Incident Response Policy and Procedure

Office of Technology Services
Information Security and Compliance
State of Louisiana

Revision: 2.00
Date: July 17, 2024

Table of Contents

Overview

The state of Louisiana's Incident Response Policy and Procedure (IRP) is a critical element to ensure effective priorities and management of an Incident is managed and prioritized as required by the state of Louisiana's Information Security Policy (ISP).

This Incident Response Policy and Procedure clearly outlines required actions in the following; identification, response, remediation, and follow-up to the occurrence. The intent of this policy and procedure is to outline actions performed by the Information Security Team (IST), and respond to security incidents in a timely, efficient manner.

Purpose

The purpose of the IRP is to ensure Incidents are fully documented from declaration through recovery and remediation.

Scope

The scope of the IRP includes Identification and Classification of an Incident; Communication; Investigation and Evidence Collection; Containment; Root Cause Analysis; Eradication; and Recovery and Remediation. All steps of the IRP must be followed, including documentation of Lessons Learned, Continuous Evaluation, and Annual Testing of the policy and procedure.

Procedure

Incident Response is the process of reacting to Information Technology (IT) threats to an organization or entity such as a cyberattack, server downtime, and/or security breach. The seven phases of the Office of Technology Services (OTS) Incident Response Policy and Procedure are detailed below.

Incident Identification and Classification

Upon notification and determination that a Security Event is an Incident, the Chief Information Security Officer(CISO) and Incident Response Team (IRT) will begin the formal Incident management process starting with assigning an appropriate classification level to the Incident.

Classification

- The CISO or designee within the IST will determine if the Security Event does or does not require a formal Incident Response. If a Security Event does require a formal Incident Response, the CISO must be involved and classify the event.
- Security Events that do not require a formal written Incident Response will be forwarded to appropriate staff members from either OTS, or the Agency to ensure that all support services required are rendered.
- Security Events that do require a formal written Incident Response will have its classification level assigned by the CISO according to the Incident Classification Matrix outlined in this policy and procedure.

Classification Criteria

- Classifications are determined by evaluating the likelihood versus potential impact of an Incident.
- The details of Security Incidents, events, or breaches, which must be reviewed thoroughly by the IST before including the CISO, to determine the likelihood of a reoccurrence of the event. The IST should also perform an impact analysis and document the details (criticality of the affected resources and the consequences) of the event.
- The analysis of the likelihood of occurrence and the impact of the affected resources shall result in the assignment of one of four classifications.

Likelihood - shall be determined based on the following criteria:

- **Rare** - Highly unlikely, but may occur in exceptional circumstances.
- **Unlikely** - Event is not expected, and a slight possibility of occurrence may exist. Identified vulnerability or issue may be legitimate; however, compensating controls are in place and make exploitation impossible or unreasonably difficult.
- **Possible** - The event might occur at some time, as there is a history of casual occurrence of the observed behavior.
- **Likely** - There is a strong possibility and expectation of occurrence, or there is a history of frequent occurrence.
- **Almost Certain** - The event is expected to occur in most circumstances, there is a precedent for regular occurrence, and preventative controls are not adequate or in place.

Impact - shall be determined by the associated criticality of affected resources and the following criteria for determining the current or potential severity of the Incident:

- **Insignificant** - Identified risk impacts systems which are non-critical to business functionality, which do not contain Confidential or Restricted Data, and can be replaced with an alternative solution if made unavailable. Examples include printers, multi-function devices, and scanners.
- **Minor** - Identified risk impacts systems which are non-critical to business functionality, which do not contain Confidential or Restricted Data, but cannot be replaced with an alternative solution if made unavailable. Examples include meeting room devices and kiosk stations.
- **Moderate** - Identified risk impacts systems which are non-critical to business functionality but which contain a moderate amount of Confidential or Restricted Data. Examples include end-user computing devices including laptops, tablets, smartphones, and desktop computers.
- **Major** - Identified risk impacts systems which are non-critical to business functionality but contain a large volume of Confidential or Restricted Data. Major criticality may also be assigned to systems which are critical to business functionality but which do not contain Confidential or Restricted Data. Examples include file servers, development and test resources, and business analytics systems.
- **Severe** - Identified risk impacts systems which are critical to agency functionality and contain Confidential or Restricted Data. Exposure of systems determined to be critical may result in severe consequences including loss of Confidential or Restricted Data. Removing the affected resource from production will have a negative impact to agency functionality. Examples include *.laworks.net, external service applications.

Severity

Based on the likelihood of occurrence and the impact to the affected resources, the CISO will assign one of four incident severity classifications to an incident.

Once the Incident Management Team Leader (IMTL) has declared a security incident and its severity level, the Incident Response Leader will initiate an appropriate response for the given incident.

Impact – shall be determined by the associated criticality of affected resources and the following criteria for determining the current or potential severity of the Incident:

- **Low** – One instance of potentially unfriendly activity (e.g., port scan, malware detection, unexpected performance peak, observation of potentially malicious user activity, theft of a device, etc.)
- **Medium** – One instance of a clear attempt to obtain unauthorized information or access (e.g., attempted download of secure password files, attempt to access restricted areas, single computer infection on a non-critical system, successful unauthorized vulnerability scan, etc.) or a repeated or persistent Low Incident. Incidents classified as Medium risk may also include the incidental internal exposure of one employee record. Medium incidents may also include vulnerabilities with a rare rate of occurrence on critical systems, due to either compensating controls, network isolation, or other factors.
- **High** – Serious attempt or actual interruption in availability, or negative impact to confidently or integrity, or Data Breach. (e.g., multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, multiple concurrent infections of systems, successful buffer/stack overflow, successful unauthorized access to systems hosting or transmitting Confidential or Restricted Data, broken lock, stolen papers, etc.) Or; a repeated or persistent Medium Incident. Incidents with a high criticality may include systems with low to moderate criticalities, which are affected by vulnerabilities are most likely to be exploited.
- **Emergency** – Incidents that involve the potential breach of Restricted or Confidential Data. Incidents classified as Emergency risk require immediate attention including the engagement of Data Owners and SMEs to perform short-term containment including taking down potentially compromised systems and applications. Incidents with an emergency criticality are likely to be assets with high criticality to business functionality, affected by threats, and almost certain to occur.

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

Incident Response Team

Service Level Agreement

- Incident Management Service Level Agreements (SLAs) shall be based on the severity classification.
- SLAs shall include metrics for acceptance, containment, and resolution phases of the Incident Management process.
- The IRT leader shall remain aware of pending SLA violations by identifying when a metric is within a specified threshold of violation.

Response Phase	Severity Class	Service Level Objective	Description
Acceptance	Emergency	1 hour (24×7)	Acceptance is the receipt of an incident by the IST. Acceptance includes assigning a criticality level to the Incident and initiating the formal Incident Response Policy and Procedure.
	High	1 business hours	
	Medium	2 business hours	
	Low	8 business hours	
Containment	Emergency	3 hours (24×7)	Containment is the successful implementation of mitigating controls to prevent any possibility of Propagation.
	High	5 hours (24×7)	
	Medium	8 business hours	
	Low	2 business days	
Recovery	Emergency	8 business hours	Resolution is the successful restoration of an affected resource to production use after implementing long-term Corrective actions.
	High	1 business days	
	Medium	3 business days	
	Low	5 business days	

Roles

Individuals from applicable operational areas or sections within OTS and Agencies will have responsibilities assigned as outlined below. This team may be use additional staff as warranted by the specific circumstance of the incident.

The following table notes the individuals and roles comprising the Incident Response Team (IRT).

Group	Roles	Primary	Secondary
Security Steering Group (SSG)	CIO, CISO, and Designees	Derek Williams	Michael Allison
Incident Management Team Lead	CISO	Chase Hymel	Donny Brown Barry Faulk
Incident Management (IMT)	CISO, Data Center Operations (DCO), Applications and Data Management (ADM), Network Services (NS), End User Computing	Joe Lee – DCO Michael Andresen – ADM Catherine Shain – DCO Network Eric Cloud - EUC	Eric Grimmer - DCO Tammy Stalsby – ADM Tonya Monette – DCO NS Debbie Griffith – EUC Donna Roman – EUC Voice Brad Coney - ARM

	(EUC), Agency Relationship Manager (ARM)	Jolene Ardoin –EUC Voice Thomas Allsup – ARM	
IMT– Incident Response Manager (IRM)	IRM - designated by the Incident Response Team Lead	Appointed by the IMTL	Appointed by the IMTL
IMT – Legal	Subject Matter Expert in Legal and Compliance	Stephen Kogos	TBD
IMT – Public Relations	Subject Matter Expert in Public Communications	TBD	TBD
IMT – Human Resources	Subject Matter Expert in HR	Cheryl Shillings	TBD
IRT – Incident Handler	Lead IRT Resource – Assigned Permanently until the Incident is resolved	Appointed by IRTL	Appointed by IRTL
IRT - Investigator	IMT/IRT member	Appointed by IRTL	Appointed by IRTL
IRT – Infosec Specialist	Subject Matter Expert in Information Security	Appointed by IMTL	Appointed by IMTL
IRT – Agency Relationship Manager (ARM)	Appointed by OTS for Service Management for each State Agency	As applicable	As applicable
IRT – Asset Owner / Agency Contact	Effected agency owner or designee, as identified by the ARM	As applicable	As applicable
IRT – Specialist/ SMEs	Subject Matter Expert in OTS Section or Business Services Areas	As applicable	As applicable

Responsibilities

The following provides the list of all primary responsibilities of the roles listed above.

- **Security Steering Group (SSG) Members**
  - Take responsibility for overall incident management and response concept.
  - Approve exceptions/deviations.
  - Make final decisions.
  - Review, update, and approve the IRP annually

- **Incident Management Team (IMT)**
  - In coordination with SSG and IRT, under the guidance of IMT Lead, the IMT manages the incident.

- **IMT Lead (IMTL) [CISO]**
  - Develops and maintains incident management and response capability.
  - Effectively manages identified Security Events, Risks, and Incidents.
  - Performs proactive and reactive measures to reduce information risk to an acceptable level.

- Effectively communicates IRT needs or hurdles to SSG.
- Manages communications outside of IRT resources.
- Appoints Incident Response Manager and Information Security Specialist(s).

- **Incident Response Manger (IRM)**
  - Review the ticket information, incident documentation and any associated events/reports.
  - Appoints Incident Handler.
  - Responsible for creation and updating of Incident Report.
  - Provides direction and manages IRT activities.
  - Coordinates resources to effectively perform incident response tasks.
  - Escalates IRT resource needs, SLA violations, and challenges to IMT in a timely manner.
  - Sets up the communication channels for IRT upon notification of the incident (conference call, meeting, cell phones, emails, etc.)
  - Coordinates the response and investigation phases.
  - Responsible for successful execution of Incident Response Policy and Procedure.
  - Presents incident response report and lessons learned to IMT Leader and SSG members.

- **Incident Handler/Incident Response Team (IRT)**
  - Assigned as a dedicated resource until Incident has successfully completed all phases.
  - Follows Incident Response Policy and Procedure, and Processes as documented.
  - Logs details of IRT activities and provides timely and reoccurring updates to IRM.
  - Verifies all phases of Incident Management Response were successfully completed.
  - Coordinates with IRT members to complete each phase of Incident Response.
  - Responsible for evidence collection retention and chain of custody.
  - Assist IRM with post-incident closure activities and the Lessons Learned process.

- **Agency Relationship Manager (ARM)**
  - Coordinates with IRM and IMTL for any Agency level communication.
  - Identifies Agency contacts or Asset owners.
  - Coordinates any additional Agency resources or Process SMEs as needed by the IRT.

- **Asset Owner (Agency Leadership or Delegate)**
  - Make decisions related to assets/systems when an incident happens, based on IMTL/IRT recommendations.
  - Provide clear overview of potential process impact during IRT activities.

- **Technical or Process Specialists/Representatives**
  - Provide support to IMT or IRT when resolving incidents.
  - Maintain information systems in a good condition per company policy and best practices.
  - Report any additional information as applicable to incident.
  - Not authorized to share details of any incident outside of IRT without explicit direction from IMTL.

- **Legal/Compliance**
  - Provide legal response to a breach including compliance with notification requirements for the Payment Card Industry Data Security Standard (PCI DSS), consumer and employee privacy, third-parties, and additional as required.

- Coordinate with the IMTL and SSG whether general counsel is required for Incidents with legal impacts and ramifications, to include collection of evidence, prosecution of individuals, lawsuits, etc.

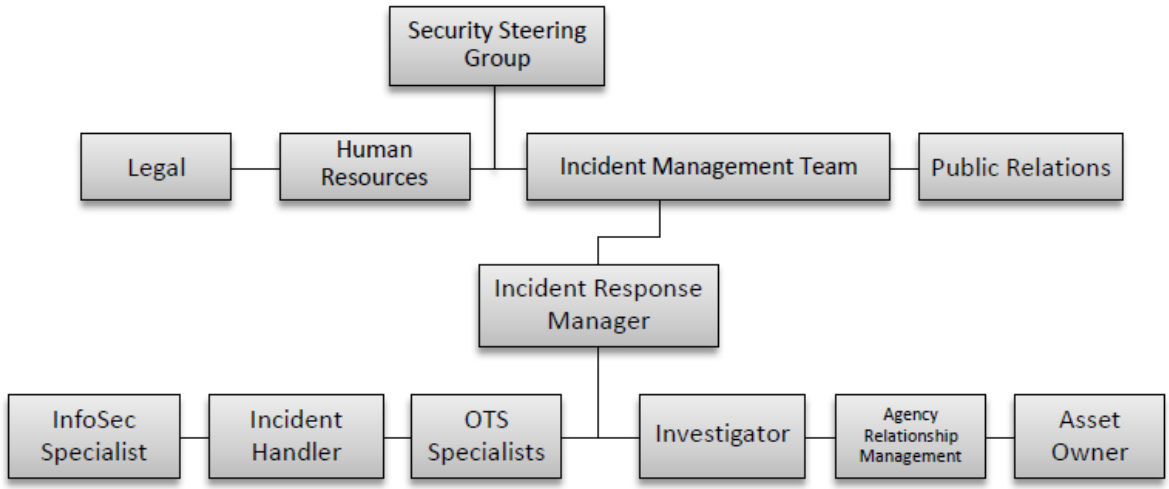
Note: Legal or Compliance Resources may be internal or external counsel that is specifically designated by the Asset Owner or as applicable for the impacted Agency or Agencies.

- **Human Resources**
  - Provide disciplinary or consulting support for instances where an internal employee was the cause of, or impacted by, the Incident.
  - Integrates HR policy to support Incident Management Program.
  - Sanctions to employees found in violation of Acceptable Use or involved in an incident.

- **Public Relations**
  - In coordination with Legal and SSG, provides all external relations and centralized responses to public entities or additionally identified resources.

Organizational Chart

The following provides the list of all primary responsibilities of the roles listed above.



Communications

Timely, accurate, and consistent notification is a critical operational requirement of any Incident Managementeffort and as such, any incident or breach notification must follow the processes outlined below.

Internal Notifications

- Incidents involving, or potentially involving, Confidential or Restricted Data must be communicated to all applicable IRT members, including, Legal, Human Resource, and Public Relations contacts, to ensure that appropriate measures are taken to report the incident both internally and externally.
- Incidents specifically involving employee personally identifiable information (PII) elements will ensure appropriate members of Human Resources are involved prior to any internal or external communication is released.
- Progress notifications and applicable updates to IMT and SSG will only be sent from the IRM.
- Any other notification containing incident or investigation details to resources outside of the IRT is strictly prohibited, without prior approval from the IMTL.

External Notifications

- The IMT will discuss the potential need for external notifications with Legal, Public Relations, and SSG.
- Legal will then determine if there are legal requirements for notifying external parties of the incident, whether actual or suspected.
- Communications sent to any external or public entity (with exception of Partners required for Incident Response activities that have signed a Non-Discloser Agreement) will only initiate from Legal or Public Relations representatives.
- IMT, in conjunction with other applicable organizational or Agency 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 Incident, the IMTL, in conjunction with Legal and SSG, will review the need to involve the appropriate State or Federal enforcement Agency.

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

Breach Notifications

The Breach Notification process will depend on the Agency and Restricted Data elements impacted by the Incident. Each Agency has specific regulatory, legal, or contractual obligations to initially notify a Federal Department or Partner.

- Within the first initial hour of Incident, the IMTL or designee, working with applicable Legal resources, will review the need to notify any external Federal Agency or Agency Partner.
  - If initial notification to a Federal Agency or Partner is required, the IMTL will notify the SSG.
  - The SSG will assign an individual within the IMT to establish and maintain communication with the required Federal Agency or Partner during the course of the Incident.
    Note: Federal Agency and Partner Contacts are listed in the contacts table located within the last section of this document.

  - Incidents involving or potentially involving unauthorized disclosure of Federal Tax Information (FTI) requires immediate notification, but no later than 24 hours after identification of a possible issue involving FTI data, to the local Treasury Inspector General for Tax Administration (TIGTA) Field Division Office, to the Special Agent-in-Charge and to the IRS Office of Safeguards.
- If the organization experiences or suspects a breach or loss of PII or a security incident, which includes Social Security Administration (SSA) provided information, they must notify the State officials responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one hour, the responsible State organization official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 1-877-697-4889 (select "Security and PII Reporting" from the options list). As the final option, in the event SSA contacts and NNSC both cannot be reached, the organization is to contact SSA's Office of Information Security, Security Operations Center at 1-866-718-6425. OTS IST will provide updates as they become available to SSA contact, as appropriate. The link for the worksheet provided in the Memorandum of Understanding (MOU) agreement to facilitate gathering and organizing information about an incident can be found in the ***Reference*** section of this procedure.
- If the organization experiences or suspects a breach or loss of PHI/PII or a security incident, which includes Center for Medicare and Medicaid Services (CMS) provided information, the IMTL or designee must notify the State agency official responsible for Systems Security designated in the agreement. OTS Compliance will notify the designated LDH Legal/Privacy Officer, who is responsible for notifying CMS within one (1) hour.
- If the organization experiences or suspects a breach or loss of Criminal Justice Information Systems (CJIS) data, the IMTL or designee must notify the state CJIS ISO, the state CJIS CSO, and the state CJIS Systems Agency (CSA) the Louisiana State Police. The state CJIS ISO will notify the FBI CJIS ISO within one (1) hour and will remain in communication with the IMT, CSA, CJIS CSO and the FBI CJIS ISO throughout the incident response.
- Any additional required breach notifications will be facilitated by an individual designated by Legal or SSG, working with IMTL or designee.

Investigation and Evidence Collection

Should there be an explicit or implied need to collect evidence the following requirements will apply.

Data Retention

- Retention of audit logs, e-mails, memos, etc. shall be maintained in accordance with State Record Retention Policy.

Chain of Custody

- An accurately maintained Chain of Custody is required when collecting and retaining the following evidence types.
  - Device or System images
  - Drive or Disk captures
  - Forensic System Exports

Required Evidence

- As required by the Incident Management and Response Policy, the following evidence should be collected, based on Incident severity, when available or applicable.
  - Application, System, or Security Logs
  - Applicable Reports
  - Emails (including message headers)
  - Helpdesk Tickets
  - Signed Statements of first-hand accounts

Containment

The primary goal of the Containment phase is to prevent any increase in impact by additional data or system exposure, or allowing any propagation of unauthorized software.

Additionally, when possible, the Incident should be contained in a manner that will allow assigned IRT resources acceptable time to analyze to determine root cause.

Short-term Containment

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

Long-term Containment

When required, in addition to Short-Term Containment options, the following Long-term containment options shall be taken:

- 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 Change in Application
- Any additional technical control approved by the IMTL

Root Cause Analysis

The IRT shall review all available network, system, database, and application logs to determine the Root Cause of the incident.

The Root Cause analyst shall cover the following:

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

Eradication

Depending on the details, cause, and scope of the Incident, eradication may be required. The requirements are applicable under the following conditions.

- Unauthorized Software or Configuration has been added to or modified on any system or device.
- Confidential or Restricted Data has been moved or replicated to an unauthorized storage location.
- If required, an eradication strategy or approach should be used that will also the system to be validated or measure to confirm eradication was successful.

Recovery and Remediation

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

As applicable, 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 incident
- Updated Impacted Application to mitigate identified vulnerability
- Implementation of new Information Security control or technology to prevent Incident

Lessons Learned

Once the Recovery and Remediation phase is complete, the IMTL will schedule a meeting with all IMT and IRT members to discuss the details associated with the Incident.

Minimally, the following areas or topics shall be discussed:

- Was this Incident due to a control failure? If so, how has it been improved to prevent future 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 an incident?

Continuous Evaluation

Training

- All State employees, contractors, consultants, temporary employees, and other staff members, receive security awareness training upon hire and annually thereafter, that includes their responsibilities in notifying the CISO, or designee when they become aware or observe a Security Event.
- Applicable IRT members, and others as warranted, are required to attend incident response training on a regular basis as well as the Incident Response Procedures on an annual basis.

Testing

- The Incident Response Policy and Procedure must be organized by the CISO to be tested at

least every 12 months basis without prior notification to the remainder of the IMT. Upon the reasonable discretion of the CISO, prior notification may be made to the Public Relations contacts so that external parties are not mistakenly notified because of testing.

- Following the test, the IMTL must compile a report to be distributed to the IMT & IRT with comments that may include:
  - Was the incident responded to following the policy and procedure?
  - Were the appropriate personnel notified internally?
  - Were the necessary technology resources available as needed?
  - Was the incident contained with the least amount of impact on other systems?
  - Are there any improvements to be made to the process?

References

NIST Computer Security Incident Handling Guide
OTS Information Security Policy (ISP)

Definitions and Terms

The terms and definitions below are listed for the purpose of this document.

- **Agency** – organizational units within the Louisiana Department of Administration established to provide services to the citizens of Louisiana.
- **ARM** – Agency Relationship Manager – OTS liaison who works with the customer agency.
- **Chain of Custody** – Agency Relationship Manager – OTS liaison who works with the customer agency.
- **CISO** - Chief Information Security Officer
- **Confidential or Restricted Data** – Confidential Data is data that the unauthorized disclosure of could seriously and adversely impact an Agency, third party, suppliers, individuals, or the State of Louisiana. Additionally, Confidential Data has been specifically excluded or granted exemption within the State's Public Records Law. Restricted Data is data that requires strict adherence to legal obligations such as Federal, State, or local law, specific contractual agreements, or data specifically designated as Restricted Data in applicable state or Agency policy. The unauthorized disclosure of Restricted Data is expected to have a severe or catastrophic adverse effect on an Agency, partners, individuals, or the State of Louisiana. Additionally, Restricted Data has been specifically excluded or granted exemption within the State's Public Records Law.
- **Containment** – the third step in the seven-phase Incident Management program. A strategy used to limit the impact of a cyber-attack.
- **Data Retention** – Policies of persistent data and records management for meeting legal and business data archival requirements. Eradication – the fourth step in the seven-phase Incident Management program. This step presents a more permanent fix towards eliminating access points for cyberattack agents.
- **Eradication** – the fourth step in the seven-phase Incident Management program. This step presents a more permanent fix towards eliminating access points for cyber-attack agents.
- **FTI** – Federal Tax Information. Any return or return information received from the IRS or an IRS secondary source, including but not limited to; Federal Office of Child Support Enforcement, Bureau of Fiscal Services, or the Center of Medicare and Medicaid Services.

- **IMT** – Incident Management Team - In coordination with SSG and IRT, under the guidance of IMT Lead, the IMT manages the incident.
- **Incident Handler** – assigned, dedicated resource until Incident has successfully completed all phases.
- **IRT** – Incident Response Team begins the formal Incident management process starting with assigning an appropriate classification level to the Incident. Team of individuals from applicable operational areas or sections within OTS and Agencies that will have responsibilities as assigned. Depending upon the specific incident, this team may use additional staff as warranted.
- **NNSC** – National Network Service Center - incidents involving Social Security data must be reported to the SSA's National Network Service Center.
- **Remediation** – the act of improving or correcting something that is wrong, especially something to change or stop damage to the environment.
- **Risk** - the likelihood of a threat successfully leveraging an identified vulnerability and the level of negative impact on any asset, system, data, or operational process.
- **Root Cause Analysis** – the process of discovering the core issue or highest-level cause of problems.
- **SLA** - Service Level Agreement, a legally binding contract or agreement related to the provision of goods or services that sets forth the terms, expected duties (typically including processing or response time), and responsibilities of the parties.
- **SSA** – Social Security Administration.
- **SSG** – Security Steering Group that takes responsibility for the overall incident management and response concept
- **Threat** - any source of danger that can cause negative impact to an asset, data, and/or business operations (e.g., act of nature, system vulnerability, manmade disasters, hacker, Employee, etc.).
- **TIGTA** – Treasury Inspector General for Tax Administration – any incidents involving FTI must be reported to TIGTA.

Owner

Division of Administration, Office of Technology Services, Information Security

Contact Information:
OTS Information Security Team - InfoSecTeam@la.gov
OTS Information Security Compliance Team – InfoComp@la.gov
OTS User Support - OTSSupport@la.gov

Effective Date: 12/04/2015

Revision History

Version	Date	Description	Author
1.00	09/17/2014	Initial draft for Information Security Workgroup.	Dustin Glover

1.01	06/30/2015	Update format in preparation for adding as Appendix item within the Information Security Policy.	Dustin Glover
1.02	07/29/2015	Review document and update with initial contacts and title updates.	Dustin Glover
1.03	12/04/2015	Remove “draft” reference.	Dustin Glover
1.04	11/28/2021	Review document, update grammar, and add dates.	Paula Sobolewski
1.05	08/30/2023	Updated SSA entry.	Donny Brown
1.06	09/01/2023	Reformatted document with internal standard procedure layout.	Carla Simoneaud
1.06	12/06/2023	Added internal and external contact tables. Updated page numbers in table of contents.	Marnie Cook
1.06	12/12/2023	Reviewed and finalized document.	Carla Simoneaud
1.07	12/28/2023	Updated roles, formatted response phase chart, added phase numbering, edited to match PDF.	Marnie Cook
1.07	01/03/2024	Updated TOC, Purpose, Scope, Roles (Primary and Secondary Contacts) and Definitions.	Susan Eversull
1.07	01/04/2024	Updated other areas based upon requirements. Corrections to spelling and punctuation.	Susan Eversull
1.07	01/22/2024	Updated contacts, reviewed for cleanup.	Susan Eversull
1.07	02/08/2024	Updated CMS Section and CJIS Section; updated contact chart with FBI CJIS.	Susan Eversull
1.07	02/16/2024	Finalized Document.	Susan Eversull
1.07	02/19/2024	Reformatted using new OTS Brand Guide.	Marnie Cook
1.07	02/19/2024	Updated Contact List, need chart on page 11 updated, so that all text shows.	Susan Eversull

1.07	03/11/2024	Updated text and removed highlights.	Susan Eversull
1.07	04/03/2024	Change from Plan to Policy and Procedure	Donny Brown
2.00	04/17/2024	Updated to 2.0, corrected table of contacts, finalized document for signature	Susan Eversull
2.00	07/17/2024	Reviewed and finalized document.	Chase Hymel

Authorization:

DocuSigned by:
Derek Williams
8EDEB93D1FD14E7...

9/26/2024

Derek Williams, State Chief Information Officer — Date

DocuSigned by:
Chase Hymel
FC675CD5A9734DF...

9/26/2024

Chase Hymel, Chief Information Security Officer — Date

Appendix

Contacts (External)

Agency	Name	Phone	Email
Law Enforcement			
FBI – **Cyber Intrusion** (P)	[redacted]	[redacted]	[redacted]
FBI – **Cyber Intrusion** (S)	[redacted]	[redacted]	[redacted]
FBI - CJIS	[redacted]	[redacted]	[redacted]
LA-SAFE (Fusion Center)	[redacted]	[redacted]	[redacted]
LA State Police	**Contact should be coordinated via OTS-ARM assigned to DPS or coordinated via LA-SAFE for incidents requiring escalation or involvement of Louisiana State Police.**		
LA Office of Inspector General	Contact should be coordinated via the SSG for incidents requiring escalation to or involvement of Louisiana's Office of Inspector General.		
Federal Agencies			
IRS (P)	**Office of Safeguards**	n/a	[redacted]
IRS (S)	[redacted]	[redacted]	[redacted]
TIGTA (P)	[redacted]	[redacted]	n\a
TIGTA (S)	[redacted]	[redacted]	n\a
TIGTA (S)	[redacted]	[redacted]	n\a
SSA (P)	[redacted]	[redacted]	n\a
SSA (S)	[redacted]	[redacted]	[redacted]
SSA (T)	[redacted]	[redacted]	n\a

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

Contacts (OTS Internal)

Name	Title	Phone #:	Email
Derek Williams	Chief Information Officer	[redacted]	[redacted]
Michael Allison	Chief Administrative Officer	[redacted]	[redacted]
Chase Hymel	Chief Information Security Officer	[redacted]	[redacted]
Jeremy Deal	Chief Technology Officer	[redacted]	[redacted]
Thomas Allsup	ARM Director	[redacted]	[redacted]
Eric Cloud	EUC Administrator	[redacted]	[redacted]
Joe Lee	DCO Administrator	[redacted]	[redacted]
Michael Andresen	ADM Administrator	[redacted]	[redacted]
Catherine Shain	DCO Network Director	[redacted]	[redacted]

Jolene Ardoin	EUC Voice Director	[redacted]	[redacted]