|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Information Security Process | | | | | | |
| Cyber Incident Response Process | | | | | | |
| Process # |  | | Effective Date |  |
| Version |  | Last Review Date | |  | Contact |  |

Table of Contents

[Purpose 1](#_Toc115087056)

[Scope 2](#_Toc115087057)

[Process 2](#_Toc115087058)

[Preparation 3](#_Toc115087059)

[Detect 3](#_Toc115087060)

[Analysis 3](#_Toc115087061)

[Containment 3](#_Toc115087062)

[Eradication 4](#_Toc115087063)

[Recovery 4](#_Toc115087064)

[Post-Incident Activity 4](#_Toc115087065)

[Process – Detailed Flow Diagram / Process 5](#_Toc115087066)

[Process – Detailed Steps 5](#_Toc115087067)

[Measurement Metrics 5](#_Toc115087068)

[Verification of Implementation 5](#_Toc115087069)

[Archiving Incident Response Data 5](#_Toc115087070)

[Purging of Incident Response Archives 5](#_Toc115087071)

[Definitions 5](#_Toc115087072)

[Computer Incident / Cyber Security Incident 5](#_Toc115087073)

[Threats 6](#_Toc115087074)

[Impact 9](#_Toc115087075)

[Prioritizing and Reporting Events 10](#_Toc115087076)

[Roles and Responsibilities 10](#_Toc115087077)

[RACI 10](#_Toc115087078)

[Training 10](#_Toc115087079)

[Monitoring and Audits 10](#_Toc115087080)

[Process Compliance 10](#_Toc115087081)

[Resources 10](#_Toc115087082)

[Approval and Ownership 10](#_Toc115087083)

[Revision History 11](#_Toc115087084)

Purpose

The purpose of this document is to describe the high-level process that <COMPANY> will use to respond to a cyber-security related incident, including the subsequent investigations on the causes, a damage assessment, and remedial actions to prevent recurrence. These measures are necessary to ensure the confidentiality of our data, the integrity of our data, and the reliability/availability of our information systems. The incident response process document does not restate the requirements outlined in the incident response policy but includes references to them. The <COMPANY> incident response policy document and the incident response process documents (cyber and / or data) have been designed so that they may evolve independently.

Scope

This process applies to all lines of business within <COMPANY>. It is directed at all cyber-security incidents. It sets the minimum requirements for recognizing and responding to a cyber-security related incident within <COMPANY>.

This process is directed at cyber-security incidents of all types. A cyber-security incident is an event that adversely affects some portion of the computing resources such as malware propagation, unauthorized intrusions, or security violations originating from within our own organization.

This process does not cover responding to a computer “crisis” but can be included as part of the <COMPANY> crisis response plan. A crisis is an unplanned event with the potential for significant injury to people or the environment, or the potential for significant damage to the company, its employees, facilities, products, financial condition or reputation.

Process

Each incident encountered is unique. The process used will vary based on the events and the environment in which they occurred. Existing processes should be adapted responsibly in order to balance security with operational requirements. The response processes for common types of incidents are detailed as appendixes in this document.

<describe any guidelines you’re following>

### Preparation

Preparation consists of actions taken before an incident to prepare to minimize incidents, to timely and efficiently respond to those incidents that do occur, and to rapidly implement corrective actions once an incident occurs.

#### Preparation - Training

<preferred training>

#### Preparation - Resources

<what IR team needs to be prepared>

### Detect

Describe your inputs for security events

### Analysis

Describe how events come in and are escalated as necessary

### Containment

Containment is critical for preventing the incident from overwhelming IT resources or further damaging the business. When sufficient information has been gathered and analyzed to understand the incident, the incident response team member will formulate an initial containment plan. This plan will then be communicated to the responsible parties for execution. Updates to the strategy may be required as analysis continues.

Containment strategies will vary based on the type of incident, however several elements must be considered when determining the containment strategy:

* Potential damage to other information assets
* Need to preserve evidence
* Impact to the business
* Time and resources required to implement
* Effectiveness
* Duration of the solution

### Eradication

Once an incident has been contained it is normally necessary to eliminate artifacts created by the incident such as removing malware, reversing changes made by an attacker, and disabling user and service accounts used or comprised by the attacker.

In some incidents, eradication is either not required or is done by recovering the information asset to a known good state in the recovery phase.

### Recovery

Recovery involves returning the information asset to normal operation. This involves confirming that the systems are configured properly and are functioning normally, as well as mitigating the vulnerabilities that were exploited by the attacker.

Once system administrators and application owners have confirmed the system are configured properly and all necessary mitigation has been completed and verified by the incident response team the effected system may be put back into production.

In some cases, it may be required to restore the entire system to a prior known good state. If this is done the backup used for the restore must be from prior to the incident. If an exact date of compromise cannot be determined, then the system shall be rebuilt from scratch.

If a system is restored to a prior known good state it will still be necessary to confirm that the systems are configured properly and are functioning normally, as well as mitigating the vulnerabilities that were exploited by the attacker.

Both eradication and recovery should be done in a phased approach. This phased approach should take into account the impact to the business. Because eradication and recovery can take some time to complete it may be necessary to hand off the process of eradiation and recovery to other representatives of <COMPANY> for completion. When this is done the individual responsible for completion of the eradiation and remediation becomes responsible for the verification of the eradication / recovery and returning the systems to production.

### Post-Incident Activity

Once an incident has been declared by the incident response team to be closed there is still one more important and often overlooked step – learning and improving.

A “lessons learned” meeting with representation from all involved parties shall be done after every major incident and after minor incidents if deemed necessary. The meeting should be held within one week of the end of the incident. Questions that should be asked during that meeting are, but not limited to:

* Exactly what happened, and at what times?
* How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
* What information was needed sooner?
* Were any steps or actions taken that might have inhibited the recovery?
* What would the staff and management do differently the next time a similar incident occurs?
* How could information sharing with other organizations have been improved?
* What corrective actions can prevent similar incidents in the future?
* What precursors or indicators should be watched for in the future to detect similar incidents?
* What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Draft recommendations will be presented to IR leadership, Legal, and the business. With approval, changes to the environment will be formally tracked to ensure they are completed in a timely manner.

# Process – Detailed Flow Diagram / Process

<insert diagrams>

## Process – Detailed Steps

<break down each step of flow diagrams>

# Measurement Metrics

<how are you tracking incidents? What metrics can you take?>

# Verification of Implementation

Self-audits, such as lessons learned follow-up meetings, will be performed to verify implementation and improvements to the incident response process/procedures.

# Archiving Incident Response Data

<Describe archiving activities and standards>

# Purging of Incident Response Archives

<Describe purging schedule, and how legal holds are handled. Note naming convention/labeling as needed>

Definitions

Terms contained within this document are standard international terms used for information security. For general definitions see NISTIR 7298, Rev 2 - Glossary of Key Information Security Terms (<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>)

## Computer Incident / Cyber Security Incident

The terms *"computer incident"* and *"cyber-security incident"* are used interchangeably and refer to any situation dealing with a potential breach or violation of cyber security. Violations or breaches generally fall under the control of the following areas:

|  |  |  |
| --- | --- | --- |
| **Area of Violation** | **Questions To Ask** | **Whom To Ask** |
| Law | Have any local, state, federal / national, or international laws been broken? Cyber security related events are considered crimes under these laws, and include such things as embezzlement, theft, extortion, vandalism, sabotage, and espionage. | * Legal |
| Regulations | Have regulatory controls been violated? | * Legal * Compliance |
| Policy | Have any <COMPANY> policies been violated? | * Information Security * Human Resources * Finance * Legal * Compliance |
| <COMPANY> corporate brands / image and / or credibility | Has damage been done to adversely affect the image of the company? Examples might include postings on social media, web sites or other external sites and services. | * Legal * Compliance |
| Adverse effect on normal operations | Has damage been done to adversely affect the availability or integrity of information systems? Examples include virus/worm or denial of service attacks. | * Information Technology * Information Security * Information Owners |

## Threats

A threat is the potential for an event that can exploit vulnerabilities and cause harm by violating security on an information asset. Many threats have been identified by <COMPANY> at the enterprise level and prioritized based on potential impact and likelihood of occurrence.

These threats, if realized, can result in one or more of the following types of incidents:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Related Threats** | **Definition** | **Example** |
| Unauthorized Access | Computer Intrusions  Insider Actions / Inappropriate  Activities  Computer  Worms/Viruses  Web Site Defacement  Departing Employee  Malicious Actions | When information assets are accessed in an unspecified or unauthorized manner.  Unauthorized access encompasses a broad range of activities.  Unauthorized access includes any attempt to gain access to a system or its data when the company has not specifically authorized such access. | Logging into an account not owned by the person attempting the action.  Accessing files, directories, or applications to which one does not have explicit access.  Obtaining privileged access when it is not authorized.  Exploiting known security vulnerabilities to yield an unauthorized result.  Hacking into a system by using a legitimate account defined on the system. |
| Misuse / Abuse | Unauthorized Disclosure of Sensitive Data, Sales & Marketing Data, or  Personnel Records  Computer Intrusions  Insider Actions / Inappropriate  Activities  Departing Employee  Malicious Actions | When an information asset is used for purposes other than intended, as specified in <COMPANY> policy. | Accessing sexually explicit Internet sites.  Use of privileged accounts beyond the scope of intended responsibilities.  Harassment.  Criminal activity.  Personal gain (running a business, day trading, etc.) |
| Intrusion / Penetration | Computer Intrusions  Computer Worms / Viruses | An event that violates system security through unauthorized access, such as when an unauthorized program attempts to access a network or computer system. | Hacker attack.  Exploit scripts run against known vulnerabilities.  Social engineering. |
| Reconnaissance / Probe | Computer Intrusions  Computer Worms / Viruses | Use of manual and/or electronic tools to gather information in preparation for an attack. | Port scans.  Ping sweeps.  Banner grabbing.  Social engineering.  War dialing.  War driving/walking for accessible Wi-Fi hotspots. |
| Compromise of Integrity | Computer Intrusions  Insider Actions / Inappropriate  Activities  Computer Worms / Viruses  Web Site Defacement  Departing Employee  Malicious Actions | When information is altered in an unauthorized manner. | Changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.  Purposely changing permissions on files and systems to facilitate unauthorized access. |
| Denial of Service | Computer Intrusions  Insider Inappropriate  Activities  Computer Worms / Viruses  Web Site Defacement  Departing Employee  Malicious Actions | Any user or program that disrupts any network or computer services by denying access to them or degrading normal service. | Flooding traffic on a network.  Looping programs that monopolize service.  Bandwidth-hogging utilizing a program or web service that meets misuse criteria.  Purposely shutting down critical infrastructure and systems with direct business impact. |
| Malicious Code Attack  Unauthorized Changes | Computer Intrusions  Insider Inappropriate  Activities  Computer Worms / Viruses  Web Site Defacement  Departing Employee  Malicious Actions | Unauthorized changes to system hardware, firmware, software, or data files that destroy data and/or cause programs to work in unauthorized ways. | Computer Virus  Trojan Horse  Worm  Exploit of vulnerabilities |
| Theft | Unauthorized Disclosure of Sensitive Data, Sales & Marketing Data, or  Personnel Records  Insider Actions / Inappropriate  Activities  Computer Worms / Viruses  Web Site Defacement  Departing Employee  Malicious Actions | Any loss of an  information asset that  results from stealing | Stolen laptop  Stolen hardware (memory, disk drives, etc.)  Confidential information  published without  authorization |
| Fraud | Unauthorized Disclosure of Sensitive Data, Sales & Marketing Data, or  Personnel Records  Insider Actions / Inappropriate  Activities  Departing Employee  Malicious Actions | Any intentional scheme to obtain money or property belonging to <COMPANY> by means of false pretenses. | Email scam (phishing)  Social Engineering to obtain information |

*Note: Not every event fitting these definitions requires a formal incident response. For example, there are routine attempts to send viruses into the system, and these are prevented daily by information security countermeasures. Such expected, unsuccessful events do not need to be treated as cyber-security incidents. However, users must immediately report to the <COMPANY> Service Desk any incidents that are unexpected, successful (or nearly successful), or indicate a new vulnerability, threat source, or motivation. If there is doubt about whether to report an incident, it should be reported. Each location's IT support team shall work with their designated Cyber Incident Response Team representative to determine the level of response and documentation needed.*

## Impact

Cyber security incidents have an impact in the following three areas:

|  |  |
| --- | --- |
| **Security Impact** | **Definition** |
| Confidentiality | The protection of information assets from unauthorized access, leakage, or copying. (Losing customer data, unauthorized access to an information asset, etc.) |
| Integrity | The protection of information from unauthorized modification. (Accuracy of data, sensitivity to fraud, etc.) |
| Availability | Ensuring information assets are available to authorized users when needed and expected. (Extended outages, denial of service, etc.) |

Security incidents can be quantified in terms of their overall impact to the company:

|  |  |
| --- | --- |
| **Business Impact** | **Definition** |
| Financial | Dollar loss (direct and indirect) |
| Legal | Legal effects (loss of contract, compliance, liability, etc.) |
| Customer / Business Partner | Impact on customers (loss of trust, loss of customer, spread of damage to external partners, etc.) |
| Company Image | <COMPANY> image (bad publicity, reputation, shareholder confidence, etc.) |

## Prioritizing and Reporting Events

<describe how company classifies severity level for various incident types and importantly, describe SLAs for acknowledgement, containment/resolution, and whether there is expectation of 24/7 response>

Roles and Responsibilities

# RACI

<add RACI if applicable>

Training

<Required training for team>

Monitoring and Audits

<who is auditing to ensure the process is being followed>

Process Compliance

This process becomes effective upon publication.

Resources

* NIST Special Publication 800-61 Rev 2 - *Computer Security Incident Handling Guide*

<any internal policies>

Approval and Ownership

Copy in the electronic approval of each approver. Type the name of the approver, and the date approved on each approval line on the cover page.

|  |  |  |
| --- | --- | --- |
| Owner | Title | Date |
|  |  |  |
| Approved By | Title | Date |
|  |  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Rev** | **Date** | **Author** | **Description** |
|  |  |  |  |