Cyber and Data Security Incident Response Plan Template

This incident response plan template has been derived from the public domain information of the SANS Institute cybersecurity sample policies and other public sources. It is available for usage, alteration, and reformatting according to the specific needs of your organization.

Goals for Cyber Incident Response

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is a critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

1. Preserve and protect the confidentiality of constituent and employee information and ensure the integrity and availability of <COMPANY NAME> systems, networks and related data.

2. Help <COMPANY NAME> personnel recover their business processes after a computer or network security incident or other type of data breach.

3. Provide a consistent response strategy to system and network threats that put <COMPANY NAME> data and systems at risk.

4. Develop and activate a communications plan including initial reporting of the incident as well as ongoing communications, as necessary.

5. Address cyber related legal issues.

6. Coordinate efforts with external Computer Incident Response Teams and law enforcement.

7. Minimize <COMPANY NAME>'s reputational risk.

Purpose and Scope

This publication provides practical guidelines on responding to cyber security and data breach incidents in a consistent and effective manner. The plan establishes a team of first responders to an incident with defined roles, responsibilities, and means of communication.

While this plan is primarily oriented around cyber-related incidents and breaches, it can also be utilized for data breaches that are not related to computer systems.

Incident Response Team (IRT)

A team comprised of company staff, advisors, and service providers shall be responsible for coordinating incident responses and known as the Incident Response Team (IRT). The IRT shall consist of the individuals listed in Appendix A, having the noted roles and responsibilities. This team will have both primary members and secondary members. The primary members of the IRT will act as first responders or informed members to an incident that warrant IRT involvement, according to the incident's severity. The entire IRT would be informed and involved in the most severe incidents.

IRT members may take on additional roles during an incident, as needed. Contact information, including a primary and secondary email address, plus office and mobile telephone numbers shall be maintained and circulated to the team. The IRT will draw upon additional staff, consultants or other resources, (often referred to as Subject Matter Experts – SME's) as needed, for the analysis, remediation, and recovery processes of an incident. The Information Technology (IT) function plays a

significant role in the technical details that may be involved in an incident detection and response and can be considered an SME in that regard.

There shall be a member of the IRT designated as the Incident Response Manager (IRM), who will take on organizational and coordination roles of the IRT during an incident where the IRT is activated for response to the incident.

Incident Response Life Cycle Process

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response process elements that comprise the Cyber Incident Response Plan include:

1. **Preparation:** The on-going process of maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, applications, and data handling processes are sufficiently secure, and employee awareness training is in place. Practice exercises (aka Table-top Exercises) for the IRT are conducted periodically, where various incident scenarios are presented to the Team in a practice session.

2. **Identification:** The process of confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.

3. **Notification:** Alerting IRT members to the occurrence of an incident and communicating throughout the incident.

4. **Containment:** Minimizing financial and/or reputational loss, theft of information, or service disruption. Initial communication with constituents and news media, as required.

5. **Eradication:** Eliminating the threat.

6. **Recovery:** Restoring computing services to a normal state of operation and the resumption of business activities quickly and securely. Provide reputational repair measures and news media updates, if needed. Provide credit monitoring services to effected constituents, or other remediation measures, as appropriate.

7. **Post-incident Activities:** Assessing the overall response effectiveness and identifying opportunities for improvement through, ‘lessons learned’ or mitigation of exploited weaknesses. Incorporation of incident’s learnings into the cyber fortification efforts and the response plan, as appropriate.

These process elements are depicted in Figure 1, showing the closed loop nature of the process, in that the learnings from any prior incidents are used to improve the prevention and response process of potential future incidents.

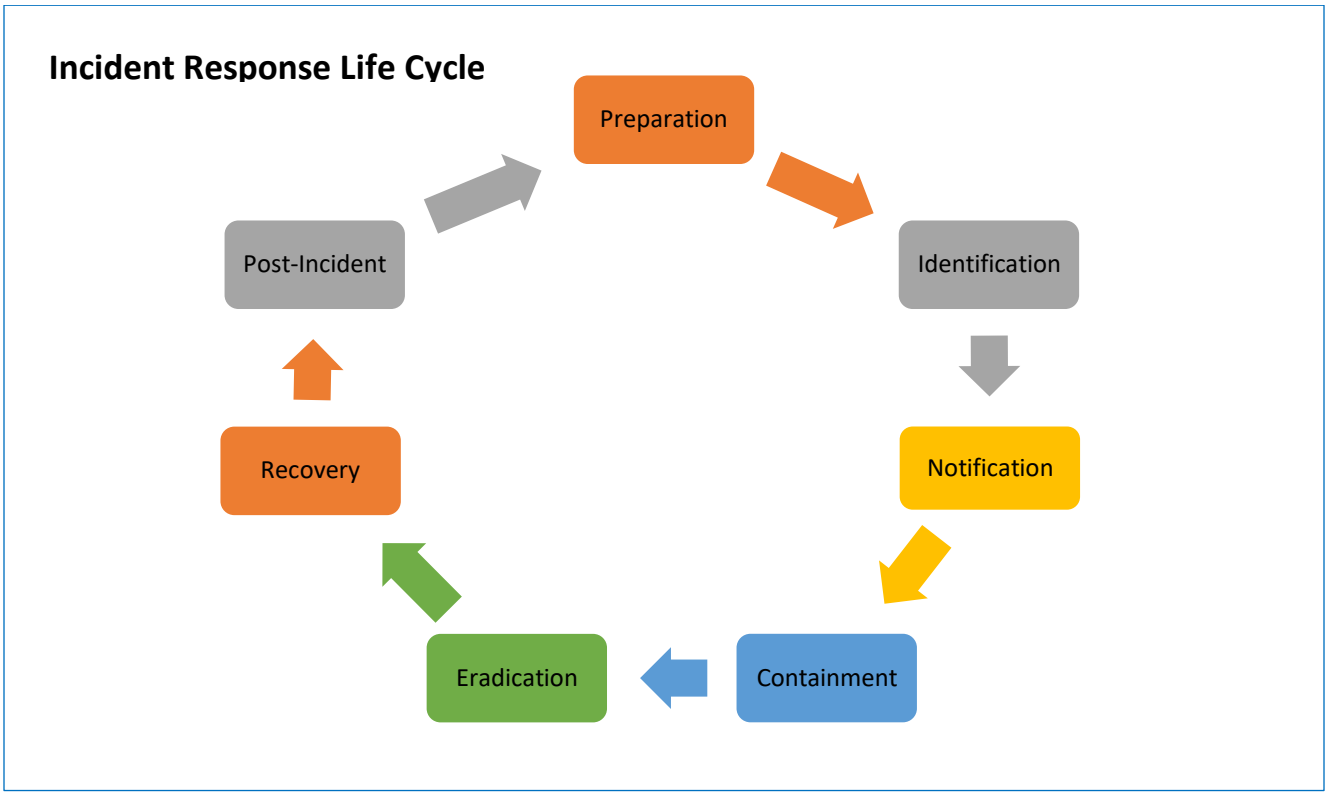

Figure 1

Incident Occurrence & Awareness

The way an incident becomes know will have an impact on the response process and its urgency. Examples by which <COMPANY NAME> becomes aware of an incident include, but are not limited to the following:

1. <COMPANY NAME> discovers through its internal monitoring that a cyber incident or data breach has occurred.
2. <COMPANY NAME> is notified by one of its technology providers of an incident or becomes aware of the same.
3. <COMPANY NAME> is made aware of a breach through a constituent or a third-party informant.
4. <COMPANY NAME> and the public are made aware of the incident through the news media.

Incident Response Process Detail

The response process, at a detail level, for an incident includes 5 of the 6 life cycle phases, as it excludes the Preparation phase. The detailed steps and general timing of an incident response are outlined below. The IT function is specifically called out as an involved party, separate from other SME's.

Process Phase & Approximate Timing	Process Detail Steps	Involved Parties
Identification (Hours)	1. Identify and confirm that the suspected or reported incident has happened and whether malicious activity is still underway. 2. Determine the type, impact, and severity of the incident by referring to **Appendices B, C, and D**. 3. Take basic and prudent containment steps.	IT and any monitoring service provider
Notification (Hours – 1 Day)	4. Inform or activate the IRT, based on the severity of the incident, as outlined in Appendix D, and provide the type, impact, and details of the incident to the extent that they are known. 5. Determine the need for Subject Matter Experts (SME) to be involved in the Containment, Eradication, and Recovery processes.	IT & IRT
Containment (Hours-2 Days)	6. Take immediate steps to curtail any on-going malicious activity or prevent repetition of past malicious activity. 7. Re-direct public facing websites, if needed. Provide initial public relations and legal responses as required.	IRT, IT, SME's
Eradication (Days -Weeks)	8. Provide full technical resolution of threat and related malicious activity. 9. Address public relations, notification, and legal issues.	IT, IRT, SME's
Recovery (Weeks -Months)	10. Recover any business process disruptions and re-gain normal operations. 11. Address longer term public relations or legal issues, if required, and apply any constituent remedies.	SME's, IRT
Post-incident (Months)	12. Formalize documentation of incident and summarize learnings. 13. Apply learnings to future preparedness.	IRT

Communication Methods

Company communication resources (email, phone system, etc.) may be compromised during a severe incident. Primary and alternate methods of communication using external infrastructure will be established and noted on the IRT member contact list to provide specific methods of

communication during an incident. The IRT and any other individuals involved in an incident resolution will be directed as to which communication method will be used during the incident

Information Recording

Information recording is very important during an incident, not only for effective containment and eradication efforts, but also for post-incident lessons learned, as well as any legal action that may ensue against the perpetrators. Each member of the IRT shall be responsible for recording information and chronological references about their actions and findings during an incident, using the IRT Incident Record Form in Appendix E.

Incident Response Exercises

The IRT should conduct 'table-top' exercises to practice the response process on a periodic basis, but at least annually, so all members of the IRT are familiar with the activities that would occur during an actual incident and their related responsibilities. The exercises may provide the opportunity for enhancing the coordination and communication among team members.

Summary

No perfect script can be written for the detailed activity encountered and decisions that will need to be made during an incident, as each incident will have its own uniqueness. This plan shall serve as a framework for managing cyber security and data breach incidents, allowing the details of confirmation, containment, eradication, and communication to be tailored to fit the specific situation.

Appendix A - <COMPANY NAME> Cyber Incident Response Team (IRT)

Team Members and Roles - *Substitute staff names and titles below as appropriate. Not all the positions may be available in your organization and/or the same person may have multiple roles within the IRT.*

Primary Team Members

1. <Head of Information Technology>
    a. Maintain proactive cybersecurity policies and procedures
    b. Discover and/or verify cyber incidents
    c. Notify IRT members of incidents and provide updated
    d. Coordinate computer forensic and technical remediation activities
    e. Apply corrective actions to technology infrastructure

2. <Incident Response Manager> (IRM)
    a. Coordinate communications and activities of the IRT when it is activated

3. <Executive level manager in charge of financial management>
    a. Financial impact and financial data exposure

4. <Executive level manager in charge of external communications and public relations>
    a. Public relations
    b. News media management
    c. External and internal communication

5. <Executive level manager in charge of human resources>
    a. Communication to employees
    b. Employee data exposure issues

6. <Executive level manager in charge of company operations>
    a. Operational impact and/or overall data exposure assessment

7. <Executive level manager in charge of physical security>
    a. Building access and control

Secondary Team Members

8. <Security event monitoring vendor and/or computer forensics vendor>
    a. Detection
    b. Mitigation
    c. Technical Forensics

9. <Legal representative>
    a. Legal advisor
    b. Contractual matters

10. <Public relations vendor>
    a. Public relations advisor

11. <Cyber insurance provider>
    a. Cyber Insurance advisor

Contact information and communication methods for the IRT members should be distributed to the team separately as confidential information.

Appendix B - Incident Categorization

COMMON CATEGORIES OF CYBER INCIDENTS

Incident Type	Type Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a company network, system, application, data, or other resource.
Denial of Service (DoS, DDoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
Improper or Inappropriate Usage	When a person violates acceptable computing policies, including unauthorized access or data theft.
Suspected PII Breach	An incident where it is suspected that Personally Identifiable Information (PII) has been accessed.
Suspected loss of Sensitive Information	An incident that involves a suspected loss of sensitive information (not PII) that occurred because of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) use, where the cause or extent is not known.

Appendix C – Incident Impact Definitions

Security Objective	General Description	Potential Impact Examples		
		Low	**Medium**	**High**
Confidentiality: *Preserving restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*	The unauthorized disclosure of information could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Limited to a single or several Users or computers in an isolated fashion, with easy remediation	Involving or affecting a group of Users, resulting in access to proprietary information. Limited or no external exposure.	A severe breach of proprietary information with external exposure.
Integrity: *Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.*	The unauthorized modification or destruction of information could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Inadvertent or non-malicious alteration or deletion of company data that is easily remediated.	An on-going improper data alteration act (or series of acts) of malicious or negligent nature that will having a moderate business impact.	A massive alteration or destruction of company data of a malicious or obstructive nature.
Availability: *Ensuring timely and reliable access to and use of information systems.*	The disruption of access to or use of information or an information system could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Isolated outage or inaccessibility affecting a limited number of Users for a short amount of time (< 2 hours)	A widespread outage or inaccessibility of a primary business system lasting more than 2 hours, but less than a day	Severe outage or inaccessibility of the company business systems lasting a day or more.

Appendix-D IRT Incident Severity & Response Classification Matrix

Severity Level (5=Most Severe)	Typical Incident Characteristics	Example of Impact	Incident Response	Activate IRT?
5	DDoS attack against on-premise or hosted Servers. Active attacks against network infrastructure. Access to internal company data by nefarious parties.	An enterprise-wide attack involving multiple departments that prevents access to systems and disrupts business operations. Access to or theft of proprietary data.	IRT and the IRM direct response. Remediation coordinated by IT, Forensics, and SME's. Possible Legal Counsel, Law Enforcement involvement	Full Team Active
4	Affects data or services for a group of individuals and threatens sensitive data, or involves accounts with elevated privileges with potential threat to sensitive data	Compromised business application. Improper or unauthorized access to data.	Response coordinated by IRM, IT, and SME's; IRT advised. Legal Counsel specifically notified if there is a PII breach.	Full Team Informed and Advised
3	Affects data or services of a single individual, but involves significant amounts of sensitive data, may include PII.	Employee computer or account with sensitive data access compromised, physical theft of device, unprotected media, or hard copy data.	Response coordinated by IT or IRM, with information sent to the IRT members. Legal Counsel notified if a PII breach	Primary Team Informed
2	Affects data or services of a group of individuals with no sensitive data involved.	Compromise of an account or device with shared folder access.	Response coordinated by IT. IRM advised and IRT informed. IT documentation process used to record findings.	Primary Team Informed
1	Affects data or services of a single individual with no sensitive data beyond them; focus is on correction and future prevention	Compromised computer with no sensitive data etc.	Documentation of issue and findings. Response/remediation coordinated by IT, IRM advised of incident.	No
0	Occurrences of very minor or undetermined focus, origin and/or effect for which there is no practical follow-up	Impaired computer requiring review of system access logs, AV scans, or other repairs.	Documentation through normal IT support processes to record actions and resolution. Reset passwords as needed.	No

Appendix-E IRT Incident Record Form

Incident: _____

Discovery Date: _____

Recorded By: _____ Page _____ of _____ Pages

Recorded Information and Events

Date/Time	Detail

Document Version History

Version	Date	Changes/Notations
1.0	<Insert Release date>	Initial release