover roles and responsibilities of other functions beyond the CSIRT members (for example, legal counsel, human resources, insurance provider, etc.). It is recommended that provisions be made for alternate staff to take on certain roles, in the absence of the primary CSIRT members. [NOTE – a future release of this template will include a RACI chart to display roles and responsibilities.]

The next section (#8) basically states that the company will comply with legal reporting or disclosure requirements. Depending on the type of data the company collects, maintains or uses in transactions, this section may be modified with the specific regulatory information. Additional information sharing is encouraged, but at the discretion of the company.

company's Legal Department, {{if applicable: cybersecurity insurance provider,}} and management to establish clear procedures and priorities regarding information sharing. CSIRT members, or anyone else sharing incident information must ensure that only authorized information is released and that anyone receiving confidential or sensitive incident information has been appropriately authorized to have it (as evidenced by a non-disclosure agreement (NDA)). The CSIRT should document all contacts and communications with external parties for liability and evidentiary purposes.

Law Enforcement – One reason that many security-related incidents do not result in convictions is that some organizations do not properly contact law enforcement. [Your Company Name] should consider contacting the local municipal police, county Sheriff, county District Attorney, state Attorney General, state Office of Information Security, Federal Bureau of Investigation (FBI) local field office, and U.S. Attorney General. Some jurisdictions have integrated, joint law enforcement teams to help combat cybercrime in their region; for example, the San Diego Law Enforcement Coordination Center (LECC). The CSIRT members should become acquainted with these agencies, before an incident occurs, to discuss conditions under which incidents should be reported to them, how the reporting should be performed, what evidence should be collected, how it should be collected, and when and how it should be transferred. The CISO {{or equivalent position}} will be the primary contact with law enforcement, consistent with the requirements of the law and the company's procedures. The CSIRT should understand what the potential jurisdictional issues are (e.g., physical location – [Your Company Name] headquarters being located in [State (e.g., California)] may have IT Resources located in another state, attacked from a system in a third state, being used remotely by an attacker in some other location). [Some content in this section taken from NIST SP-800-61, Rev-2, Aug. 2012, p. 11]

For any external information sharing related to security incidents, you should consult with your legal counsel. During the creation of this Plan/Policy, you should get input from legal counsel on what should be included or excluded from this section.

Keep in mind that almost all cyber attacks are criminal acts and should involve an investigation by the appropriate law enforcement agency. You can notify them and share non-proprietary information with them to help with an investigation; however, a key point to remember when the CSIRT is in the Response mode of an incident, is the preservation of evidence and maintaining a tight chain of custody (refer to the next page). The CISO or equivalent manager should contact your local law enforcement agency to find out how they want to handle such incidents, and to get the necessary contact information for when an incident occurs.

9. Incident Response and Incident Management Lifecycle Overview

NIST standards outline four major phases of an Incident Management Lifecycle – (1) Preparation, (2) Detection & Analysis, (3) Containment, Eradication, & Recovery, and (4) Post-Incident Activity (see Figure 1). If CSIRT members want more information, these phases are described in detail in NIST Special Publication SP-800-61, Rev. 2, while a sample of the NIST Incident Handling Checklist is provided in Appendix B. To assist the CSIRT in documenting an incident, a detailed Incident Handling Response Form is provided in Appendix C.

9.1. Evidence Retention

The CISO and CSIRT should follow established [Your Company Name] policies and procedures for the collection and retention of evidence, as they apply to computer security incidents, based on requirements defined by [company legal counsel] or pursuant to state or federal law. Retention may last for several months to years. Factors that need to be considered when determining the retention period for particular computer incident evidence include criminal prosecution efforts, civil case actions, general data or records retention requirements, and costs for hardware (e.g., computer devices, hard drives, or removable media) and storage facilities.

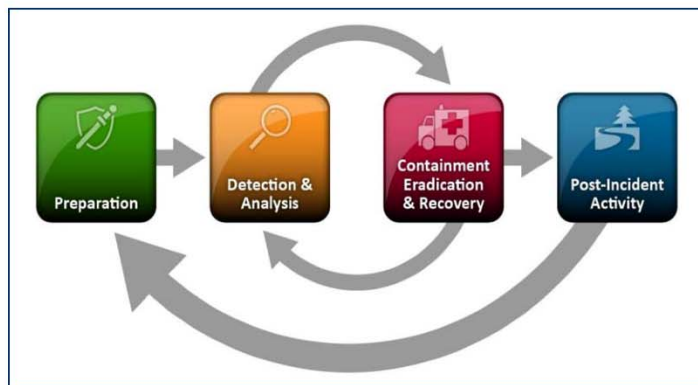


Figure 1 - Incident Response Lifecycle
[NIST SP-800-61 Rev-2, Aug. 2012, p. 21]

This section (#9) provides a brief overview of what is fully described in detail in the NIST publication, SP-800-61 Rev. 2, covering Incident Response Management. It is recommended that the company download the NIST document for further reference. One main theme of the national standard and best practices, is that incident response is an ongoing process of improvement, by learning from review of actual incidents (lessons learned) and applying those to making changes to policies and procedures.

The company may choose to expand this section with basic information from each of the four phases in the Incident Response Lifecycle.

[Note – the “Comprehensive” version of this template includes an already expanded section that can be used as reference.]

10. References

The following organization web sites and resource document links are provided as reference information, in addition to the NIST & SEI/CERT documents listed in Section 3 above, on the topic of computer security-related Incident Management and its components. These sources may benefit CSIRT members in learning more about their roles and responsibilities, and provide managers and executives a better understanding of the interconnected relationships between business risk, information security, and incident management.

Organizations:

- U.S. Department of Homeland Security, National Cyber Security Division, U.S. Computer Emergency Readiness Team (US-CERT)
 - <https://www.us-cert.gov/>
- CERT Coordination Center, Carnegie Mellon University
 - <http://www.cert.org/incident-management/>
- National Institute of Standards & Technology (NIST), Computer Security Resource Center
 - <http://csrc.nist.gov/>
- Information Systems Audit and Control Association (ISACA)
 - <https://www.isaca.org/>
- ISACA – San Diego Chapter
 - <http://isaca-sd.org/>
- Center for Internet Security, Multi-State Information Sharing & Analysis Center (MS-ISAC)
 - <http://msisac.cisecurity.org/>
- InfraGard San Diego Members Alliance
 - <http://www.infragardsd.org/>
- InfraGard National Members Alliance
 - <http://infragardmembers.org/>
- Securing Our eCity Foundation
 - <http://infragardmembers.org/>
- Information Systems Security Association (ISSA)
 - <https://www.issa.org/>
- ISSA – San Diego Chapter
 - <http://www.sdissa.org/>
- San Diego County Office of Emergency Services (OES)
 - <http://www.sandiegocounty.gov/content/sdc/oes.html>
- San Diego County Emergency Site
 - <http://sdcountyemergency.com/>

This page and the following one include reference websites for organizations involved in computer security incident response and other websites for obtaining documents related to incident management.

If the company has other places or contacts with government or private sector organizations that can assist with incident response, you should add them to these lists. Examples would include trade or professional associations or specific IT service providers.

Incident Management Documents:

- *Action List for Developing a Computer Security Incident Response Team*, August 2014, CERT/CC
 - <http://www.cert.org/incident-management/csirt-development/action-list.cfm>
- *Combating the Insider Threat*, May 2014, US-CERT
 - https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf
- *Creating a Computer Security Incident Response Team: A Process for Getting Started*, August 2014, CERT/CC
 - <http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm>
- *Defining Incident Management Processes for CSIRTs: A Work in Progress*, October 2004, SEI
 - http://resources.sei.cmu.edu/asset_files/TechnicalReport/2004_005_001_14405.pdf
- *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd Edition, April 2003, SEI
 - http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf
- *Incident Management* (Whitepaper), December 2005, CERT/CC
 - http://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_295923.pdf
- *Malware Threats and Mitigation Strategies*, May 2005, US-CERT & MS-ISAC
 - <https://www.us-cert.gov/sites/default/files/publications/malware-threats-mitigation.pdf>
- *Staffing Your Computer Security Incident Response Team – What Basic Skills are Needed?*, August 2014, CERT/CC
 - <http://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm>

[Remainder of Page Intentionally Left Blank]

APPENDIX A

DEFINITIONS OF TERMS, ABBREVIATIONS, AND ACRONYMS

Terms, phrases, abbreviations, and acronyms used in this document are intended to be interpreted as defined below.

"Breach" – means unauthorized access to company's Computer Equipment, Computer Systems, Email, or Network Services was, or is reasonably believed to have been, acquired or attained by an unauthorized person.

"CND" – Computer Network Defense, including the devices, systems, and processes to protect an organization's network, using a defense-in-depth approach with layers of security measures and mechanisms. [SEI CERT/CC, "Incident Management Capability Metrics Version 0.1", April 2007, pp. 135 & 215]

"CSIRT" – Computer Security Incident Response Team, as further defined below in this Plan.

"CSM" ["Continuous Security Monitoring"] – also called "information security continuous monitoring" (previously known as "security continuous monitoring"), is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. 'Continuous,' used in this context, means regular and routine monitoring, sometimes on an hourly basis, as necessary to promptly analyze alerts or alarms from computer security devices to determine their validity, and 'Ongoing,' used in this context, means that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organizational information. [NIST SP-800-137, Sept. 2011, p. 1]

"Event" ["Information Security Event"] – a single occurrence identified in a computer or network system that indicates an attempted or actual breach of information security policies or failure of security mechanisms.

- An *event* is any observable occurrence in a system or network. Events include, but are not necessarily limited to, a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. [NIST SP-800-61, Rev-2, p. 6]
- *Adverse events* are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This Computer Security Incident Response Plan addresses only adverse events that

The definitions in **Appendix A** are generally accepted as part of incident response management or for cybersecurity, and mostly come from the NIST standards. The company should add any other specific terms, abbreviations or acronyms you have added to this Plan or which apply to your specific industry sector.

are computer security-related, not those caused by natural disasters, power failures, acts of terrorism (e.g., bombings), etc. [NIST SP-800-61, Rev-2, p. 6]

“IDS” and “IPS” – Intrusion Detection Systems and Intrusion Prevention Systems include hardware devices and software products designed to monitor network and host activity based on either a database of known malware signatures or by using anomaly detection methods to evaluate real-time activity against a baseline of expected, normal activity. An IDS will log suspicious activity, send alerts or notifications to security staff, and has the ability to integrate with firewalls and routers to block potential malware or intrusions. An IPS performs the same functions as an IDS; however, it can also take its own protective actions to block potential attacks. IDS and IPS can be either host-based (monitoring a particular server or network device) or network-based (monitoring traffic on a particular network segment).

“ISCM” [“Information Security Continuous Monitoring”] - is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. This necessitates: (1) Maintaining situational awareness of all systems across the organization; (2) Maintaining an understanding of threats and threat activities; (3) Assessing all security controls; (4) Collecting, correlating, and analyzing security-related information; (5) Providing actionable communication of security status across all tiers of the organization; and (6) Active management of risk by organizational officials. [NIST SP-800-137, Sept. 2011, p. 1]

“Incident” [“Computer Security Incident”] – the occurrence of a single or series of information security events having a high probability of threatening the information security infrastructure and compromising business operations. Further, a *computer security incident* is considered a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash;
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host; and
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services. [NIST SP-800-61, Rev-2, p. 6]

“Individual” – includes any person who is a [Your Company Name] employee, volunteer or agent (i.e., contractor, vendor, etc.), granted access and using some or all of company’s IT Resources.

"Information Assets" – includes information or data relating to the conduct of the public's business which is prepared, owned, used or retained by [Your Company Name] regardless of physical form or characteristics, including, but not limited to paper, microfilm, microfiche, or any analog or digital format, whether located on internal company Computer Systems or on external systems owned or managed by third party service providers under contract and on behalf of [Your Company Name].

"IT Resources" – means all IT resources owned or leased by [Your Company Name] and any company-paid IT accounts, subscriptions or other technology services. This includes office telephones, wireless/cellular telephones, smart phones, desktop and portable computer systems, printers, facsimile (fax) machines, Internet and World Wide Web (Web) access, internal and external Email, electronic bulletin boards or newsgroups, file transfer protocol (FTP), other wireless systems, and emerging communications systems or devices when implemented by [Your Company Name].

"NIST" – National Institute of Standards & Technology; the organization within the U.S. Department of Commerce responsible for developing and issuing national standards in the area of computer technologies, among other fields; specifically those from their Computer Security Resource Center (<http://csrc.nist.gov/>).

"Security mechanisms" – layers of business processes and roles within [Your Company Name] that have input into the best security practices, procedures and controls, including the use of security technologies, to ensure the desired security of company's assets.

"SIEM" – Security Information & Event Management [system] includes hardware or software products used for security monitoring, alerting, and notifications. A SIEM usually gathers and aggregates data from all security sensors across network segments or an entire network, including host devices (e.g., servers), to give security staff a broad view (enterprise-wide) of any potential security incidents.

"User" – any Individual who has been granted privileges and access to [Your Company Name] Computer Equipment, Network Services, applications, resources, or information. User is also any person who is identified in the company Information Security Plan.

APPENDIX B

NIST INCIDENT HANDLING CHECKLIST

Ref #	Actions	Date Completed	Responsible Party
Detection & Analysis			
1.	Determine whether an incident has occurred		
1.1	Analyze the precursors and indicators		
1.2	Look for correlating information		
1.3	Perform research (e.g., search engines, knowledge base)		
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence		
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)		
3.	Report the incident to the appropriate internal personnel and external organizations		
Containment, Eradication, & Recovery			
4.	Acquire, preserve, secure, and document evidence		
5.	Contain the incident		
6.	Eradicate the incident		
6.1	Identify and mitigate all vulnerabilities that were exploited		
6.2	Remove malware, inappropriate materials, and other components		
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them		
7.	Recover from the incident		
7.1	Return affected systems to an operationally ready state		
7.2	Confirm that the affected systems are functioning normally		

The brief, 2-page checklist in **Appendix B** was taken from the NIST Incident Response document and modified slightly, by adding the two columns on the right, for tracking and accountability purposes.

This checklist provides a very basic set of steps and actions; however, there are more detailed steps that should be taken and documented, which are described in the NIST standard. This checklist might be appropriate as a guideline to ensure primary actions are identified. The more complete checklist in the next Appendix is more appropriate for actual incident response situations.

Ref #	Actions	Date Completed	Responsible Party
7.3	If necessary, implement additional monitoring to look for future related activity		
Post-Incident Activity			
8.	Create a follow-up report		
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)		

[Derived from NIST SP-800-61, Rev-2, Aug. 2012, p. 42]

APPENDIX C

SAMPLE - DETAILED INCIDENT HANDLING FORM

The following report form contains the types of information and incident details that will be used to track and report security incidents for [Your Company Name]. The format of this report is subject to change as reporting standards and capabilities are further developed.

Date/Time of Report: _____

Page ____ of ____

Incident Contact Information			
Last Name		First Name	
Job Title			
Primary Phone		Alternate Phone	
Mobile Phone		FAX	
Primary Email			
Alternate Email			

Incident Description			
Incident Date, Time, & Recovery Information			
Date/Time of First Event	Date		Time
Date/Time Incident Detected	Date		Time
Has Incident Ended?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Duration of Incident, as of this Report (in hours)			
Estimated Severity of Incident	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
Estimated Recovery Time, as of this Report (in clock hours)		Estimated Recovery Time, as of this Report (in staff hours)	
Estimated Damages (\$\$\$ Loss), as of this Report		Number of Host Systems Affected	
Number of Endpoint Systems Affected		Number of User Accounts Affected	
Type of Incident Detected			
<input type="checkbox"/> Exposing Confidential/Classified/Sensitive Information		<input type="checkbox"/> Theft of IT Resources / Other Assets	
<input type="checkbox"/> Creating User/System Accounts		<input type="checkbox"/> Altering Data (DNS / Website / Logs)	
<input type="checkbox"/> Destroying Data		<input type="checkbox"/> Anonymous FTP Abuse	
<input type="checkbox"/> Denial of Service / Distributed Denial of Service Attack		<input type="checkbox"/> Credit/Debit Card Fraud	
<input type="checkbox"/> Unauthorized Use/Access		<input type="checkbox"/> Other Fraud	
<input type="checkbox"/> Using Company Computer Illegally		<input type="checkbox"/> Attacking the Internet	
<input type="checkbox"/> Attacking Attackers / Other Sites		<input type="checkbox"/> Password Cracking	

This **Appendix C** provides a detailed information form for incident response handling. If the company has any specific information it wants to capture for an incident, you should add a new section for it, or expand an existing section, as applicable.

Depending on the nature and scope of an incident, some of the boxes will be left blank and the person completing the form can indicate "n/a" in those areas; otherwise, as much information as possible should be completed while the incident response is in progress.

Some of the information (on later pages) may not be known right away, some may require a more detailed analysis or root cause analysis, and some may need a forensic analysis, before the details are known.

Keep in mind that some security incidents are discovered days, weeks or even months after they originally began; so, document as much as is known at the time of discovery.

Incident Description			
<input type="checkbox"/> Impersonation <input type="checkbox"/> Increasing Notoriety of Attacker <input type="checkbox"/> Life-Threatening Activity <input type="checkbox"/> Other (Specify): _____	<input type="checkbox"/> Network/System Sniffer <input type="checkbox"/> Installing Malware (Virus / Trojan / etc.) <input type="checkbox"/> Unknown		
SB1386 – Is Email Notification Required?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
SB1386 – Email Notification Sent Out?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Law Enforcement Notified?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
Comments (Specify Incident Details and any additional, relevant information)			

General Incident Information	
How did You Initially Become Aware of the Incident?	
<input type="checkbox"/> Automated Software Notification <input type="checkbox"/> Manual Review of Log Files <input type="checkbox"/> Third Party Notification <input type="checkbox"/> Other (Specify): _____	<input type="checkbox"/> Automated Review of Log Files <input type="checkbox"/> System Anomaly (i.e., crashes, slowness) <input type="checkbox"/> Unknown
Attack Technique (Vulnerability Exploited / Exploit Used)	
<input type="checkbox"/> Malware (Virus, Worm, Trojan Horse) <input type="checkbox"/> Scanning / Probing <input type="checkbox"/> Unauthorized Access to Affected Computer System(s) Privileged User Compromise (Root/Admin Access) / User Account Compromise / Web Server Compromise <input type="checkbox"/> Other (Specify): _____	<input type="checkbox"/> Denial of Service / Distributed Denial of Service <input type="checkbox"/> CVE / CERT-VU / BugTraq # _____
Suspected Perpetrator(s) or Possible Motivation(s) of Attack	
<input type="checkbox"/> Current Employee / Contractor <input type="checkbox"/> Third Party Vendor/Supplier <input type="checkbox"/> External Party (outside of U.S.) <input type="checkbox"/> Other (Specify): _____	<input type="checkbox"/> Former Employee / Contractor <input type="checkbox"/> External Party (within U.S.) <input type="checkbox"/> Unknown

Malicious Software (Malware)	
Virus, Worm or Trojan Horse	
Type of Malware:	<input type="checkbox"/> Virus <input type="checkbox"/> Worm <input type="checkbox"/> Trojan Horse
Name or Description	

Malicious Software (Malware)		
Is Anti-Malware Software Installed on Affected Computer(s)?	Specify: <input type="checkbox"/> Yes	<input type="checkbox"/> No
Did the Anti-Malware Software Detect the Infection?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
When was Anti-Malware Software Last Updated?		

Network Activity Summary	
Name or Description of Exploit (if known)	
Protocol(s) Targeted or Used	<input type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> FTP <input type="checkbox"/> Telnet <input type="checkbox"/> IPSec <input type="checkbox"/> IPv6 <input type="checkbox"/> ICMP <input type="checkbox"/> SMTP <input type="checkbox"/> IP Multicast <input type="checkbox"/> SSL <input type="checkbox"/> SSH <input type="checkbox"/> RDP <input type="checkbox"/> Other (Specify): _____
Identify Source IP Addresses in the Incident	
Identify Source Ports in the Incident	
Identify Destination IP Subnet in the Incident	
Identify Destination Ports in the Incident	

Impact of Incident/Attack			
Hosts Compromised (for more than 2 Hosts, use the "Bulk Hosts" section to list Host Names below and provide details on additional pages)			
Individual Host #1	Host Name		
Does this Host Represent an Attacking or Victim Host?	<input type="checkbox"/> Victim	<input type="checkbox"/> Attacker	<input type="checkbox"/> Both
Operating System Affected		Patch Level	
Applications Affected			
Databases Affected			
Web Sites Affected			
Other Host Impacts			

Impact of Incident/Attack			
Primary Purpose of This Host	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;"><input type="checkbox"/> Application Server</div> <div style="width: 50%;"><input type="checkbox"/> Database Server</div> <div style="width: 50%;"><input type="checkbox"/> Web Server</div> <div style="width: 50%;"><input type="checkbox"/> Email Server</div> <div style="width: 50%;"><input type="checkbox"/> FTP Server</div> <div style="width: 50%;"><input type="checkbox"/> NFS/File Server</div> <div style="width: 50%;"><input type="checkbox"/> Time Server</div> <div style="width: 50%;"><input type="checkbox"/> Other Server</div> <div style="width: 50%;"><input type="checkbox"/> Domain Name Server</div> <div style="width: 50%;"><input type="checkbox"/> Domain Controller</div> <div style="width: 50%;"><input type="checkbox"/> End User Laptop</div> <div style="width: 50%;"><input type="checkbox"/> End User Desktop</div> <div style="width: 50%;"><input type="checkbox"/> Infrastructure Device (i.e., router or firewall)</div> <div style="width: 50%;"><input type="checkbox"/> Other (Specify) _____</div> </div>		
Individual Host #2	Host Name		
Does this Host Represent an Attacking or Victim Host?	<input type="checkbox"/> Victim <input type="checkbox"/> Attacker <input type="checkbox"/> Both		
Operating System Affected	Patch Level		
Applications Affected			
Databases Affected			
Web Sites Affected			
Other Host Impacts			
Primary Purpose of This Host	<div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;"><input type="checkbox"/> Application Server</div> <div style="width: 50%;"><input type="checkbox"/> Database Server</div> <div style="width: 50%;"><input type="checkbox"/> Web Server</div> <div style="width: 50%;"><input type="checkbox"/> Email Server</div> <div style="width: 50%;"><input type="checkbox"/> FTP Server</div> <div style="width: 50%;"><input type="checkbox"/> NFS/File Server</div> <div style="width: 50%;"><input type="checkbox"/> Time Server</div> <div style="width: 50%;"><input type="checkbox"/> Other Server</div> <div style="width: 50%;"><input type="checkbox"/> Domain Name Server</div> <div style="width: 50%;"><input type="checkbox"/> Domain Controller</div> <div style="width: 50%;"><input type="checkbox"/> End User Laptop</div> <div style="width: 50%;"><input type="checkbox"/> End User Desktop</div> <div style="width: 50%;"><input type="checkbox"/> Infrastructure Device (i.e., router or firewall)</div> <div style="width: 50%;"><input type="checkbox"/> Other (Specify) _____</div> </div>		
Bulk Hosts (more than 2) – List Host Names below and include above details on additional pages			
Host Names			
Comments (provide any additional details about the Incident, not already captured)			

Impact of Incident/Attack	
Data Compromised	
Did Incident Result in Loss/Compromise of Sensitive or Personal Information?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown
Comments	
Did the Incident Result in Damage to System(s) or Data?	<input type="checkbox"/> Yes (Specify) _____ <input type="checkbox"/> No <input type="checkbox"/> Unknown
Comments	
Remediation	
Please detail/specify what corrective actions have been taken for this Incident	
Lesson Learned Information (Optional)	
Did your Detection & Response process and procedures work as intended? [Enter Comments Below]	
Provide any Discovery Methods, Indicators of Compromise, and/or Monitoring Procedures that would have improved your ability to detect an Intrusion. [Enter Comments Below]	

Lesson Learned Information (Optional)
Are there improvements to Procedures and Tools that would have aided you in the Response Process? [Enter Comments Below]
Are there improvements that would have enhanced your ability to contain an Intrusion? [Enter Comments Below]
Are there Corrective Procedures that would have improved your effectiveness in Recovering your systems? [Enter Comments Below]

APPENDIX D

CSIRT POINTS OF CONTACT LIST

The following list, when filled in, should be considered as "Confidential Information" and only available to CSIRT members and other authorized individuals as approved by [Your Company Name]'s executive team. When completing this list, the CISO or other responsible person must consider the inclusion of third party (external) IT service providers, as well as other trusted business partners, suppliers or vendors who have a valid "need to know" status. When including external CSIRT members, insert their company affiliation with the other information. The CISO should add CSIRT team members or others to the completed list, as necessary, depending on the company's requirements.

This list does not determine WHAT information (nature or extent) is shared with each person or entity, it merely provides the contact information. This list also does not determine WHEN the person or entity should be contacted or details of WHAT information can or should be shared – those requirements will be contained in contracts or operating agreements, security policies or procedures, non-disclosure agreements, etc.

[Note: Delete those positions or categories which do not apply to your organization and add or modify ones that do apply.]

Category or Position	Description
Company's Primary Executive	[Your Company Name] Owner or CEO
Full Name	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
Chief Information Officer	[Your Company Name] CIO
Full Name	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	

For this Appendix, note the warning in the first sentence – this should be considered **CONFIDENTIAL INFORMATION** and should be kept separate from any accessible version of the Plan/Policy document. It should only be shared with the CSIRT members and other authorized persons who have a "need to know" the information. When sharing this with external partners (e.g., ISP or IT service providers) who are part of the CSIRT, it is recommended to include this in a Non-Disclosure Agreement. A public version of this Appendix may contain a simple list of position titles for the CSIRT members.

Fill out the appropriate contact information for each CSIRT member. Remove the boxes/rows for those positions which are not applicable, and delete the instructions highlighted here in cyan.

Category or Position	Description
Other Method of Contact	
Chief Financial Officer	[Your Company Name] CFO
Full Name	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
Human Resources Director/Manager	[Your Company Name] Head of Human Resources
Full Name	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
Company Legal Counsel	[Your Company Name] Legal Counsel (Attorney)
Full Name	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
Cybersecurity Insurance Provider	Cyber Insurance – Confidential Claims Representative
Insurance Company Name	
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	

Category or Position	Description
Secondary Email	
Other Method of Contact	
Chief Information Security Officer	[Your Company Name] CISO (CSIRT Leader)
Full Name	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – CISO's Alternate	CSIRT Member – Alternate for CISO
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Network Operations	Primary CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Network Operations	Alternate CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	

Category or Position	Description
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Data Center Operations	Primary CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Data Center Operations	Alternate CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Information Security	Primary CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Information Security	Alternate CSIRT Member

Category or Position	Description
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Website Management	Primary CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Website Management	Alternate CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Applications Management (Development/Support)	Primary CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	

Category or Position	Description
Secondary Email	
Other Method of Contact	
CSIRT Member – Applications Management (Development/Support)	Alternate CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Database Administration (DBA)	Primary CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Database Administration (DBA)	Alternate CSIRT Member
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Internet Services Provider(s) (ISPs)	Primary CSIRT Member
Company Name	

Category or Position	Description
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Internet Services Provider(s) (ISPs)	Alternate CSIRT Member
Company Name	
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Cloud Services Provider(s) (CSPs)	Primary CSIRT Member
Company Name	
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Cloud Services Provider(s) (CSPs)	Alternate CSIRT Member
Company Name	
Full Name	

Category or Position	Description
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Managed Security Services Provider(s) (MSSPs)	Primary CSIRT Member
Company Name	
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Managed Security Services Provider(s) (MSSPs)	Alternate CSIRT Member
Company Name	
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Company Operations (Functional Business Unit #1)	Primary CSIRT Member – [Operational Business Unit]
Full Name	
Position/Title	
Primary Phone	

Category or Position	Description
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Company Operations (Functional Business Unit #1)	Alternate CSIRT Member – [Operational Business Unit]
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Company Operations (Functional Business Unit #2)	Primary CSIRT Member – [Operational Business Unit]
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Company Operations (Functional Business Unit #2)	Alternate CSIRT Member – [Operational Business Unit]
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	

Category or Position	Description
Other Method of Contact	
CSIRT Member – Company Operations (Functional Business Unit #3)	Primary CSIRT Member – [Operational Business Unit]
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	
CSIRT Member – Company Operations (Functional Business Unit #3)	Alternate CSIRT Member – [Operational Business Unit]
Full Name	
Position/Title	
Primary Phone	
Alternate Phone	
Pager/Text Messaging	
Primary Email	
Secondary Email	
Other Method of Contact	

Computer Security Incident Response Plan Template – Short Version

CONCLUSION OF
GUIDE AND INSTRUCTIONS