A picture containing graphical user interface

Description automatically generated

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comment** |
| 0.1 | Oct 5, 2022 |  |  |
|  |  |  |  |
|  |  |  |  |

# Contents

[Version History 1](#_Toc115865031)

[Contents 1](#_Toc115865032)

[Purpose/Goals 2](#_Toc115865033)

[Definitions 2](#_Toc115865034)

[Incident Response Team Contact List 3](#_Toc115865035)

[Example Flow 4](#_Toc115865036)

[Using this Plan 5](#_Toc115865037)

[Role Responsibilities 5](#_Toc115865038)

[Communications 7](#_Toc115865039)

[Measurement 8](#_Toc115865040)

[Documentation & Reporting 9](#_Toc115865041)

[Internal Review & Post-Incident Activity 9](#_Toc115865042)

[Appendix A: Common Definitions 10](#_Toc115865043)

[Appendix B: Critical Systems Inventory 11](#_Toc115865044)

[Appendix C: Recommended Additional Resources 12](#_Toc115865045)

# Purpose/Goals –

* We encourage you to consider your goals carefully
* They should be unique to your organization

# Definitions –

Definitions are important to empower the rest of your team

Here are some common ones:

* Security Controls - A safeguard, something intended to reduce risk
* Information Security Policy - Mandatory, high-level management directives.
* Event - An event is an action taken that alters a system's state.
* Incident - An incident is event that indicates a violation of policy or a security control.

# Incident Response Team Contact List:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Contact Info** | **Call Priority** |
|  | *Incident Commander* |  |  |
|  | *CSIRT* |  |  |
|  | *Leadership Role* |  |  |
|  | *Communications* |  |  |
|  | *IT Team* |  |  |
|  | *Legal Counsel* |  |  |
|  | *Insurance Agent* |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Example Flow

Not every step may be necessary. See relevant plan section.

# Using this Plan

**Activating the IRT:**

What is an acceptable way to begin this process?

Who can be activated before authorization is required?

**Incident Assessment:**

What do you need to make intelligent decisions?

Who is going to be getting that information?

Where are you keeping track of the information provided?

**Activate CSIRT:**

Special activation at specific threshold?

Pre-Existing relationship?

**Remediate Incident:**

How will you track progress?

Will you need to preserve forensic evidence?

**Recovery:**

Who will determine recovery effort?

Is the recovery team able to provide separate environment?

# Role Responsibilities

*Have you decided who:*

o Declares Incident o Activates CSIRT o Calls Insurance o Notifies regulatory body

Incident Team:

Incident Commander:

CSIRT:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Leadership Role I.e. CEO, CFO, President, etc.):

IT Team:

Communications:

# Communications

How will we communicate during the incident?

Who will notify staff?

Who will talk to the public?

What is our backup communication channel?

What regulatory bodies should be considered for notification of this event?

Will we have different people speaking to media? Law Enforcement? External stakeholders?

# Measurement 🡪Prioritization

Rules of Thumb

1. Is a critical system affected?
2. What sensitivity is the data at risk?
3. How extensive is the scope?
4. Do we understand the source of the attack?

**Information Risk Assessment**

|  |  |  |
| --- | --- | --- |
| None | No information is believed to be at risk. | No IR required. |
| Limited | Non-sensitive data is at risk. | Consult with data owner. |
| Moderate | Internally sensitive data is at risk. | Notify leadership. |
| Critical | Protected / Regulated / Proprietary data is at risk. | Activate CSIRT and legal counsel. |

# Documentation & Reporting

Where will this plan be kept?

Where are we going to store the record of the incident?

What are we going to capture in our record?

How long should we preserve these records?

# Internal Review & Post-Incident Activity

Who will create the after-action report?

Will this be shared externally?

Who will review the report? Will there be a meeting to review collectively?

Is there a mechanism to incorporate recommendations into the program?

# Appendix A: Common Definitions

*While we recommend each organization define these terms as best fits their purposes, these definitions should provide a good starting point.*

**Breach:** A legal term that can be summarized as unauthorized or impermissible use or disclosure of sensitive information. Be cautious using this term during a response effort!

**Breach Counsel:** A specialized attorney who can lead response efforts and advise organizations on legal liability during an incident.

**CSIRT:** Cyber Security Incident Response Team, the specialized technical experts who can make definitive statements about how a threat originated, what was accessed, and whether the threat is eradicated. Often an external resource.

**Due Care:** The Prudent Person concept – what would a reasonable person do, the informal expectation of risk reducing behavior.

**Due Diligence:** The practice of applying Due Care, the formal and ongoing program applied to reduce risk, the validation of expectation.

**DR:** Disaster Recovery, a process to recover mission critical data after a significant loss event.

**Event​:** An event is an action taken that alters a system's state.​ Adverse events are those that negatively affect a system or data.

**Incident​:** An incident is an event that indicates a violation of policy or a security control.​ An incident jeopardizes the confidentiality, integrity, or availability of information.

**Incident Commander:** The individual responsible for leading an incident response, and often accountable to the organization leadership for managing the response program.

**Information Security:** The application of administrative, physical or technical controls to protect the confidentiality, integrity, or availability of information.

**Information Security Policy​:** Mandatory, high-level management directives.​

**IRT:** The Incident Response Team; the people identified with specific roles and responsibilities to handle during incident response.

**Security Controls​:** A safeguard, something intended to reduce risk​

# Appendix B: Critical Systems Inventory

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **System or Process** | **Business Function** | **System Criticality** | **Dependencies** | **Data Sensitivity** |
| *e.g. Payroll* | *Payroll* | *Critical* | *Vendor, Bank, HR system* | *High* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Expand this inventory to include Maximum Tolerable Downtime, Recovery Time Objectives, System Ownership, etc.

# Appendix C: Recommended Additional Resources

**NIST SP 800-61 Rev. 2 “Computer Security Incident Handling Guide”**

https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

**SANS “Incident Handler’s Handbook”**

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

**CIS Critical Security Control 17 “Incident Response and Management”**

https://www.cisecurity.org/controls/incident-response-and-management/

*This ‘Incident Response Plan’ (IRP) handout is intended as a starting framework to help you on your Incident Planning and Preparation journey. This is not intended to be a fully comprehensive IRP to cover all potential incident scenarios.*