

Louisiana’s

Cyber State University

 **Cyber Incident Management and Response Plan**

Created: 07.21.2022

[LA CIRP TRAINING TEMPLATE]

PUBLIC

## Overview

Cyber State University (CSU) recognizes the importance of establishing a Cyber Incident Management and Response Plan (CIMRP) capable of timely actions and communications to ensure comprehensive and consistent responses to each Security Event and Cyber Incident.

This document outlines the actions and procedures required for the initial analysis, evidence collection, and classification of any reported Security Events. If any Security Event becomes classified as a “Cyber Incident,” this document further establishes the phases, action items, responsibilities, and documentation required for managing all Cyber Incidents in compliance with the [State’s Information Security Policy](https://www.doa.la.gov/media/wvmhsr1r/infosecpolicy-v-1-0-2.pdf).

## Scope

This plan applies to all networks, devices, and services provided to students, faculty, guests, partners, colleges, departments, or divisions of Cyber State University.

## Approval

The Cyber Incident Management and Response Plan was reviewed, approved, and published on XXXX,XXXX 2022.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jannie Smith,

Chief Information Security Officer (CISO)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Robert J. Palson,

Chief Information Officer (CIO)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mary Winsalot,

Chief Operational Officer (COO)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dr. Ian Freely,

University President

Contents

[Overview 2](#_Toc109256473)

[Scope 2](#_Toc109256474)

[Approval 2](#_Toc109256475)

[Cyber Incident Management by Phase 5](#_Toc109256476)

[Preparation 6](#_Toc109256477)

[Cyber Steering Group (CSG) 7](#_Toc109256478)

[Cyber Incident Response Manager (CIRM) 7](#_Toc109256479)

[Information Collection Requirements 12](#_Toc109256480)

[Security Event Reporting 13](#_Toc109256481)

[Evidence Collection Process 15](#_Toc109256482)

[Identification and Classification 17](#_Toc109256483)

[Identification 17](#_Toc109256484)

[Classification 18](#_Toc109256485)

[Post-Classification Actions 19](#_Toc109256486)

[Containment 20](#_Toc109256487)

[Short-Term Containment 20](#_Toc109256488)

[Root-Cause Analysis 21](#_Toc109256489)

[Long-Term Containment 22](#_Toc109256490)

[Eradication 23](#_Toc109256491)

[Eradication is required when: 23](#_Toc109256492)

[Short Term Recovery 24](#_Toc109256493)

[Long Term Recovery 24](#_Toc109256494)

[Recovering from Complete System Failure 25](#_Toc109256495)

[Critical Post Recovery Actions and Monitoring 25](#_Toc109256496)

[Lessons Learned 26](#_Toc109256497)

[Minimum Topics of Discussion 26](#_Toc109256498)

[Training and Communication 27](#_Toc109256499)

[Testing and Table-Top Exercises 27](#_Toc109256500)

[Volunteers 27](#_Toc109256501)

[Referenced or Supporting Documents 28](#_Toc109256502)

[State Documents 28](#_Toc109256503)

[Federal Documents 28](#_Toc109256504)

[Contacts 30](#_Toc109256505)

[Cyber Steering Group (CSG) Assignments 30](#_Toc109256506)

[Cyber Incident Response Team (CIRT) Assignments 30](#_Toc109256507)

[Federal and State Partners 31](#_Toc109256508)

[Third Parties and Partners 32](#_Toc109256509)

[Incident Response Plan - Revision and Review Log 33](#_Toc109256510)

[REFERENCE FIGURES 34](#_Toc109256511)

[**Figure 1:** 34](#_Toc109256512)

[**Figure 2:** 35](#_Toc109256513)

[**Figure 3:** 36](#_Toc109256514)

[**Figure 4.1:** 37](#_Toc109256515)

[**Figure 4.2:** 38](#_Toc109256516)

[GLOSSARY 39](#_Toc109256517)

## Cyber Incident Management by Phase

**The Plan**

All Cyber Incidents are managed in accordance with a proven programmatic method that follows seven phases in chronological order, which incorporates a Cyber Incident Response Plan:

1. Preparation
2. Identification and Classification
3. Containment
4. Eradication
5. Recovery and Remediation
6. Lessons Learned
7. Continuous Plan Evaluation

**Phase 1**

## Preparation

A Cyber Incident Management and Response Plan requires minimum preparatory actions, absent which a Cyber Incident Response Plan cannot function.

Proper Preparation includes, but is not limited to, the following action items:

* The development, implementation, and on-going maintenance of a formal Cyber [Incident](#_Incident_Response_Plan) Response Plan (CIRP).
* The creation and assignment of named individuals to a Cyber Steering Group (CSG).
* The designation of a Cyber Incident Response Manager (CIRM) to a named individual or entity.
* The creation and assignment of named individuals to a Cyber Incident Response Team (CIRT).
* Establish, document, and maintain Cyber Incident notification procedures.
* Establish, document, and maintain minimum information collection requirements.
* Procure required supplies, tools, technologies, and facilities required to support CIRT standard processes and timely actions.
* Ensure all servers, web applications, workstations, firewalls, and security platforms are implemented and maintained with configurations to produce the required system events and audit logs.
* Ensure alerts are systematically generated for all known critical and high severity threat events (network, server, or workstation) and sent to individuals or partners who are assigned the responsibility for active threat monitoring.
* Create and publish Policy and Procedures for Reporting Security Events to Students, Faculty, and Partners.
* Ensure critical University Services have scheduled backups produced daily and stored completely external to the university or service provider network.

**Critical Note:**

* **System backups used for the Recovery and Remediation phase must be stored offline *prior to* a cyber incident or attack.**

### Cyber Steering Group (CSG)

CSG Core Responsibilities:

* Serve as executive decision-making authority for CSU’s Cyber Incident management and response activities and planning.
* Assigns the responsibility of Cyber Incident Response Manager to a named individual, entity, or organization.
* Serve as the sole approving authority for requested exceptions/deviations to any policy, plan, or procedure that affects this Cyber Incident Management and Response Plan.

CSG Core Members (pre-determined and unaffected by any Security Event or Cyber Incident):

* Chief Operations Officer (COO) (or as designated by the University President)
	+ Considers and evaluates impact of Cyber Incident on current and future operations.
* Chief Information Officer (CIO)
	+ Considers and implements mitigation controls, maintains, and reviews network maps, provides updates and guidance to senior leadership, plans recovery and remediation.
* Chief Legal Officer (likely to be separate from other counsel representing the University)
	+ Provides guidance on impact to regulated data, maintaining confidentiality and privilege, reviewing vendor agreements for outside assistance, control third party communications, and evaluate insurance benefits.
* Public Relations Officer
	+ Manages all external and internal communications according to procedures set forth herein.

### Cyber Incident Response Manager (CIRM)

CIRM Responsibilities:

* Akin to CSG members, the CIRM is pre-determined and unaffected by any Security Event or Cyber Incident.
* Creates, reviews, and finalizes of Cyber Incident Response Report (CIRR).
* Successful coordination and collection of minimum required information requirements.
* Assigns Cyber Incident Handler and activates CIRT.
* Coordinates resources to effectively perform Cyber Incident response phases and tasks.
* Escalates CIRT resource needs and challenges to CSG in a timely manner.
* Facilitates communication needs for CIRT upon notification of the Cyber Incident (conference call, meeting invitations, cell phones, emails, etc.)
* Presents Cyber Incident response report and lessons learned to CSG members.

 **Cyber Incident Response Team** (CIRT)

Unlike the CSG members and CIRM, CIRT personnel are subject to change depending on the Cyber Incident. CIRT personnel are assigned from the applicable operational areas or sections within CSU that correlate to the type or originating point of the Cyber Incident and then tasked with the specific roles and responsibilities as outlined below.

* **Incident Handler**
	+ Assigned as a dedicated resource until Cyber Incident successfully completes all phases.
	+ Follows and verifies that all phases of Cyber Incident Response Plan (CIRP) are successfully completed according to pre-determined processes.
	+ Requires operational knowledge of and administrative rights to the network, systems, and workstation applications.
	+ Logs timeline details and CIRT activities in the Cyber Incident Response Report (CIRR); provides updates to CIRM.
	+ Coordinates with CIRT members to complete each phase of the CIRP.
	+ Responsible for facilitating evidence collection retention and chain of custody.
	+ Assist CIRM with post-Cyber Incident closure activities and the Lessons Learned process.
* **Technical or Process Specialists/Representatives**
	+ Provide support to ClRT when resolving and recovering from Cyber Incidents.
	+ Maintain information systems in a good condition per CSU policy and best practices.
	+ Report any additional information as applicable to CIRM.
	+ Not authorized to share details of any Cyber Incident outside of CIRT without explicit direction from CSG.
* **Asset Owner** (University Leadership or Delegate)
	+ Make decisions related to assets/systems based on CIRM recommendations.
	+ Provide clear overview of potential process impact during CIRT activities.
* **Legal**/**Compliance** (Internal or Outside Counsel)
	+ Provide legal response to a breach including compliance with notification requirements for the PCI DSS, consumer and employee privacy, and third-party concerns, as applicable.
	+ Review and consider potential insurance coverage for Cyber Incident.
	+ Perform due diligence analysis to mitigate liability, identifying reporting obligations, preserve and document evidence collection, determine impact on regulated data, and control external communications to preserve confidentiality and privilege rights.
	+ Consider and/or provide recommendations regarding law enforcement involvement and scope of consent, as applicable.
	+ Examine vendor agreements (as applicable) for potential additional insured status benefits and indemnity obligations; examine terms and conditions for commercial product procurement.

**Note**: Legal or Compliance Resources may be internal or external counsel that is specifically designated by the Asset Owner or as applicable for the impacted Agency or Agencies.

* **Public Relations**
	+ In coordination with Legal and CSG and according to Cyber Incident Notification Procedures outlined in CIMRP:
		- provides all external relations and centralized responses to public entities or additionally identified resources.
		- Answers questions from University faculty, staff, students, and contractors to control information dissemination during and following a Cyber Incident.

 **Cyber Incident Notification Procedures**

A timely, accurate, consistent, and legally compliant notification process is a critical operational requirement of any Cyber Incident management effort. Notifications to regulatory agencies may be required **immediately** following the discovery of a Security Event. Immediate notifications to regulatory agencies are included in the Cyber Incident Notification Procedures below:

Internal Notifications

* Cyber Incidents involving, or potentially involving, Confidential or Restricted Data must be communicated to all applicable CIRT members, including, Legal, Human Resource (HR), and Public Relations contacts, to ensure that appropriate actions are taken in a timely manner.
* Cyber Incidents involving employee information elements require notification to HR, Legal, and CIRM members prior to communicating with potential third parties.
* Progress notifications and applicable updates to CSG will only be sent from the CIRM, or designee.
* Any other notification containing Cyber Incident or investigation details outside of the CIRT is strictly prohibited without prior approval from the CSG.

External Notifications

* External notifications discussed by CIRM with CSG; CSG is deciding authority for releasing information to any party outside of the CSG and CIRT.
* Legal will then determine if there are legal requirements for notifying external parties of the Cyber Incident, whether actual or suspected.
	+ Communications to external parties, regardless of execution of a Confidentiality and Non-Disclosure Agreement, require legal review to determine if information sought to be disseminated is Confidential Information or Restricted Data.
	+ External Communications will only initiate from Legal or Public Relations representatives.
* CIRM, in conjunction with other applicable organizational or CSG members, will determine the need for any external professional services such as forensic analysis, malware detection, etc.
* Depending upon the actual or potential criminal elements of the Cyber Incident, the CIRM, in conjunction with Legal and CSG, will review the need to involve the appropriate State or Federal enforcement Agency.
	+ Crimes involving computers, and particularly, trespass against computers owned or operated by public entities, are found in Title 14, Chapter 1, Part 3, Subpart D (La. R.S. 14:73.1 – La. R.S. 14:73.12).

**Note:** Primary and Secondary **Enforcement Contacts** are listed within the Contacts table **located within the last section of this document**.

Breach Notifications

Depending on the Restricted Data elements impacted by the Security Event or Cyber Incident, CSU may have specific regulatory, legal, or contractual obligations to notify the public, federal or state government, or contractual partners.

Data breach reporting and notification requirements vary depending on the type of data potentially exposed, definition of a “breach” under the applicable law, and (sometimes) open law enforcement investigations.

Within the first initial hour of declared Cyber Incident, the CIRM or designee, in coordination with Legal, will review the need to notify any external entity.

* The CSG will assign an individual within the CIRT to establish and maintain communication with the required Federal Agency or Partner throughout the Cyber Incident.
* If initial notification to a Federal, State, or Partner entity is required, the CIRM will notify and include the CSG.

**Immediate Breach Notifications:**

* **Notification may be required even prior to confirmation of unauthorized access or disclosure.**
	+ Cyber Incidents involving or potentially involving unauthorized disclosure of Federal Tax Information (FTI) requires immediate notification to Treasury Inspector General for Tax Administration (TIGTA) and IRS Office of Safeguards, prior to any internal investigation or Cyber Incident response efforts.
* Consult with Legal regarding nature of Security Event and again, post-classification as Cyber Incident, for other immediate reporting requirements.

**Non-Immediate Breach Notifications:**

* Non-immediate breach notifications often stem from the realize or suspected breach of protected health information or personal identifying information.
* All breach notification requirements, whether to public or regulatory agencies, require analysis by Legal in coordination with CIRM and approval by CSG.
* Breaches of protected health information require reporting to the Secretary for the Department of Health and Human Services within 60 days of breach identification, in accordance with 45 C.F.R. §164.400 *et seq*.
* Breaches of personal identification governed by state law:
	+ La. R.S. 51:3073-3074 require qualifying breaches, as defined under the Louisiana Database Security Breach Notification Act, to provide notification to both the Louisiana Attorney General’s Office and affected Louisiana residents within sixty (60) days of the discovery of a breach. However, pending law enforcement investigations may delay the commencement of that sixty (60) day period.

**Note**: **Federal, State, and Partner entity Contacts are** **located within the last section of this document.**

Recurring CIRT Communication

* Regardless of specific breach notification requirements, the [IRT](#_Definitions) shall remain informed of all currently open Cyber Incidents via the methods established in CIRP.
* The CIRT shall be notified of the status of Cyber Incidents that are currently being investigated.
* The CIRT shall also be notified of the status of currently pending Cyber Incident [remediation](#_Definitions) efforts.

### Information Collection Requirements

Upon initial discovery of a Security Event, minimum details of the event must be recorded for the Cyber Incident Response Manager (CIRM) to classify a Security Event as a Cyber Incident and initiate the Cyber Incident Response Report (CIRR).

**Cyber Incident Response Report (CIRR) Figure 4.1 & 4.2.**

Helpdesk personnel or the System Administrator, as applicable, must collect the following minimum details from the user:

* Date and time of Security Event
* Reporting Party or Source
* Hostname (impacted system)
* IPv4 Network Address (impacted system)
* Username and Email address (of impacted user)
* Short description of Security Event
	+ *Examples: System Generate Alert from Endpoint Detection Software, unexplained curser movement.*

Included as an attachment hereto is a sample Cyber Incident Response Report (CIRR), which is initiated by the CIRM and continuously updated by the Incident Handler throughout the completion of the Phase 6. CIRM finalizes the CIRR and submits to the CSG as the record owner.

### Security Event Reporting

In order to properly facilitate the timely identification of Cyber Incidents, a strategic combination of technical and non-technical [controls](#_Definitions) must be employed to collect and monitor Security Events from the necessary sources.

Without proper preparation, a Security Event or Cyber Incident will go unnoticed and cause greater negative impact to the University, students, partners, or the State. Once an individual becomes aware of a suspected, potential, or actual Security Event, the individual should report the Security Event as outlined below. A graphic depiction of the Security Event alert and notification process is found on **Initial Event Escalation and Incident Notification Path,** [Figure 1](#_REFERENCE_FIGURES)**.**

Internal Security Event Reporting

* **Faculty Members**
	+ End Users
		- Employees report Security Event to supervisors.
		- Supervisors report Security Event to helpdesk.
	+ Helpdesk
		- Helpdesk collects initial basic detail and reports to CIRM, or designee.
	+ System Administrators
		- System Administrator collects only initial basic detail and reports to CIRM, or designee.
* **Students**
	+ Students report Security Events to helpdesk
* **Guests**
	+ Guests report Security Events to helpdesk.

University, Data Owner, or CSG to ensure that contact information for the helpdesk (both email and telephone number) is readily displayed for all types of users in various locations, digitally and/or physically (Example: computer labs, homepage banners).

**Indications of Security Events for Users:**

* **System Generated Alerts**
	+ Endpoint Protection (Antivirus \ EDR)
		- Workstations
		- Servers
			* *Servers should have a differently generated alert format than protected workstations.*
		- Lab Equipment
	+ Firewall Alerts
		- Denied Communication Attempts between Isolated Networks
	+ Intrusion Detection System (IDS)
* **Inoperable applications** (that were previously operable)
* **Any type of abnormal activity**

Immediately following receipt of an internal report of a Security Event, to supervisors or helpdesk, the helpdesk shall assist user with collecting initial minimum information and provide such to the CIRM for analysis and potential classification of a Security Event as a Cyber Incident.

External Security Event Reporting

Security Events may be reported to the University by external parties. These external parties are likely to include, but not limited to the following types of entities:

* **Partners and Service Providers**
	+ Third parties conducting business with the University, shall report Security Events that potentially affect the University. The University shall include a notification requirement that sets forth a specific contact and timeframe for reporting Security Events.
	+ *Examples: managed service providers, telecommunications carriers, other universities.*
* **State Cyber Threat Analysis Center Alert**
* **Federal law enforcement/homeland security agencies**
	+ *Examples: FBI, CISA, and Department of Justice.*
* **Industry-specific Information Sharing Analysis Center/Organizations**
* **Critical Vulnerability/Threat Notice from IT Platform Provider**

### Evidence Collection Process

The final critical element for preparing for a Cyber Incident is documenting the preferences and processes for evidence collection.

Evidence collection process should be used in the initial Event Analysis process as needed, and again thereafter as outlined in the CIRP, or requested by the CIRM.

To ensure proper timely preservation of evidence requires user communication of awareness controls, obtaining evidence collection items, and standardized analysis.

User Awareness Controls

For Security Events involving a potentially compromised system asset, the *user* or system administrator, once aware, must ***refrain*** from the following actions:

* Continuing to use the workstation or server;
* Logging off the server or workstation; and
* Turning off, unplugging, or disconnecting the workstation or server.

Tampering with the server or workstation may erase forensic evidence or impede access thereto.

Evidence Collection Items

A critical component of a documented evidence collection process accounts for obtaining the following evidence collection items from active servers or workstations in a forensically sound and reliable manner:

* Memory Capture
	+ Virtual / Physical
	+ Hosted / Cloud
* Routing Table, ARP Cache, Process Table, Kernel Statistics, Active Connections
* Temporary File Systems, Event Logs, and Application Logs
* Full Disk Capture

Additional evidence collection items may include, but are not limited to:

* Application\Web\Database logs,
* VPN \ Network \ Firewall \ IDS\IPS Logs
* Configuration Records, Application Diagrams, or Network Topologies
* Archival Media or Backups
* Emails

Forensic capturing mechanisms for used for any evidence collection or handling not previously documented in the evidence collection process requires approval by CIRM.

Evidence Analysis

Once collected from the Evidence Collection Items, the CIRT reviews the items to determine the scope and source of the Security Event, as well as determine the likelihood that *Confidential or Restricted Data* was compromised.

The CIRT must use a methodical approach to the analysis, approved by the CIRM, to determine the probability of different conclusions on a scale that ranges from unlikely, to likely, to very likely. It is also possible that the evidence is not sufficient to support any conclusion. *For example, the CIRT may cite the following in the CIRR: “It is unlikely that Restricted Data was manipulated, but likely that Restricted Data was accessible to unauthorized parties.”*

The CIRT should seek to draw conclusions on the particular people, places, items, events, and any relationship between these informational elements when conducting its analysis. Often, this effort will include correlating data among multiple sources. For instance, a network intrusion detection system (IDS) log may link an event to a host, the host audit logs may link the event to a specific user account, and the host IDS log may indicate what actions that user performed.

CIRT shall collect, log, and retain evidence of the Security Event or eventual Cyber Incident based on severity and record the evidence collected and conclusions drawn from the analysis on the CIRR.

**Note:** If unauthorized code or executable files are detected during evidence analysis, it is very likely that the Security Event will be classified as a Cyber Incident in Phase 2, requiring an assignment of severity.

Additional Considerations

An important consideration is how and when the Security Event or Cyber Incident should be contained. Isolating the pertinent systems from external influences may be necessary to prevent further damage to the system and its data or to preserve evidence.

In many cases, the analyst should work with the CIRT to make a term containment decision (e.g., disconnecting network cables, unplugging power, increasing physical security measures, gracefully shutting down a host), which is further referenced in Phase 3.

The organization should also consider in advance the impact that various containment strategies may have on the ability of the organization to operate effectively.  For example, taking a critical system offline for several hours to acquire disk images and other data might adversely affect the ability of the organization to perform its necessary operations.  Significant downtime could result in substantial monetary losses to the organization.  Therefore, care should be taken to minimize disruptions to an organization’s operations.

**Phase 2**

## Identification and Classification

This Phase initiates the Cyber Incident Response Plan. The primary goal of this phase is to ensure all Security Events are identified in a timely manner and consistently analyzed to ensure appropriate classification of Security Events as Cyber Incidents, as applicable. Strict adherence to analysis requirements is critical for accurate classifications.

### Identification

Upon receipt of a [Security Event](#_Definitions) notification, the CIRM or designee, will assess, evaluate for legitimacy by following a documented Security Event to make final determination if the Security Event is classified as a Cyber [Incident](#_Definitions). The CIRM will determine if information beyond that collected as part of the initial information requirement is needed to classify the Security Event as a Cyber Incident. If the CIRM requires more information, the evidence collection process may be initiated to facilitate the capture of the requisite data for the CIRM’s analysis.

A graphic overview of the Initial Security Event Classification Process and Cyber Incident Response Plan Initiation, is illustrated on [Figure 2](#_REFERENCE_FIGURES).

Once a Security Event is classified as a Cyber Incident by the CIRM, the CIRM and CIRT will begin the CIRR and management process starting with assigning an appropriate classification level to the Cyber Incident. The CIRM will further notify the Chief Information Officer (CIO) and initiate the CIRT process.

If the CIRM finds that the Security Event does **NOT** classify as the Cyber Incident, the CIRM shall proceed as follows:

* The CIRM, or designee will determine if the Security Event justifies a formal response.
* If a formal response is **NOT** required: the Security Event information is forwarded to the System Administrator (assigned to the originated department of the University) for resolution and/or support services with the Data Owner.
* If a formal response is required: the CIRM or designee, assigns a Classification level in accordance with the Cyber Incident Classification Matrix.

NOTE:

Identified Security Events that involve any potential University own server or workstation should imitate evidence collection prior to completing identification phase of the CIRP.

### Classification

If the CIRM finds that the Security Event does classify as a Cyber Incident, the CIRM, or designee, shall assess the severity of the Cyber Incident and assign a Classification level in accordance with the Cyber Incident Classification Metrix.

Cyber Incident Severity

Cyber Incidents vary in severity, and some can rise to the level of an emergency. For example, if a Cyber Incident can impact campus safety mechanisms, potentially jeopardizing physical safety (such as, security cameras, fire or smoke alarms), the Cyber Incident is classified as an emergency.

Based on the likelihood of occurrence and the impact to the resources, the CIRM will assign one of four severity classifications to a Cyber Incident.

|  |  |
| --- | --- |
| **Likelihood** | **Impact** |
| Insignificant | Minor | Moderate | Major | Severe |
| Almost Certain | M | H | H | E | E |
| Likely | M | M | H | H | E |
| Possible | L | M | M | H | E |
| Unlikely | L | M | M | M | H |
| Rare | L | L | M | M | H |

Once the CIRM determines the severity of the Cyber Incident, he/she/they will initiate an appropriate response, manage executive communication, and begin mitigation measures.

### Post-Classification Actions

CIRT Assignments

Following classification and determined severity level, the CIRM must identify and assign positions to various members of the Cyber Incident Response Team.

The CIRM must identify and assign a named Incident Handler, who is granted authorization and operational knowledge of the affected or potentially affected network, systems, and workstation applications.

If the Cyber Incident involves the likely or potential unauthorized release of Confidential or Restricted Data, the CIRM shall consult CSG for appropriate legal counsel contact and, as applicable, approve the participation of Human Resources (HR).

Cyber Incident Report and Documentation

The CIRM initiates the Cyber Incident Response Report and provides it to the Incident Handler. The Incident Handler then ensures the CIRR records consistent updates and accurately reflects the progression of the Cyber Incident Response Plan through the remaining phases.

Incident Communication

Once a Cyber Incident is classified, an Incident Handler assigned, and the CIRR initiated, communication flow must begin. The CIRM will immediately send the initially crafted CIRR to the CSG and coordinate with the Incident Handler to ensure that the most recently updated CIRR draft is included with each step in the communication progression.

A graphic depiction of the **Cyber Incident Response Plan and Incident Report Workflow Path** is provided on [Figure 3](#_REFERENCE_FIGURES).

## Containment

**Phase 3**

The primary goal of the Containment phase is to prevent any increase in impact by additional data, system exposure, or the propagation of unauthorized software. Additionally, when possible, the Cyber Incident should be contained in a manner that will allow assigned CIRT resources acceptable time to analyze to determine root cause.

The CIRT, under the direction of the CIRM, shall first initiate Short-Term Containment actions. Once the Short-Term Containment actions are implemented and the root-cause analysis of the Cyber Incident is underway, the CIRM can determine the transition point into Long-Term Containment actions.

Note: The Eradication phase cannot begin until the root-cause analysis is complete.

### Short-Term Containment

Concept

Based on the criticality of the affected system or source, and the likelihood of exploitation of the identified [vulnerability](#_Definitions), the CIRT may work in accordance with [Data Owners](#Data_Owner) and identified Subject Matter Experts to achieve short-term containment. Examples include, but are not limited to, taking backups, isolating backups, preventing network traffic, shutting down [systems](#_Definitions), denying network traffic, and system isolation.

The determination to remove a system from production use may be made by the CIRT in conjunction with the affected Data Owners; however, the CIRT maintains exclusive rights to remove an affected system from production depending on the identified or potential criticality of the Cyber Incident.

Actions

If appropriate, the following actions shall be taken:

* Network Isolation via Firewall or Internal Routers
* Disabling of Account Credentials
* Blocking outbound or inbound traffic via Web Proxy or Intrusion Prevention Systems
* End User Education

### Root-Cause Analysis

Identifying the root cause(s) of a Cyber Incident is important to planning the best response, containment, and recovery actions. Without root cause determination, long-term containment cannot be confirmed and Recovery phase procedures have a high chance of being ineffective and cause organization to incur additional cost, redundant labor, and longer/subsequent operational disruptions.

Root-cause analysis should include but is not limited to, system or application vulnerabilities, system or application misconfigurations, network misconfigurations, breaches of physical security, or other non-technical scenarios.

In conjunction with subject-matter experts, the CIRT shall review all available network, system, database, and application logs to determine the Root Cause of the Cyber Incident. The root cause analysis shall identify the following informational elements:

* Point of Entry or Compromise
* Source (to include user, IP, mac address, email address, etc.)
* Impacted Systems and Applications
* Data Types Accessed, Disclosed, or Modified

Note that some scenarios such as ransomware or extortion threats of system and information destruction may impose a deadline on achieving these objectives, forcing the organization to use incomplete information for the objectives in the recovery.

Additional Considerations

While knowing the full root cause is always desirable, adversaries are incentivized to hide their methods, so discovering the full root cause is unfortunately not always achievable. Therefore, determining two key objections is minimally required prior to determining the recovery strategy:

* Basic knowledge of the adversary’s objective, likely requiring subject matter expert consultation.
	+ *Examples:* *gain access to intellectual property, financial data, customer and partner data, disrupt organization business functions for monetary gain apparent.*
* High confidence in either understanding the technical mechanisms the adversary used to persistently access the environment or confirming non-persistent intent.
	+ It is imperative that the full extent of the Cyber Incident is understood and strong containment mechanisms are in place to confirm that the attackers are no longer present or in control of the IT resources. Most targeted attacks that are part of a large campaign involve multiple types of well-concealed persistence mechanisms.

Note: The identified root-cause analysis must be included in the CIRR and must be specifically reviewed in the Eradication and Lessons Learned phases set forth in this policy.

### Long-Term Containment

Long-Term Containment Concept

* After ensuring the Cyber Incident is contained, the CIRT shall work with Data Owners and Subject Matter Experts to devise a long-term strategy for containment.
	+ *Example***:** *cloning an infected system into a quarantined network for analysis and restoring the compromised system to production use.*
* A system cannot be restored to production until completion of the Eradication phase.

Long-Term Containment Actions

When required, in addition to Short-Term containment actions, the following Long-term containment actions may be required:

* System, Application, or Database Isolation via termination of physical network cable or virtual network interface.
* System, Application, or Database Isolation via host migration to separate Physically isolated Non-Production Network.
* Code Changes/updates in Applications.
* Any additional technical controls approved by the CIRM.

## Eradication

**Phase 4**

The goal of the Eradiation Phase is partially dependent on the results of the root cause analysis. However, the purpose is to ensure that any code, software adaptation, installed application, or system configuration employed by a bad actor or caused by another faulty system element is remediated or removed.

### Eradication is required when:

* Unauthorized Software or Configuration is added to or modified on any system or device either unintentionally or without CSG authorization.
* Confidential or Restricted Data is moved, accessed by an unauthorized party, or replicated to an unauthorized storage location.

An eradication strategy requires a confirmation mechanism to ensure success. The CIRT, in conjunction with system or application owners and relevant subject matter experts, shall work through a formal process to identify and eliminate all components that may have led to the root cause of the Cyber Incident prior to returning an affected system to production use.

[Eradication](#_Definitions) actions may include, but are not limited to:

* **System and Application Patching**
	+ All available, relevant system and application patches must be applied prior to restoring a system to production use.
* **Resetting, Reconfiguring, or Removing User Accounts**
	+ Compromised or potentially compromised [network](#_Definitions), system, or application account passwords shall be disabled until able to be reset.
* **Re-Imaging Compromised Systems or Devices**
	+ If determined to be compromised at the machine-level, the C[IRT](#_Definitions) may require that a system be rebuilt to ensure that all vulnerabilities, unapproved software, or configuration are removed. Re-imaging may include a completely new server, instance of the operating system, and application software.
* **Improving Network Defenses**
	+ The CIRT may require that [network](#_Definitions) [controls](#_Definitions) be re-evaluated depending on the results of the Cyber Incident investigation.

Additional [controls](#_Definitions) may include, but are not limited to firewall rules, intrusion detection/prevention signatures, web application firewalls, web access filters, or host firewall rules.

Recovery and Remediation

**Phase 5**

Before any recovery efforts start, the CIRM should confirm the successfully identification of the root cause(s) of the Cyber Incident, in addition to the successful completion of the Eradication phase. Therefore, the purpose of this phase is to ensure that Eradication in the systems affected by the Cyber Incident is successful. Failure to execute a full and successful Eradication of both root-cause and subsequent impacts of the Cyber Incident prevents returning any affected system to production status.

The goal of the Recovery and Remediation phase is to both restore any impacted technical or operational service and ensure the environmental changes necessary are successfully implemented to prevent a repeat Cyber Incident.

Recovery and Remediation actions should be approached by prioritizing actions into short-term and long-term phases.

For large-scale Cyber Incidents, recovery or remediation may take several months; the intent of short-term actions should be to restore critical services while increasing the security posture with relatively quick (days to weeks) high value changes to prevent future Cyber Incidents.

The long-term recommendations should focus on actions that may require more involved changes or procurement (e.g., infrastructure changes) to keep the entity as secure as possible.

### Short Term Recovery

Based on Root Cause analysis, the following Recovery and Remediation options shall be used:

* Fresh Install and Patched Operating System
* Fresh install and Patched Application
* Modification of impacted control to prevent future Cyber Incident
* Updated Impacted Application to mitigate identified vulnerability
* Implementation of new Information Security controls or technology to prevent subsequent Cyber Incidents
* Not all Cyber Incidents will cause an entity to experience an actual loss in service(s). An entity may also be capable of continuing operations with a brief interruption to non-critical services.

### Long Term Recovery

Upon identification of the root-cause of the Cyber Incident, the CIRT and affected [Data Owners](#Data_Owner) must agree to a long-term resolution. Remediation actions which require further effort, such as the acquisition of new technology, reconfiguration of existing systems and networks, and additional logging, must be formally documented with reasonable timelines established. Such timelines may be dependent on the severity of the Cyber Incident and the likelihood of re-exploitation. All Cyber Incidents must be considered “open” until all members of the CIRT and affected Data Owners agree that all identified corrective measures have been implemented.

In the unlikely event that Long-Term remediation actions cannot be agreed upon, CSG consulting with the CIRM, shall determine the actions required for Long-Term remediation.

### Recovering from Complete System Failure

When/if Complete System Failure is realized or believed imminent, the CIRM must immediately notify the CSG. Together with the CIRM, the CSG will review the University’s Continuity of Operations Plan (COOP) to determine whether the COOP anticipates and prescribes remedial measures for a complete cessation of system services.

If the University COOP ***does*** anticipate Complete System Failure, CSG and CIRM implement the remedial process prescribed in the COOP provided that remedial processes reflect the majority of current system services.

If the University COOP either ***does not*** anticipate the Complete System Failure, ***or*** is too outdated to accurately guide a temporary restoration process, then the following actions are immediately taken under the supervision of the CIRM and with operational support from the CSG:

1. Ensure the status of any current \ viable backups are stored offline / on a physically separate network prior to progressing.
2. Inventory all system assets, such as servers, firewalls, and workstations to determine whether such items contain end-of-life software/operating systems or outdated technology.
3. Assess back-up data sources for potential malware infection and determine data restoration options.
4. Remove all system assets found with end-of-life or outdated technology from network.
5. Identify and procure items required to replace the removed system assets.
6. Restore legacy assets to factory settings with thorough data removal.
7. Develop new image for servers and workstations with updated operating systems, EDR software, and minimum applications (*Examples: Microsoft Office Suite; Adobe products*)
8. Configure firewalls or additional security tools.
9. Bring severs and endpoints online with server connectivity.
10. Load image onto serve and push to workstations.
11. Restore back-up data to server *if applicable.*

Depending upon the severity of the Cyber Incident, root-cause determination, and pervasiveness of any tools, applications, or code utilized by a bad-actor, it may be necessary to instigate Complete System Failure and follow either the COOP remediation process or actions outlined above.

### Critical Post Recovery Actions and Monitoring

Where possible, the CIRT shall implement additional monitoring [controls](#_Definitions) of affected systems for an appropriate period of time after re-entry into production.

* These additional controls include both scheduled one-time events to check system health and new/reconfigured firewalls paired with commercial endpoint detection software.

The CIRT may employ internal Subject Matter Experts or external parties to evaluate implemented [remediation](#_Definitions) efforts. Additionally, the CSG, CIRM, or designee, may periodically re-evaluate the security posture of the affected systems or resources.

## Lessons Learned

**Phase 6**

The goal of the Lessons Learned phase is to identify what happened (in addition to the root cause), determine whether the Cyber Incident was preventable through existing [controls](#_Definitions), and to identify opportunities to improve the cybersecurity posture of the affected area, system, service or network.

Once all Recovery and Remediation activities are complete, all members of the CIRT and any other affected parties will meet to review the results of the investigation to discuss the root cause of the Cyber Incident in accordance with this CIRP.

Separately, but equally important to ensure the effectivity of the response process, the CIRM shall evaluate the effectiveness of this CIRP and recommend any appropriate changes to the CSG.

### Minimum Topics of Discussion

Minimally, the following areas or topics shall be discussed:

* Was this Cyber Incident due to a control failure? If so, how has it been improved to prevent future Cyber Incidents?
* Does the remediation method or newly improved or implemented control impact other operational areas?
* Does it need to impact other areas to address similar risk?
* How could operational processes be improved to identify similar vulnerabilities prior to a Cyber Incident?

**Continuous Plan Evaluation**

**Phase 7**

In order to ensure the Cyber Incident Management and Response Plan (CIMRP) maintains the appropriate support, preparedness, and [awareness](#_Definitions), a commitment to Continuous Plan Evaluation efforts is required.

### Training and Communication

* All University employees, contractors, consultants, temporary employees, and other staff members, receive cybersecurity awareness training upon hire and annually thereafter; this training must include recognizing and reporting protocols for Security Events.
* Applicable CIRT members, and others as warranted, are required to attend Cyber Incident response training on a regular basis on incident response procedures.

### Testing and Table-Top Exercises

* The Cyber Incident Response Plan (CIRP) must be organized by the CIRM, or designee to be tested at least every 12 months basis without prior notification to the remainder of the CIRT. Upon the reasonable discretion of the CIRM, prior notification may be made to the Public Relations contacts so that external parties are not mistakenly notified of the testing.
* Following the test, the CIRM or designee must compile a report to be distributed to the Incident Handler and CIRT with comments that may include:
	+ Was the Cyber Incident responded to following the plan?
	+ Were the appropriate personnel notified internally?
	+ Were the necessary technology resources available as needed?
	+ Was the Cyber Incident contained with the least amount of impact on other systems?
	+ Are there any improvements to be made to the process?

### Volunteers

## Referenced or Supporting Documents

**Links**

### State Documents

* State’s Emergency Operation Plan (EOP)
* <http://gohsep.la.gov/Portals/0/2014_State_EOP_Final_Copy_Updated_1272015.pdf>
* State’s Information Security Policy
* <http://www.doa.la.gov/OTS/InformationSecurity/InformationSecurityPolicy-LA-v.1.0.pdf>

### Federal Documents

* The National Cyber Incident Response Plan (NCIRP)
* <https://www.us-cert.gov/ncirp>
* Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience
* <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

## Contacts

**Call Tree**

### Cyber Steering Group (CSG) Assignments

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Phone** | **Email** |
| **Chief Operations Officer** (COO) |  |  |  |
| **Chief Information Officer** (CIO) |   |  |   |
| **Chief Legal Officer** (CLO) |   |  |  |
| **Public Relations Officer** (PR) |  |  |  |
|  |  |  |  |

### Cyber Incident Response Team (CIRT) Assignments

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Phone** | **Email** |
| **Cyber Incident Response Manager** (CIRM) |  |  |  |
|  |   |  |   |
|  |   |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Note**: (**P**) - **Primary**, (**S**) - **Secondary**, (**T**) - **Tertiary**

### Federal and State Partners

|  |  |  |  |
| --- | --- | --- | --- |
| **Entity** | **Name** | **Phone** | **Email** |
| **Law Enforcement**  |  |  |  |
| **Louisiana State Police** (LSP) | **Cyber Incident Reporting Hotline** | **1-800-434-8007** | LaFusion.Center@la.gov  |
| Cyber Crime Unit (CCU) |  | ccu@la.gov  |
| **State Resources and Agencies** |  |  |  |
| **GOHSEP ESF-17** (ESF17) | Emergency Cyber Management Assistance | 1-800-434-8007 | esf17@la.gov |
| **Office of Technology Services** (OTS) | State’s Information Security Team (IST) | 1-844-692-8019 | InfoSecTeam@la.gov |
| **Federal Agencies** |  |  |  |
| **CISA** (P) | CISA Cyber Incident Hotline | (888) 282-0870 |  |
| **FBI** (P) | FBI New Orleans Field Office | (504) 816-3000 |  |
| **DHSI** (P) | DHSI | (866-347-2423) |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Note**: (**P**) - **Primary**, (**S**) - **Secondary**, (**T**) - **Tertiary**

### Third Parties and Partners

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Phone** | **Email** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Incident Response Plan - Revision and Review Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Date** | **Action** |
| Initial Template |  | 2022.07.21 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### REFERENCE FIGURES

**Figure 1: Initial Security Event Escalation and Incident Notification Path**

 

**Figure 2:**

**Initial Security Event Classification Process and Cyber Incident Response Plan Initiation**



**Figure 3:**

**Cyber Incident Response Plan and Incident Report Workflow Path**



**Figure 4.1:**

**Cyber Incident Response Report (CIRR)** [Template Page01]****

**Figure 4.2:**

**Cyber Incident Response Report (CIRR)** [Template Page02]



### GLOSSARY

**Definitions:**

All definitions contained in the [State of Louisiana’s Information Security Policy](https://www.doa.la.gov/media/wvmhsr1r/infosecpolicy-v-1-0-2.pdf) are incorporated by reference, in addition to the following:

**Asset Owner:** the individual or entity who is tasked with responsibility for the portion(s) of the System affected by Cyber Incident or Security Event.

**Cyber Incident:** An attempted, suspected, or successful unauthorized access, use, disclosure, modification, or destruction of data; interference with information technology operations; or a violation of any End User Agreement. *This is the definition of “Incident” in the State of Louisiana Information Security Policy.*

**Acronyms:**

The following acronyms are used in this document:

|  |  |
| --- | --- |
| **CIMRP:** Cyber Incident Management and Response Report | **EOP:** Parish Emergency Operation Centers |
| **CIO:** Chief Information Officer | **ESF-17:** State of Louisiana Emergency Support Function – 17 (Cyber Incident Management and Response) |
| **CIRM:** Cyber Incident Response Manager | **FBI:** Federal Bureau of Investigation  |
| **CIRP:** Cyber Incident Response Plan | **FTI:** Federal Tax Information |
| **CIRR:** Cyber Incident Response Report  | **GOHSEP:** State of Louisiana Governor’s Office of Homeland Security and Emergency Preparedness |
| **CIRT:** Cyber Incident Response Team | **HR:** Human Resources |
| **CISA:** Cybersecurity and Infrastructure Security Agent | **IDS:** Intrusion Detection System |
| **CISO:** Chief Information Security Officer | **LSP:** Louisiana State Police |
| **CLO:** Chief Legal Officer | **OTS:** Office of Technology Services |
| **COO:** Chief Operations Officer**COOP:** Continuity of Operations Plan | **PCI DSS:** Payment Card Industry Data Security Standard |
| **CSG:** Cyber Steering Group | **TIGTA:** Treasury Inspector General for Tax Administration |
| **EDR:** Endpoint Detection and Response | **USSS:** United States Secret Service |

*NOTE:*

*This document was produced by the State of Louisiana, Office of Technology Services (OTS), Managed Cyber Services for the specific purpose of CIRP plan crafting and training for higher education entities facilitated by the Board of Regents.*

Please contact ESF17@la.gov with any questions, comments, or concerns.



LET’S GO CYBER DAWGS!!

😊