Cybersecurity Incident Response Plan

Contents

Change/Review Log 3
1 Purpose 4
2 Applicability 4
3 Contact & Responsibilities 4
4 References 4
4.1 Development References 4
5 Definitions & Acronyms 5
6 Mission Statement for Psinuvia Cybersecurity Incident Response Team (CSIRT) 5
7 Incident Response Life Cycle 6
8 CSIRT Team & Response Plans 8
Detection & Analysis 10
Containment Eradication & Recovery 16
Post-Incident Activity 17

Appendix A: Sample Response Plan Flowchart 18
Appendix B: Threats Scenarios as Identified by Edison Electric Institute (EEI) 19
Appendix C: Impact Classification Matrix 22
Appendix D: Threat Vectors Taxonomy 23

Change/Review Log

Date	Author	Highlight of Changes / Verification of Review

This plan has been reviewed and is current for use in IT security events impacting Psinuvia Inc. It is approved for release and use.

Director IT Security	Date
CISO	Date
CTO	Date

1 Purpose

Computer security incident response has become an important component of IT programs. Performing an incident response is a complex undertaking. Establishing the capability to respond successfully to an incident requires substantial planning and resources. This plan provides standards for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

Annual training and testing, of varying levels of intensity, will be conducted to ensure that the Cybersecurity Incident Response Team (CSIRT) plan remains relevant, specific, and viable in the protection of IT services and the reputation of Psinuvia Inc.

Psinuvia's "Cybersecurity Incident Response Plan" is intended to guide the company's actions for responding to and handling a cybersecurity incident. Psinuvia's management and the CSIRTs may modify incident response activities as needed to address emergency situations or respond appropriately to a particular cybersecurity incident.

2 Applicability

This plan applies to all corporate, business units, field personnel, consultants, contractors, and any third party interacting with the operations, security, and maintenance of all Psinuvia-related computer systems, networks, and IT assets.

3 Contact & Responsibilities

The sponsor for this plan is the chief technology officer (CTO) of Psinuvia. The responsible manager and primary contact for this plan is the director of IT security, who is responsible for the content, distribution, and testing of this plan. Monitoring compliance with the plan is the responsibility of the IT Security Team.

4 References

Development references are documents used to develop this document.

4.1 Development References

[1] **Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). (United States, U.S. Department of Commerce, National Institute of Standards and Technology). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*:*** Assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.
[2] **Homeland Security Incident Handling – Preparing for Incident Analysis:** Homeland Security guidance on security incident handling.
[3] **US CERT – Control Systems Security Program:** U.S. Computer Emergency Response Team guidance for control systems incident response.
[4] **Payment Card Industry (PCI) Data Security Standard; *Requirements and Security Assessment Procedures, version 3.1, April 2015.* Retrieved from: https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf**: Provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing

[5] **Psinuvia Cybersecurity Incident Response Policy:** Outlines the processes for identifying and classifying a cybersecurity incident and the process for responding to a cybersecurity incident.

5 Definitions & Acronyms

Selected terms used in this plan are defined below:

Base lining: Monitoring resources to determine typical utilization patterns so that significant deviations can be detected
Computer security incident: See *incident*
Computer Security Incident Response Team (CSIRT): A capability set up to assist in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center or Computer Incident Response Capability)
Event: Any observable occurrence in a network or system
False positive: An alert that incorrectly indicates that malicious activity is occurring
Forensics: Analysis, containment, and resolution of potential security incidents
IT asset: Any electronic device capable of storing, transmitting, modifying, or routing electronic data. (e.g., smartphones, PDAs, laptops, tablet PCs, network switching and routing devices)
Incident: An event that results in, or presents an imminent threat of, a violation of computer security policies, acceptable use policies, or standard security practices
Incident handling: The mitigation of violations of security policies and recommended practices.
Incident response: See *incident handling*
Indicator: A sign that an incident may have occurred or may be occurring in real time
Intrusion Detection and Prevention System (IDPS): Software that automates the process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents
Malware: A virus, worm, trojan, or other code-based malicious entity that is capable of successfully infecting an IT asset
Precursor: A sign that an attacker may be preparing to cause an incident
Profiling: Measuring the characteristics of expected activity so that changes to it can be more easily identified
Sensitive personal information: An individual's first name or first initial and last name in combination with the following (when either the name or the other data elements are unencrypted):

- Social Security number
- driver's license number or state ID card number
- account number or credit or debit card number

And, when combined with any required security code, access code, or password, would permit access to an individual's financial account; does not include public information that is lawfully made available to the public from the federal, state, or local government
Signature: A recognizable, distinguishing pattern associated with an event, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system
Social engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to profile and/or attack IT assets
Threat: The potential source of an adverse event
Vulnerability: A weakness in a system, application, network, or any IT asset that is subject to exploitation or misuse

6 Mission Statement for Psinuvia's Cybersecurity Incident Response Team (CSIRT)

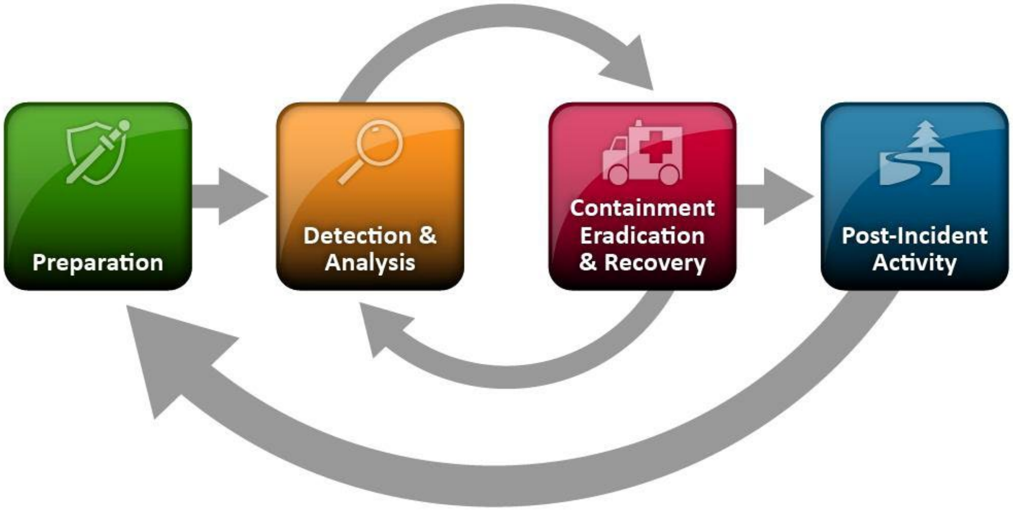
The purpose of the CSIRT is to provide governance of security-related system monitoring, create a discipline of security event monitoring, and demonstrate a coordinated response to events. The CSIRT was established to take proactive measures to protect the environment and develop and publish response procedures of Psinuvia Inc.

The goals of the CSIRT are as follows:

1. Prohibit or remediate unauthorized access or disclosure of confidential data.
2. Maintain and/or restore business continuity.
3. Limit immediate incident impact within Psinuvia's IT environment.
4. Limit immediate incident impact to customers and business partners.
5. Preserve evidence.
6. Perform root cause analysis of qualifying events and determine proactive measures to prevent the event from reoccurring.
7. Determine who or what initiated the incident.
8. Ensure existing policies and standards are followed and updated to prevent further attack.

7 Incident Response Life Cycle

Shown below are the four phases of the "Incident Response Life Cycle" from the National Institute of Standards and Technology's *Computer Security Incident Handling Guide* (Special Publication 800-61 Revision 2)[1]:



Preparation

Although the CSIRT is not typically responsible for incident prevention, it is fundamental to the success of incident response programs. Therefore, incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Specific preparation activities are addressed in corporate policies and are the responsibility of the VP IT Risk, Compliance, and Security Teams for Psinuvia.

[1] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). (United States, U.S. Department of Commerce, National Institute of Standards and Technology). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Detection & Analysis

For many organizations, the most challenging part of the incident response process is accurately detecting and assessing possible incidents, i.e., determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. What makes this so challenging is a combination of three factors:

1. Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based intrusion prevention systems (IPSs), antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.
2. The volume of potential signs of events is typically high; for example, it is not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day. It is important for the CSIRT to assist in the detection of true events by continuing to tune detection methods to eliminate as many benign alerts per day.
3. Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.

Containment, Eradication, & Recovery

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, and disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly.

Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based distributed denial of service (DDoS) attack. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making.

Criteria for determining the appropriate strategy:

- potential damage to and theft of resources
- need for evidence preservation
- service availability (e.g., network connectivity, services provided to external parties)
- time and resources needed to implement the strategy
- effectiveness of the strategy (e.g., partial containment, full containment)
- duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution)

Post-Incident Activities

Post-Incident Activity

One of the most important parts of incident response is also the most often omitted: learning and improving. Each CSIRT should evolve to reflect new threats, improve technology, and lessons learned. Holding a “lessons learned” meeting with all involved parties after a major incident—and periodically after lesser incidents, as resources permit—can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single “lessons learned” meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident.

Questions to be answered in the meeting include the following:

- 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 additional tools or resources are needed to detect, analyze, and mitigate future incidents?

8 CSIRT Team & Response Plans

Preparation

First Responders	**Cybersecurity Operations Center (CSOC)**		
	Role	**Name**	**Cell phone**
	IR manager		
	Alt IR manager		
Internal Communication			
	Role	**Name**	**Cell phone**
	ITCC/Service desk		
Technology Services Extended Team			
	Team Title	**Name**	**Cell phone**
	Disaster Recovery/Data Center Ops		
	Forensics Lead		
	Network Data		
	Technology Service, Risk, & Compliance		

Technology Services		

Technology Services Leadership

Job Title	Name	Cell phone
CTO		
CISO		

Key Internal Contacts

Role	Name	Cell phone
Legal		
Corporate Communications		
External Affairs		
Human Resources		
Physical Security		
Enterprise Risk Management		

Key Vendors

Job Title	Name	Cell phone
Incident Consulting		
Web Host		

Detection & Analysis

Notify Incident Response Core Team Members	The manager of security operations should be informed immediately when an incident has occurred. Sources of notification that an event has occurred can come from any number of sources, but primarily include active monitoring by the IT or security organization, active monitoring by an external organization, notification of problems from internal users, and notification of problems from external partners. Examples include the following: • DDoS detection and prevention • Managed network services • Web Team • Management or employee (CSOC notification though email or phone) • IT Help Desk or IT Security Team • Fraud & Ethics Hotline • Physical security • Government agencies The notification of a security incident triggers the “General Incident Response Plan.”

Investigate Event & Declare Incident	**Event** An event is any observable occurrence in a system or network (e.g., user connecting to a file share, firewall blocking a connection attempt). **Security Incident** A security incident is any unlawful, unauthorized, or unacceptable action that involves a computer system, cell phone, tablet, or any other electronic device with an operating system or that operates on a computer network. Examples: • data theft, including sensitive personal information, email, and documents • theft of funds, including bank access, credit card, and wire fraud • extortion • unauthorized access to computing resources • presence of malware, including remote access tools and spyware • possession of illegal or unauthorized materials **Basic Assessment Questions**: • Has the information been confirmed to be correct and accurate? • Who, what, when, where, why, and how? • What information is available from the firewall, router, server, system, intrusion detection system (IDS), system logs, etc.? • What type of data is involved, and what is its classification? • Are there obscenities, child pornography, or confrontational data? • Is there criminal activity? • Is the data protected by an encryption solution? • What is the magnitude of the systems being impacted? • Is the event still in progress? • Has preliminary containment been performed (i.e., disable account, reset password, remove remote access, isolate device in segregated segment)? • What is the estimated value of the impacted data and systems? Depending on the answers to the assessment questions, the incident response lead will need to determine at this point if the event should be closed as a false positive, worked as an operational security incident, or declared as a significant security incident. The level of impact should be considered when determining if an event will be considered a low security incident or a significant security incident. Once a significant security incident is declared, all further written communications should include “Client Attorney Work Product” in the subject line. All low security incidents will be worked through the routine operational CSOC processes.

Assign Incident Response Manager & Notify Extended Team Members	For each incident, one of the individuals listed as a core team member will be assigned the role of incident response (IR) manager for the CSIRT. The IR manager is the leader of the CSIRT during the entire course of the incident. Depending on the severity of the incident and staff availability, the core team may or may not require all members' participation for the incident. **If declared as an official incident, notify CISO, CTO, and the Legal Department.** The CSIRT extended members include subject matter experts (SMEs) from their respective areas. Depending on the circumstances of the incident, the IR manager will call upon the *essential* extended members to form the CSIRT for that incident. Please note that most events or incidents do not require all extended members. In some situations, additional staff from the extended member area may be needed to facilitate the incident.
Fill Out Incident Report Form & Document Incident	The IR manager should begin filling out the "NOC Reporting Template" and gathering information to document the incident. In some circumstances, the CSIRT will need to tap into external resources for assistance. Usually, the use of external resources will not require disclosure of information related to the incident. However, if divulgence of information related to the incident is required, the Legal Team must be involved and must have executive management approval before the information is released to the external parties.
Review Checklist	The checklist is essential for the incident response process. In times of panic and confusion, the checklist can help to prevent errors. Basic checklist of activities for the CSIRT: 1. Assign the incident response (IR) lead/manager. 2. Fill out an incident response form to record who, what, when, where, why, and how information. Assign a case number using the "location-abbreviated description-year/month/date" nomenclature. 3. Identify the stakeholders. 4. Prioritize tasks at hand. Allocate the appropriate time and effort with regard to the severity of the incident. 5. Set objectives and goals. Safety and preserving human lives should be number one on this list. 6. Formulate probable causes and remediation strategies. 7. Document as much as possible during the incident. 8. Disseminate information on a need-to-know basis.
Maintain Chain of Custody	Maintain a provable "chain of custody" log during the assessment of the situation. Evidence handoffs must be recorded showing storage and transfer of evidence between parties. When turning over evidence to law enforcement, have them sign for it.

<table>
<tr>
<td><b>Evaluate Severity of Incident</b></td>
<td>Evaluate the situation with the preliminary information, and assign an appropriate severity level to the incident based on event type and critical or noncritical asset impacted. As more information becomes available, the incident response lead may promote or demote the status of the severity.
<table>
<tr><th>Severity Type</th><th>Examples</th><th>Initial Response Time</th></tr>
<tr><td>Critical</td><td>• associated with an advanced persistent threat (APT)
• plant control systems compromised
• electronic perimeter breached
• sensitive data compromised
• physical loss of unencrypted sensitive data
• multiple production systems halted
• network outages across the enterprise
• severe damages to Psinuvia’s operations.
• major legal liabilities
• unauthorized use of Psinuvia’s resources to attack external parties
• child pornography involved
• criminal activity (e.g., terrorist attack on system)</td><td>60 minutes</td></tr>
<tr><td>High</td><td>• unsuccessful attempts of compromising sensitive data
• compromise of nonsensitive data
• physical loss of encrypted sensitive data
• higher-than-normal level of intruder scanning and probing activities
• minor production systems halted
• minor network disruptions
• minor damages to Psinuvia’s operations
• limited legal liabilities</td><td>4 hours</td></tr>
<tr><td>Medium</td><td>• physical loss of nonsensitive data
• network disruption, but not at a level that impacts production
• moderate increase from normal level of intruder scanning and probing activities</td><td>48 hours</td></tr>
<tr><td>Low</td><td>• This classification is only used for downgrading from the above severities.</td><td>72 hours</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td><b>Communication Protocol</b></td>
<td>
<table>
<tr><th>Severity Type</th><th>Escalation</th><th>Ongoing Communication Requirement</th></tr>
<tr><td>Critical/High</td><td>Notification given to CISO, CTO, Legal, Security, and applicable management and executive teams</td><td>Incident update sent to appropriate parties:
- a minimum of every two hours during restoration of services
- otherwise daily
- weekly during resolution phase</td></tr>
<tr><td>Medium</td><td>Notification given to CISO</td><td>Incident update sent
- daily during critical phase
- weekly during resolution phase</td></tr>
<tr><td>Low</td><td>Incident leader to update the director of Security Ops</td><td>Incident update sent weekly</td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Escalation</b></td>
<td>Depending on the severity and nature of the incident, the CSIRT may need to escalate the incident to individuals or organizations listed in the “Escalation Path.” If further escalation is needed beyond these individuals or organizations, their respective escalation plans will be executed.

<b>Escalation Path</b>
<table>
<tr><th>Contact</th><th>Name</th><th>Cell Number</th></tr>
<tr><td>CTO</td><td></td><td></td></tr>
<tr><td>CISO</td><td></td><td></td></tr>
<tr><td>Director of Security Ops</td><td></td><td></td></tr>
<tr><td>Legal</td><td></td><td></td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Notification</b></td>
<td><b>Internal:</b> The CSIRT follows the communication protocol listed above.
<b>External</b>: The CSIRT will contact the appropriate individuals to determine the regulatory and legal notification requirements. Depending on the incident, contacting multiple authorities may be required.

Notify Equifax within 72 hours of a confirmed breach.

<b><i><u>Other Notification</u></i></b>
<b>Internal</b>: The CSIRT notifies the need-to-know parties listed in the preparation phase section.
<b>External</b>: The CSIRT will contact the Legal and Regulatory Affairs departments to determine the regulatory and legal notification requirements. Depending on the incident, contacting multiple authorities may be required.</td>
</tr>
</table>

External Disclosure or Notification	The CSIRT will work with the Legal Team to determine if any external disclosure or notification is required. **If an external disclosure or notification communication (regulatory or voluntary) is necessary, it must be approved by the Legal Team, corporate communication, and executive management.**

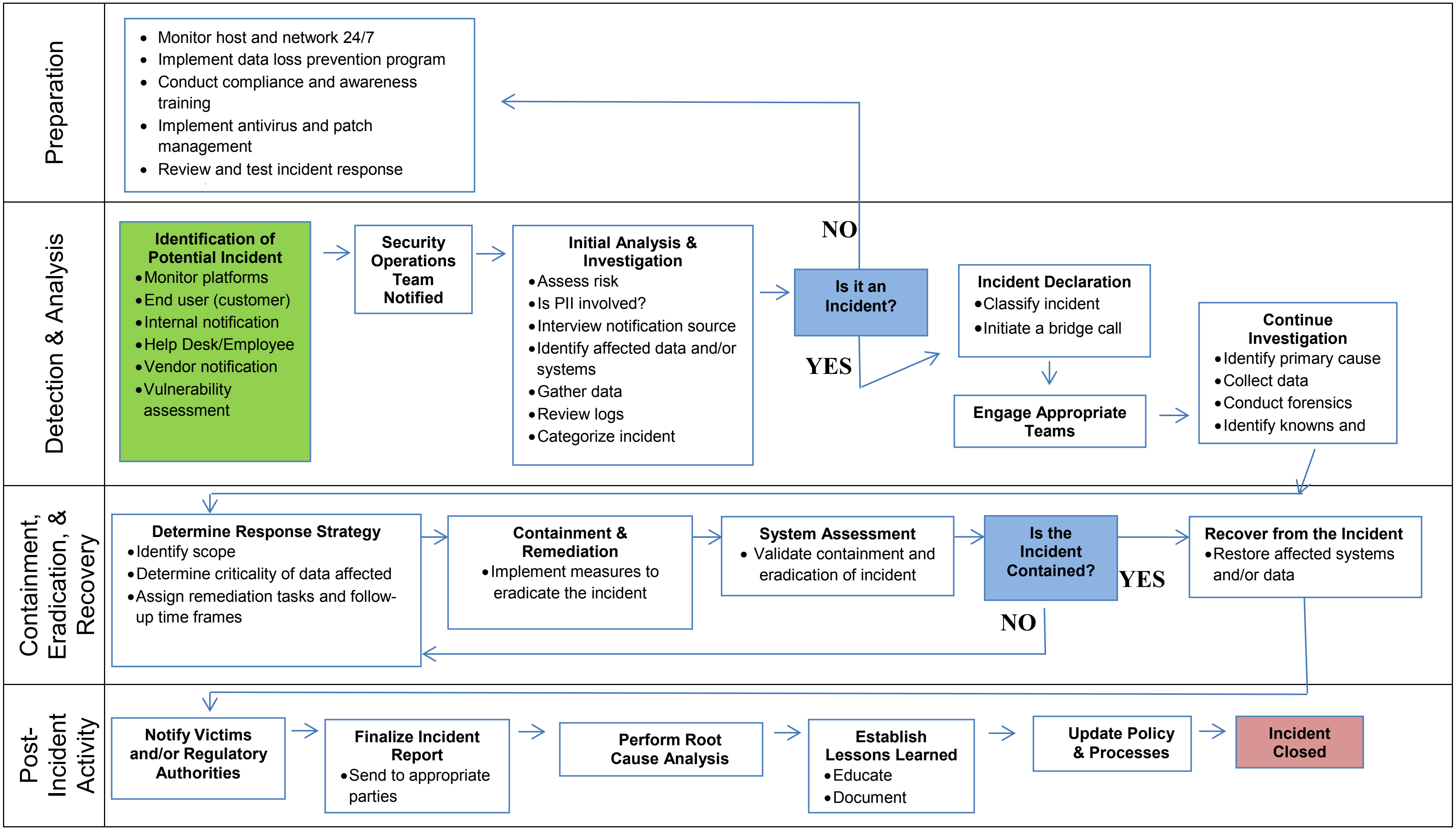
Containment Eradication & Recovery

Develop an Action Plan to Contain the Incident (Remediation)	The CSIRT will need to develop an action plan to contain the incident. The action plan activities must be developed and conducted with minimum impact to the affected assets and production environment in mind. The SMEs from the extended team will be great contributors to the development of the action plan. Things to consider in the action plan: • All changes must follow the production change control process. • If necessary, forensics investigation should be included.
Develop an Action Plan to Eradicate the Incident (Remediation)	Develop an action plan to eradicate the incident by doing the following: • Determine the cause(s) of the incident from the investigation and forensics analysis from the previous phases. • Remove causes of the incident (e.g., personnel, virus, spyware, backdoors etc.). In the case of a compromised system, this may require restoring the system from a recent clean backup or vendor CD-ROMs. • Perform a vulnerability analysis on the environment. • Improve defenses by strengthening administrative controls, physical control, and technology controls. • Move to a new security architecture if necessary.
Test System	In the case of a compromised system, the affected system(s) should be tested and retested before being brought back online.
Validate Business Processes	The CSIRT should validate that all business processes are back to normal conditions through the Business Continuity Team.
Monitor	Continue to monitor the affected system(s) or situation carefully to ensure the security threat is gone.

Post-Incident Activity

Hold Post-Mortem Meeting	Hold a post-mortem (“lessons learned”) meeting with involved parties. Document all lessons learned.
Document Estimated Costs for the Incident	Document the estimated costs incurred to handle the incident. Include hours from all parties involved.
Summarize Recommendations	Summarize recommendations from the team on preventing future occurrences of the incident.
Look for Process Improvement	Look for ways to improve the Incident Response Plan process from the preparation phase through to the recovery phase. Create action plans and communicate the changes to the people who need to know.
Perform Risk Analysis and Document Remediation Plan	If deficiencies are identified in the current processes and/or technologies, escalate the situation to IT Risk Management for risk analysis. The business owner may also need to develop a remediation plan to mitigate the risk of future occurrences. Remediation tasks will be tracked via the normal compliance and remediation tracking process. In the circumstance that the remediation is cost prohibitive or not feasible, the risk exception process will be used to seek management approval of acceptance of the risk.
Finalize Incident Report	Conclude the incident report with the root cause, actions taken, and relevant information. Store all documents in the encrypted incident library.

Appendix A: Sample Response Plan Flowchart



Preparation

- Monitor host and network 24/7
- Implement data loss prevention program
- Conduct compliance and awareness training
- Implement antivirus and patch management
- Review and test incident response

Detection & Analysis

Identification of Potential Incident

- Monitor platforms
- End user (customer)
- Internal notification
- Help Desk/Employee
- Vendor notification
- Vulnerability assessment

Security Operations Team Notified

Initial Analysis & Investigation

- Assess risk
- Is PII involved?
- Interview notification source
- Identify affected data and/or systems
- Gather data
- Review logs
- Categorize incident

Is it an Incident?

Incident Declaration

- Classify incident
- Initiate a bridge call

Engage Appropriate Teams

Continue Investigation

- Identify primary cause
- Collect data
- Conduct forensics
- Identify knowns and

Containment, Eradication, & Recovery

Determine Response Strategy

- Identify scope
- Determine criticality of data affected
- Assign remediation tasks and follow-up time frames

Containment & Remediation

- Implement measures to eradicate the incident

System Assessment

- Validate containment and eradication of incident

Is the Incident Contained?

Recover from the Incident

- Restore affected systems and/or data

Post-Incident Activity

Notify Victims and/or Regulatory Authorities

Finalize Incident Report

- Send to appropriate parties

Perform Root Cause Analysis

Establish Lessons Learned

- Educate
- Document

Update Policy & Processes

Incident Closed

Appendix B: Threats Scenarios as identified by the Edison Electric Institute (EEI)

#1 **Coordinated Cyberattack**	**Definition:** an attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network **Examples:** attack paths via wireless network, remote connections, internet-facing devices, or communication links **Outcomes:** blackouts due to loss of control and/or situational awareness; disruption of communications; breakdown of critical processes; refortification of cyber systems and restoration of public confidence
#2 **Advanced Persistent Threat**	**Definition:** internet-enabled espionage using a variety of intelligence-gathering techniques to access sensitive information; designed to be undetected, establishes a safe area inside the compromised system to allow further access **Examples:** insertion of malicious code, eavesdropping, zero-day vulnerabilities, or spear phishing **Outcomes:** loss of security and control of targeted networks; sensitive data sent out to targeted locations
#3 **Coordinated Physical & Cyberattack**	**Definition:** simultaneous cyber and physical attacks on multiple targets in the electric grid **Examples:** attacks against plants, GCS controls, transformers, and transmission lines **Outcomes:** Prolonged blackouts due to disruption and/or destruction of key power generation facilities, transmission components, communications, and industrial controls; significant repair costs; refortification of physical and cyber systems and restoration of public confidence in a secure and resilient power grid
#4 **Pandemic** **(not for CERT Team)**	**Definition:** Bioterrorism or illness that could make a significant portion of the workforce too ill to work **Examples:** a virus spreading naturally or weaponized by a terrorist group **Outcomes:** loss of critical staff to operate power systems, back office support functions critical to business continuity, and emergency response personnel; risk of accidents or delays in repairs, as well as recovery from other events

#5 Insider Sabotage	**Definition:** threat posed by an employee, former employee, or third-party service provider who is either co-opted by others or is retaliating against Psinuvia **Examples:** social engineering; unauthorized access or misusing legitimate access; man-in-the-middle cyberattacks **Outcomes:** depending on the level of access and knowledge, could cause data loss, disruption of communications, and compromised data
#6 Catastrophic Human Error	**Definition:** unintentional actions and inactions of people that could result in a major failure **Examples:** mistakes in performing a job; misconfiguring equipment; violation of policies due to lack of training or awareness; inadvertently or unwittingly becoming a social engineering target **Outcomes:** customer outages; generators going offline; damage to equipment; introduction of malicious software
#7 Disruption of Voice & Data Services	**Definition**: use of physical or cyberattacks to deny or disrupt communication systems and information required by operators to make good decisions about load balancing or other grid-related processes **Examples:** disruption of control signals and the ability to communicate internally as well as externally **Outcomes:** erroneous decisions that cause the grid to have instability and possible cascading failures; inability of business to function
#8 Supply Chain Disruption	**Definition:** disruption or compromise of the supply of critical equipment, parts, and fuels needed to sustain the electrical grid **Examples:** natural disasters; physical destruction; acquisition of a supplier by a hostile third party; computer appliances that are infected or have security compromised upon arrival **Outcomes:** continuity of operations; recovery from other incidents impacted

#9 **Intentional Electromagnetic Interference**	**Definition:** involves the intentional use of intense electromagnetic fields generated by a repeatable (non-explosive) high-power radio frequency generator, which are directed by an antenna to targets associated with the generation, control, or transmission of electricity **Examples:** penetrating unshielded or poorly protected buildings or conduction through inadequately shielded communication and data lines **Outcomes:** damage or destruction of control systems, transmission systems, etc.
#10 **Distributed Denial of Service** **(DDoS)**	**Definition:** large scale attacks against business systems, internet-facing web servers, or phone systems disrupting corporate operations **Examples:** saturating the target machine with requests that force the machine to reset; slowing traffic to the point where communications are disrupted; can also include inserting malware into the environment (i.e., watering holes) **Outcomes:** disruption of communications and access

Appendix C: Impact Classification Matrix

Impact Classification	Impact Description
Functional Impact	**HIGH:** Organization has lost the ability to provide all critical services to all system users.
	MEDIUM: Organization has lost the ability to provide a critical service to a subset of system users.
	LOW: Organization has experienced a loss of efficiency but can still provide all critical services to all users with minimal effect on performance.
	NONE: Organization has experienced no loss in the ability to provide all services to all users.
Information Impact	**PROPRIETARY:** The confidentiality of proprietary information such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
	PRIVACY: The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
	INTEGRITY: The necessary integrity of information was modified without authorization.
	NONE: No information was exfiltrated, modified, deleted, or otherwise compromised.
Recoverability	**REGULAR:** Time to recovery is predictable with existing resources.
	SUPPLEMENTED: Time to recovery is predictable with additional resources
	EXTENDED: Time to recovery is unpredictable. Additional resources and outside help are needed.
	NOT RECOVERABLE: Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
	NOT APPLICABLE: Incident does not require recovery.

Appendix D: Threat Vectors Taxonomy

Threat Vector	Description	Example
Unknown	Cause of attack is unidentified	The cause (vector) is unknown upon initial report. The threat vector may be updated in a follow-up report.
Attrition	An attack that employs brute-force methods to compromise, degrade, or destroy systems, networks, or services	A denial of service intended to impair or deny access to an application, such as a brute-force attack, is employed against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web-based application	Cross-site scripting attack used to steal credentials; redirection to a site that exploits a browser vulnerability and installs malware
Email	An attack executed via an email message or attachment	Exploit code disguised as an attached document; a link to a malicious website in the body of an email message
External/Removable Media	An attack executed from removable media or a peripheral device	Malicious code spreading onto a system from an infected USB flash drive
Impersonation/Spoofing	An attack involving replacement of legitimate content or services with a malicious substitute	Spoofing, man-in-the-middle attacks, rogue wireless access points, and SQL injection attacks
Improper Usage	Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories	User installs file-sharing software, leading to the loss of sensitive data; user performs illegal activities on a system
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization	A misplaced laptop or mobile device
Other	An attack that does not fit into any other vector	