TEMPLATE

StateRAMP Incident Response Plan (IRP)

Service Provider Name

Information System Name

Version:
X.X

Date:
YYYYMMDD

Prepared by

Identification of Organization that Prepared this Document		
	ORGANIZATION NAME	<Enter Company/Organization>.
	STREET ADDRESS	<Enter Street Address>
	SUITE/ROOM/BUILDING	<Enter Suite/Room/Building>
	CITY, STATE ZIP	<Enter Zip Code>

Prepared for

Identification of Cloud Service Provider		
	ORGANIZATION NAME	<Enter Company/Organization>.
	STREET ADDRESS	<Enter Street Address>
	SUITE/ROOM/BUILDING	<Enter Suite/Room/Building>
	CITY, STATE ZIP	<Enter Zip Code>

Template Revision History

Date	Description
4/6/2021	Original publication

Document Revision History

Date	Description	Version of CMP	Author
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>
<Date>	<Revision Description>	<Version>	<Author>

How to contact us

For questions about StateRAMP, or for technical questions about this document including how to use it, contact *pmo@StateRAMP.org*. For more information about the StateRAMP project, see www.StateRAMP.org

Table of Contents

List of Tables

List of Figures

No table of figures entries found.

Incident Response Plan Approvals

Signature		Signature
Name YYYYMMDD Role System Owner Organization Name		Name YYYYMMDD Role System Owner Organization Name
Signature		**Signature**
Name YYYYMMDD Role System Owner Organization Name		Name YYYYMMDD Role System Owner Organization Name

1 Introduction and Purpose

Information systems are vital to organizational mission/business functions; therefore, it is critical that services provided by {**Organization Name**} are able to operate effectively without excessive interruption. This Incident Response Plan (IRP) establishes the incident response (IR) policies and procedures to ensure that the organization can timely and effectively address computer security incidents that may have compromised sensitive and/or personally identifiable information (PII) or have a serious impact on its ability to accomplish its missions. The IRP also specifies the organizational methods for preparation, detection, analysis, eradication, and containment of an incident. This IRP describes the actions that the IRT will follow upon notification of an incident that could represent, but is not limited to, unauthorized access, alteration or compromise, denial of service (DoS), malicious code, or misuse.

1.1 Applicable Laws and Regulations

The following laws and regulations are applicable to incident planning:

- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Management of Federal Information Resources [OMB Circular A-130]
- Records Management by Federal Agencies [44 USC 31]
- Safeguarding Against and Responding to the Breach of Personally Identifiable Information [OMB Memo M-07-16]

1.2 Applicable Standards and Guidance

The following standards and guidance are useful for understanding incident planning:

- Computer Security Incident Handling Guide [NIST SP 800-61, Revision 2]
- Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach [NIST SP 800-37, Revision 1]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations [NIST SP 800-137]
- Risk Management Guide for Information Technology Systems [NIST SP 800-30, Revision 1]
- Guide to Malware Incident Prevention and Handling [NIST SP 800-83]
- Guide to Integrating Forensic Techniques into Incident Response [NIST SP 800-86, Revision 2]
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities [NIST SP 800-84]

1.3 Information System Name and Identifier

This IRP applies to the {**Information System Name**}, which has a unique identifier as noted in Table 3-1.

Unique Identifier	Information System Name	Information System Abbreviation
	{**Information System Name**}	{**Information System Name**}

Table 1-1. Information System Name and Title

1.4 Scope

This IRP has been developed for the {**Information System Name**} information system, which is classified as a moderate-impact system, in accordance with Federal Information Processing Standards (FIPS) 199. FIPS 199 provides guidelines on determining the potential impact to organizational operations and assets, and individuals through a formula that examines three security objectives: confidentiality, integrity, and availability. The procedures in this IRP have been developed for a moderate-impact system and are designed to address and minimize the impact of security incidents to the system.

This IRP does not include customer responsibilities, which are as listed below:

- Safeguarding of account access (Usernames and password)
- Violations of Acceptable Use Policy (AUP) and Rules of Behavior (ROB) impacting customer data

1.5 System Description

Instructions: Insert from SSP.

1.6 Incident Response Policy

{**Organization Name**}'s {**Information System Name**} Incident Response Policy, dated YYYYMMDD, can be found in Attachment 1 of the {**Information System Name**} System Security Plan (SSP).

1.7 Security Incident Response Capability

This document serves as an addendum to the {**Information System Name**} System Security Plan (SSP). Incident Response (IR) is managed by {**Organization Name**}. This document outlines the process for handling information security incidents related to United States government agencies that are customers of {**Organization Name**}. This plan, including procedures outlined within the plan, apply to all components of the {**Information System Name**} SaaS and are consistent with NIST 800-61, Rev. 2 guidelines.

{**Organization Name**} handles security incidents following implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4 (Recommended Security Controls for Federal Information Systems and Organizations). IR controls are documented in the IR section of the {**Information System Name**} SSP. To implement its policy, {**Organization Name**} maintains a comprehensive IR process containing detailed information on points of contact, response procedures, and training. The incident handling process outlined in this document will be followed in responding to security incidents involving U.S. Government data or systems. Responders should consult this plan and/or supporting {**repository**} for detailed procedures referenced in this document, when needed.

The procedures outlined in this document supplement existing reporting and handling procedures as described in the {**Information System Name**} SSP or in existing {**Organization Name**} IR documentation, except for reporting to customer agencies. This document includes details on the guidelines used by the {**Organization Name**} Incident Response Team for incidents that involve or relate to government customers. Where there is a conflict between existing {**Organization Name**} incident reporting/response procedures and the corresponding procedures contained in this document, the procedures in this document will take precedence for incidents.

{**Organization Name**} role with respect to assisting authorities with satisfying applicable law, regulation, legal process, or enforceable governmental request as referenced in its terms of service is beyond the scope and intent of this document. Inquiries and request of such nature should be directed to the {**Organization Name**} Information System Security Manager (ISSM) or {**Organization Name**} Legal Counsel.

1.8 Incident Response Team Structure

Instructions: Insert hierarchy diagram here.

Figure 1: {**Organization Name**} Incident Response Team Structure

1.9 Incident Response Team Services

- Triage and identification of incident including live response and analysis
- Development of indicators of compromise (IOCs) to be utilized during containment and remediation
- Development of a containment approach and strategy
- Development of remediation/eradication strategy and process
- Develop IR Report that includes investigation findings, investigative steps, containment, and remediation
- Additional remediation recommendations if applicable

1.10 Roles and Responsibilities

As the first responder to all incidents, {**Organization Name**} establishes multiple roles and responsibilities for responding to outages, disruptions, and disasters for the {**Information System Name**}. Individuals who are assigned roles for recovery operations collectively make up the IRT and are trained annually in their duties. IRT members are chosen based on their skills and knowledge.

Role	Responsibilities
IRT Program Manager	• Advise the Help Desk/System Administrator or Network Administrator on any immediate mitigation actions to be taken. • Immediately initiate an Incident/Event Log when a cyber-event/incident is suspected and ensure the documentation of all incidents/events supports technical analysis and legal evidentiary requirements. • Develop, implement, and maintain the IRP and coordinating the IRP with Incident Response Team. • Ensure that the IRT supports and participates in incident response test exercises. • Exercise the IRP on an annual basis, at a minimum. • Update the IRP to incorporate lessons learned from the annual exercise.

Role	Responsibilities
IRT Members	• Verify and identify cyber incidents and events. • Develop and approve triage and incident management mitigation strategies and actions. • Assess the operational impacts of incidents. • Provide subject matter expert guidance and recommendations in the area of individual expertise on specific mitigation and response actions. • Record and maintain a record of all security incidents.
Help Desk	• Receive reports of security events/incidents. • Report all events/incidents to the IRT Program Manager. • Record all events/incidents reported in a log file.
Information System Security Manager (ISSM)	• Oversee all aspects of information security. • Ensure the organization's incident response policy complies with organizational policies, standards, and procedures.
System Administrators	• Coordinate and cooperate with the Incident Response Team on mitigation actions impacting applications, systems, and networks with which the System Administrator interfaces.
Users	• Report all suspicious computer events/incidents to the Help Desk or security officer. • Provide input to an Incident/Event Report Log when suspicious activity is detected, or as directed by the security officer or System Administrator. • Promptly perform mitigation actions directed by the Help Desk or ISSM. • Take only those mitigation actions directed by the Help Desk or ISSM. • Coordinate and cooperate with the Help Desk and ISSM.

Table 4-1. Incident Response Roles and Responsibilities

1.11 Line of Succession & Alternates Roles

{**Organization Name**} sets forth an order of succession to ensure that decision-making authority for the IRP is uninterrupted. Individuals designated as key personnel have been assigned an individual who can assume the key personnel's position if the key personnel are not able to perform their duties. Alternate key personnel are named in a line of succession and are notified and trained to assume their alternate role, should the need arise. The line of succession for key personnel can be found in Appendix A.

1.12 Personnel Security Requirements

All personnel on the Incident Response Team (as well as all corporate employees) are required to complete a background check before employment.

Additional personnel security requirements are outlined in the Personnel Security Family Policy for {**Information System Name**} and the {**Information System Name**} System Security Plan.

1.13 Event and Incident Definitions

All computer security incidents within the {**Information System Name**} environment will be subject to classification. Security incident classification assists {**Organization Name**} management to determine the severity and criticality of the security incident and ensure that the event receives the resource level attention relative to the incident priority. This document uses the terms below to establish consistent communications. For the purposes of this document, their definitions are defined in the table below.

Classification	Definition
Attack Vector	The method or means by which a hacker or unauthorized user can gain access to computer systems or data, such as via email, removable media, web applications, etc.
Event	An occurrence suspected or confirmed not yet assessed, in an information system, network or application that may negatively affect an information system, network, or process, but has not been determined to be an incident
Incident	A violation or imminent threat of a violation of computer security policies, acceptable use policies, standards, or security practices
Indicators of Compromise	A sign that an incident may have occurred or may be currently occurring
Significant Incident	An incident involving an information system or administrative-related policy violation that represents a meaningful threat to the business process and requires immediate leadership notification
Minor Incident	A security-related incident that does not represent a significant threat to the business process and does not require immediate leadership notification
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source
Threat	Any circumstance, event, or person with the potential to adversely impact operations (including mission, functions, image, or reputation), organizational assets, or personnel
Threat Source	The intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally trigger vulnerability. Synonymous with threat agent

Table 4-2. Event and Incident Definitions.

1.14 Incident Criticality and Severity Levels

The criticality classification level list below provides several incident characteristics to assist proper incident classification and prioritization. Moreover, if an incident contains characteristics in several different severity levels, the priority of an incident must reflect the most severe rating possible. The following severity levels are used to classify {**Organization Name**} incidents.

Severity Level	Definition
1	• Unauthorized access, disclosure, or destruction of customer information or data • Disruption of the {Organization Name} system that prevents or impairs customer access to the system (such as a denial of service attack) • Any security violation determined to be a Severity 1 incident must be reported immediately
2	• System, application, or component experiencing an outage that impacts the customer's ability to use the {Organization Name} and therefore causes customer pain. • Suspicious files or malicious code identified on any server within the production environment • Phishing emails sent to/from {Organization Name} internal users or detected on production email servers within the {Organization Name} production environment • Simultaneous logins by the same user from different IP addresses
3	• Improper usage, such as a violation of the Rules of Behavior, or any unauthorized scanning or probing activities • Security vulnerabilities or bugs in {Organization Name} code or software applications used within the production environment that has the potential to be exploited
4	• Any other type of incident not included above

Table 4-3. Incident Classifications

1.15 Incident Handling

Incident response handling is the process of responding to events and incidents that impact the {**Organization Name**} and customer IT environments. {**Organization Name**} has adopted the Incident Handling Checklist per NIST SP 800-61, Revision 2; the major steps to be performed in the handling of an incident contained therein have been incorporated into this IRP. The following phases are used to handle incidents: incident preparation; detection and analysis; containment, eradication, and recovery; and post-incident activities.

During incident investigation and resolution, information about the security event/incident will only be provided to individuals on a need-to-know basis. However, report intake may occur simultaneously, particularly in cases where the preliminary assessment indicates that significant damage to {**Organization Name**} resources may have occurred.

1.16 Preparation

The preparation phase involves establishing and training an incident response team, developing applicable procedures, and acquiring the necessary tools and resources. During preparation, {**Organization Name**} also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented and therefore incident response procedures must be developed.

1.16.1 Incident Response Personnel Training

Personnel training is a key component of maintaining a state of readiness. IRT members are required to take role-specific training as well as undergo tests and exercises on at least an annual basis. The ISSM ensures that IRT members comply with the training requirements, which consists of reviewing the IRP and participating in the IR Test.

1.16.2 Incident Response Tests and Exercises

{**Organization Name**} performs an annual security incident response exercise to test the effectiveness of the incident response process it has established. The annual test consists of scenario-based tabletop exercises that involve members of the Incident Response team and are brainstorming exercises for specific types of incidents. These exercises also provide a mechanism to ensure that personnel with security incident response duties understand the roles, responsibilities, and procedures.

Any process deficiencies that are detected during the exercise are updated and documented in the form of SharePoint entries, which are assigned to the applicable stakeholders. The ISSM has overall responsibility of reviewing the annual incident response test results on an annual basis.

1.17 Detection and Analysis

The incident detection phase for {**Organization Name**} begins when the initiating event occurs and ends when IRT Program Manager creates and/or acknowledges the event in an incident record. Information Security team members become aware of events through monitoring, instrumentation, partners, customers, and inspection. During this phase, the IRT Program Manager will:

- Provide 24/7/365 monitoring and escalation.
- Respond to input sources including the Incident Ticket monitoring or engaged through automated calling mechanisms.
- Acknowledge event in Incident Management {**Information System Name**}.
    - If an event occurs and no incident record exists, then create one.

1.17.1 Generation of Events

Incidents start as events that are identified and escalated through the following sources, including without limitation, the following:

- Automated system alerts via {**SIEM NAME**} Security Incident and Event Monitoring (SIEM)
- Customer reports via the Customer Support Portal or from Customer Support Agents.
- {**Information System Name**} Administrator Incident Reports.

1.17.2 Internal Reporting of Security Events

All {**Organization Name**} personnel are expected to promptly report events when they believe a security-impacting incident has occurred. Examples of such events include, but are not limited to:

- Alerts, notifications, error messages, or other automated warnings that indicate a security incident may have occurred.
- Reports of security incidents received from external parties, including customers, members of the press, or the public.
- Personal observations of anomalies or unexpected events that might indicate a security incident has occurred.
- Indication of virus, malicious software, or hacker activity.

When these events are identified by {**Organization Name**} personnel they are reported via the following mechanisms:

- **Corporate Security and Risk:** {**Organization Name**} employees receive training to report security threats via the {**Input reporting mechanism (Email, Phone)**}. Notifications involving {**Information System Name**} are to be immediately elevated to the ISSM.
- **Incident Management System:** The {**Organization Name**} Incident Management {**Insert Tool Name**} is the tracking tool used by {**Organization Name**} Personnel.
- {**Insert Incident response reporting email address**} {**Team Name**} operates and monitors the Incident Reporting Mailbox. This process is available to non-{**Organization Name**} employees as well.

Incidents may be detected through various automated and manual means such as Intrusion Detection/Prevention Systems (IDS/IPS)'s, antivirus software, log analyzers, user reports, and unusual traffic flows. This section discusses the process by which incidents are detected and analyzed. Common attack vectors have been identified; the threats that have been deemed most relevant to the system are provided in Appendix B, Incident Handling Scenarios and Appendix C, Incident Response Form.

1.17.3 Incident Monitoring

{**Organization Name**} leverages {**SIEM Tool**} as the Security Incident and Event Monitoring (SIEM) solution in the {**Information System Name**} environment. Logs and events are gathered, indexed, and triaged. More information relating to monitoring and incident auditing may be found in the {**Information System Name**} Audit and Accountability Family Policy and Procedures attached to this {**Information System Name**} SSP.

1.17.4 Incident Reporting

Notifications during recovery include problem escalation to leadership and status awareness to system owners, customer agencies, and StateRAMP. This section describes the procedures for handling escalation notices which defines and describes the events, thresholds, or other types of triggers that may be necessary for additional action. **All** security incidents involving Government information or systems must be reported to StateRAMP PMO. Therefore, {**Organization Name**} must report security incidents to customer agencies within 60 minutes.

The information described below is required when notifying a customer agency of an incident:

1. Current level of impact on agency functions or services (Functional Impact). See Table 5-1 below for a list of Functional Impact categories. Specific thresholds for loss-of-service availability (e.g., all, subset, loss of efficiency) must be defined by the reporting organization.

2. Type of information lost, compromised, or corrupted (Information Impact). See Table 5-2 below for a list of Information Impact categories.
3. Estimate of the scope of time and resources needed to recover from the incident (Recoverability). See Table 5-3 below for a list of Recoverability categories.
4. When the activity was first detected.
5. Number of systems, records, and users impacted.
6. Network location of the observed activity.
7. Point of contact information for additional follow-up.

Important: Do not add sensitive personally identifiable information (PII) to incident submissions.

In some cases, it may not be feasible to have complete and validated information prior to reporting. {**Organization Name**} should provide their best estimate at the time of notification and report updated information as it becomes available.

Category	Description
Denial of Critical Services/Loss of Control	A critical system has been rendered unavailable.
Significant Impact to Critical Services	A critical system has a significant impact, such as local administrative account compromise.
Denial of Non-Critical Services	A non-critical system is denied or destroyed.
Significant Impact to Non-Critical Services	A non-critical service or system has a significant impact.
Minimal Impact to Critical Services	Minimal impact but to a critical system or service, such as email or active directory.
Minimal Impact to Non-Critical Services	Some small level of impact to non-critical systems and services.
No Impact to Services	Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
No Impact	Event has no impact.

Table 5-1. Functional Impact Levels for US-CERT Reporting

Note: Incidents may affect multiple types of data; therefore, you may select multiple options when identifying the information impact.

Category	Description
Destruction of Critical System	Destructive techniques, such as MBR overwrite; have been used against a critical system
Core Credential Compromise	Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated
Critical Systems Data Breach	Data pertaining to a critical system has been exfiltrated
Destruction of Non-Critical Systems	Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system

Category	Description
Proprietary Information Breach	The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
Privacy Data Breach	The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised
Suspected but not Identified	A data loss or impact to availability is suspected, but no direct confirmation exists
No Impact	No known data impact

Table 5-2. Information Impact Levels for US-CERT Reporting

Recoverability Level	Description
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly)
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Supplemented	Time to recovery is predictable with additional resources
Regular	Time to recovery is predictable with existing resources

Table 5-3. Recoverability Levels for US-CERT Reporting

The following information should also be included if known at the time of submission:

- Attack vector(s) that led to the incident. See Table 5-4 below for a list of common attack vectors.
- Any indicators of compromise, including signatures or detection measures developed in relationship to the incident.
- Any mitigation activities undertaken in response to the incident.

Attack Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The attack 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.	Denial of Service intended to impair or deny access to an application; a brute force attack 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, or a redirect to a site that exploits a browser vulnerability and installs malware.

Attack Vector	Description	Example
Email/Phishing	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or 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 flash drive.
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection attacks all involve impersonation.
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; or a 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 method does not fit into any other vector	Miscellaneous

Table 5-4. Attack Vectors for US-CERT Reporting

1.18 Incident Analysis

Incident analysis focuses on the application of techniques which may require an in-depth examination of events, alerts, processes, and activities surrounding the incident.

Diagnosis begins when an incident has been assigned a severity and ends when the Reason for Incident (RFI) is understood and documented in the incident ticket. Documenting actions and results during this phase is critical for the incident response report (IRR) analysis.

During this phase, the IRT will:

- Troubleshoot the incident using out-of-band steps.
- Document troubleshooting actions taken and status in the {**Incident Tracking Tool**} entry as each step occurs.
- Document the RFI with as much technical detail as possible in the {**Incident Tracking Tool**} entry when it is understood.

During this phase, the IRT PM will bring in additional technical and business expertise, as needed.

For Security Events:

- Escalate to {**Insert roles**}
- Work with {**Insert roles**} to classify the event based on factual data based on the evidence. Security events are classified as:
  - **False positive** is defined as an event that meets detection criteria but is found to be part of a normal business practice and may need to be filtered. The service team will identify

root cause for false positives and will address them in a systematic way leveraging and fine-tuning them as needed.

- **Security Incident** is defined as an incident which increases the risk that a customer data breach may occur but thus far has not, including violations of security policies, acceptable use policies, or standard security practices.
- **Customer-Reportable Security Incident (CRSI)** is defined as a Security Incident where unlawful or unauthorized access to or use of {**Organization Name**} SaaS resulted in disclosure, modification, or loss of Customer Data.
- **Privacy Incident** is a subtype of Security Incident involving Personally Identifiable Information (PII). Handling procedures are no different than a Security Incident.

For Security Incidents with potential impact to US Federal Customers:

- Alert IRTPM who, in turn, will determine US-CERT notification requirements.

During this phase, the System Administrators will provide technical expertise and troubleshooting support to the IRT.

1.18.1 Possible Security Breach Incident

If, during the diagnosis stage, the IRTPM determines that there exists a possibility of a data breach, the incident is managed with the Security Breach Response sub-process. Breach Incidents **must be formally declared by the {Insert Role}**.

1.19 Containment, Eradication, and Recovery

The primary objectives in executing containment, eradication, and recovery activities are aligned to the incident priority levels. These objectives are to: first and foremost, protect human life and safety; protect sensitive data; prevent system damage; and minimize disruption to computing and administrative resources. During this phase, the Service Team will:

1. Identify and present **mitigation options** to the IRTPM.
    - Mitigation options are emergency actions or temporary short-term actions that can be taken by {Organization Name} security, operations, or the customer to mitigate the issue impact.
        - Mitigation options should be described in the {**Incident Tracking Tool**} Entry.
    - When possible, mitigations should identify automated methods to validate the mitigation is in place.
        - Detection methods should be documented in the {**Incident Tracking Tool**} Entry.
2. Identify and present **long-term repair items** to the IRTPM:
    - Repair items are long-term fixes to ensure the incident does not occur again.
        - Repair items requiring code changes should be tracked in {**Code Development Tool**} and referenced in the {**Incident Tracking Tool**} Entry.
        - Repair items involving configuration changes should be tracked in the {**Incident Tracking Tool**} Entry and the Change Request System.
    - When possible, repair items should identify automated methods to validate the repair is in place.

- Detection methods should be documented in the {**Incident Tracking Tool**} Entry or the bug entry in {**Code Development Tool**}.

During this phase, the IRTPM will:

- Coordinate **mitigation decision-making** regarding implementation and validation strategies.
- Coordinate the **restoration and validation plan.**

For Security Incidents:

- In the event that the security team and the Service Team disagree on the correct course of action, the decision will be escalated to the SP AO.

During this phase, the System Administrators will:

- Assist with the identification and deployment of mitigation options and repair items.
- Validate service restoration through monitoring, partners, and customers.

During this phase, the Help Desk will:

- Validate service restoration.

1.20 Emergency Mitigation Action

During the Diagnose Stage, it may be possible that the IRT identifies an immediate mitigation or containment step to minimize the extent or impact of the incident. The IRTPM, IRT Members, and IT Manager may jointly choose to take immediate emergency mitigation steps provided they have a good understanding of RFI and scope of impact. If the incident is a potential security incident, the IRTPM should be consulted, and steps should be taken to ensure preservation of evidence.

1.21 Customer Impacting or Reported Incidents

For Customer impacting incidents or customer reported incidents (CRIs), the responding support group will resolve the incident and update the status of the incident in {**Incident Tracking Tool**}. The IRTPM has the responsibility to communicate resolution of the issue to the customer.

If this was a security and/or privacy incident, then communications to the customer about the event will be coordinated by the IRPTM and delivered by the MSP team and/or the {**Information System Name**} ISSM. If customer action is required to mitigate or verify fix, the MSP Team is responsible for engaging the customer to close any gaps.

1.21.1 Containment

Containment is important to limit the impact of an incident and prevent increased damage. Upon identification of impacted assets, the assets will be removed from the production Vnets and into a secured group for continued analysis, eliminating the affected machine's ability to communicate with other systems in the production stack. Additional information can be found in the below "Containment & Eradication"table.

1.21.2 Eradication

Eradication consists of determining the cause, eliminating the problem, and closing the point of entry based on the severity level.

Severity Level	Definition
1	• Unauthorized access, disclosure, or destruction of customer information or data • Disruption of the {Organization Name} system that prevents or impairs customer access to the system (such as a denial of service attack) • Any security violation determined to be a Severity 1 incident must be reported immediately
2	• System, application, or component experiencing an outage that impacts the customer's ability to use the {Organization Name} and therefore causes customer pain. • Suspicious files or malicious code identified on any server within the production environment • Phishing emails sent to/from {Organization Name} internal users or detected on production email servers within the {Organization Name} production environment • Simultaneous logins by the same user from different IP addresses
3	• Improper usage, such as a violation of the Rules of Behavior, or any unauthorized scanning or probing activities • Security vulnerabilities or bugs in {Organization Name} code or software applications used within the production environment that has the potential to be exploited
4	• Any other type of incident not included above

Table 5-5. Containment Eradication

1.21.3 Recovery

Recovery consists of restoring the system to the original state, confirming the resumption of normal function, and subsequently validating the clean system. Recovery may also include remediation of vulnerabilities to prevent similar incidents.

During this phase, the IR Team will*:*

- Identify and present **mitigation options** to the IRTPM
  - Mitigation options are emergency actions or temporary short-term actions that can be taken by {**Roles**} or the customer to mitigate the issue impact.
    - Mitigation options should be described in the {**Incident Tracking Tool**}.
  - When possible, mitigations should identify automated methods to validate the mitigation is in place.
    - Detection methods should be documented in the {**Incident Tracking Tool**}.
- Identify and present **long-term repair items** to the Incident Manager:
  - Repair items are long-term fixes to ensure the incident does not occur again.
    - Repair items requiring code changes should be tracked in the appropriate bug tracking system and referenced in the {**Incident Tracking Tool**}.

        - Repair items involving configuration changes should be tracked in the {**Incident Tracking Tool**}.
    - When possible, repair items should identify automated methods to validate the repair is in place.
        - Detection methods should be documented in the {**Incident Tracking Tool**} or the bug.

During this phase, the Incident Manager will:

- Coordinate mitigation decision-making regarding implementation and validation strategies.
- Coordinate the restoration and validation plan.

For Service Level Agreement (SLA) Impacting Incidents:

- Verify service restoration with appropriate personnel.
- Provide current status, impact assessment, and next steps to the Communications Manager.
- Be accountable for calling the incident "recovered."

For Security Incidents:

- In the event that the security team and the Service Team disagree on the correct course of action, the decision will be escalated to the {**Roles**}

During this phase, the Incident Engineer will:

- Assist with the identification and deployment of mitigation options and repair items.
- Validate service restoration through monitoring, partners, and customers.

During this phase, the IR Team will:

- Validate service restoration and other tools, as needed.

During this phase, the Communications Manager will:

- Send final notification to all sources (unless directed otherwise by the Security Incident Manager).

1.22 Emergency Mitigation Action

During the Diagnose Stage, it may be possible that the response team identifies an immediate mitigation or containment step to minimize the extent or impact of the incident. The Incident Engineer, IR Team and Incident Manager may jointly choose to take immediate emergency mitigation steps provided they have a good understanding of RFI and scope of impact. If the incident is a potential security incident, the Security Incident Engineer should be consulted, and steps taken to ensure preservation of evidence.

1.23 Customer Impacting or Reported Incidents

For Customer impacting incidents or customer reported incidents (CRIs), the responding support group will resolve the incident and update the status of the incident in {**Incident Tracking Tool**}. The IRTPM has the responsibility to communicate resolution of the issue to the customer.

If this was a security and/or privacy incident, then communications to the customer about the event will be coordinated and delivered by the IRTPM.

1.24 Post-Incident Activity

Any customer impacting incident that is SLA Impacting for {**Information System Name**} requires an Incident Response Report (IRR) within 14 days of completion of investigation. The IRTPM is accountable for drafting the postmortem and maintaining an inventory of all repair items, their owners, and completion dates. The PIR must contain the following:

- Customer/Business Impact
- Incident Severity
- Root Cause Description
- Repair items
- Timeline
- External Public Statement (if necessary)

The IRP template and documents are available on the {**Information System Name**} {**Document Repository**}

2 Incident Tracking System

Events and incidents are tracked in the {**Incident Tracking Tool**} and escalated as necessary. Incident tickets contain information on the following:

- The current status of the incident (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Impact assessment(s) related to the incident (Root Cause Analysis)
- Contact information for other involved parties (e.g., system owners, system administrators)
- A list of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (e.g., rebuild the host, upgrade an application)

2.1 Auditing

The Incident Manager is accountable for implementation of the incident management process. The following tasks are required at the specified intervals to ensure that compliance requirements are met and that the process is effective. Incident and Key Performance Indicator (KPI) reports will be stored for a defined period of 90 days.

2.2 Coordination and Information Sharing

Cross-organization coordination and information sharing allows CSPs to quickly and efficiently respond to incidents. It is important to maintain symbiotic relationships with other organizations by sharing threat, attack, and vulnerability information; such trusted relationships may be leveraged not only for recommended or tried-and-true solutions, but also for outsourcing IR needs for which in-house resources are not available.

2.3 Plan Distribution and Availability

The availability of the IRP is essential to the success of the incident response efforts. This plan is distributed to all key personnel listed in Appendix A in the secure {**Document Repository**}.

3 APPENDIX

3.1 Appendix A: Key Personnel and Team Members Contact List

Role	Name	Email	Phone

3.2 Appendix B: Incident Handling Scenarios

The following scenarios have been identified to be most relevant to the {Information System Name}:

Incident Type	Examples
Electronic user compromise	• Compromised/stolen/altered data • Theft and use of others' IDs
Website defacement	• Defacement of website(s) • Redirected website(s)
Reconnaissance activity	• Probes/scans • Unauthorized monitoring
Misuse of resources	• Unauthorized use of remote control • Unauthorized use of software • Inappropriate use of email • Unauthorized solicitation • Illegal log-in attempt • Hoaxes • Storage/distribution of illegal software
Malicious code activity	• Worm • Virus • Trojan horse • Rootkit

3.3 Appendix C: Incident Response Form

Contact Information for this Incident	
Name:	
Title:	
Program Office	
Work Phone:	
Mobile Phone:	
Email address:	
Fax Number:	

Incident Description
Provide a brief description:

Impact/Potential Impact Check all the following that apply to this incident
Loss / Compromise of Data Damage to Systems System Downtime Financial Loss Other Organizations' Systems Affected Damage to the Integrity or Delivery of Critical Goods, Services or Information Unknown at this time
Provide a brief description:

Sensitivity of Data/Information Involved	
SENSITIVITY OF DATA	
CATEGORY	EXAMPLE
Public	This information has been specifically approved for public release by the Marketing department managers. Unauthorized disclosure of this information will not cause concerns or issues for {Organization Name}, its customers, or its business partners. Examples are marketing brochures and material posted to {Organization Name}/{Information System Name} web pages. Disclosure of agency information to the public requires the existence of this label, the specific permission of the information Owner, or long-standing practice of publicly distributing this information.
Internal Use Only	This information is intended for use within {Information System Name} and/or between agencies, and in some cases within affiliated organizations, such as business partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for {Organization Name}, its customers, or its business partners. This type of information is already widely distributed within {Organization Name}, or it could be so distributed within the organization without advance permission from the information owner. Examples are an telephone book and most internal electronic mail messages.
Restricted/Confidential (Privacy Violation)	This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need for access may be against laws and regulations, or may cause significant problems for the Company, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information owner. Examples are customer transaction account information and performance evaluation records. Other examples include citizen data and legal information protected by attorney-client privilege.
Unknown/Other	Describe in the space provided

Select the appropriate information category:	
Public Internal Use Only	Restricted / Confidential (Privacy violation) Unknown / Other – please describe:
Provide a brief description of data that was compromised:	

Who else has been notified
Provide Person and Title:

What Steps Have Been Taken So Far	
No action taken System Disconnected from Production Vnet Updated virus definitions & scanned system	Restored backup from ASR Log files examined (saved & secured) Other – please describe:
Provide a brief description:	

Incident Details	
Date and Time the Incident was discovered:	
Has the incident been resolved?	
Vnet Location of the affected systems	
Number of Vnets affected by the incident:	

Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Are non-{Information System Name} systems, such as business partners, affected by the incident? (Y or N – if Yes, please describe)	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

3.4 Appendix E: After-Action Report Template

OBJECTIVE
The strengths and areas for improvement for each core capability aligned to this objective are described in this section.

CORE CAPABILITY STRENGTHS
The [full or partial] capability level can be attributed to the following strengths:

Strength 1:

Strength 2:

Strength 3:

AREAS FOR IMPROVEMENT
The following areas require improvement to achieve the full capability level:

AREA FOR INPROVEMENT 1:
[Observation statement. This should clearly state the problem or gap; it should not include a recommendation or corrective action, as those will be documented in the Improvement Plan.]

REFERENCE:
[List relevant plans, policies, procedures, laws, and regulations, or sections that apply. If no references apply to the observation, it is acceptable to simply list "Not Applicable."]

1. *[Name of the task and the applicable plans, policies, procedures, laws, and regulations and 1–2 sentences describing their relation to the task.]*
2. *[Name of the task and the applicable plans, policies, procedures, laws, and regulations and 1–2 sentences describing their relation to the task.]*

ANALYSIS:
[The analysis section should be the most detailed section of an Observation. Include a description of the behavior or actions at the core of the observation, as well as a brief description of what was discussed, and the implications/consequence(s) noted. If a strength was identified, include any relevant innovative approaches discussed by the exercise participants.]