Overview

The following plan is a critical element for effectively and consistently managing Incident Response as required by the Information Security Policy.

This document clearly outlines the required actions and procedures required for the identification, response, remediation, and follow-up to Incidents, with the intent of responding appropriately and in a timely manner to all Security Events and Incidents.

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 Information Security Team (IST) will determine if the Security Event justifies a formal Incident Response.
- In cases where a Security Event does not require a formal response, it will be forwarded to the appropriate area of OTS or Agency to ensure that all support services required are rendered.
- In cases where a Security Event does require a formal response, the first action will be for the CISO, or designee, to assign a Classification level in accordance with the Incident Classification Matrix outlined below.

Classification Criteria

- Classifications are determined by evaluating the likelihood and potential impact of an Incident.
- The incident must be evaluated by likelihood of occurrence while also evaluating impact (criticality of the affected resources and the consequences) of the exposure.
- 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, but a slight possibility of occurrence may exist. Identified vulnerability or issue may be legitimate; however compensating controls have been implemented 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 IMT Leader has declared a security incident and its severity level, the Incident Response Leader will initiate an appropriate response for the given 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

- **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, either due to 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 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 which are affected by threats which are almost certain to occur.

Incident Response Team

Service Level Agreement

- Incidents Management Service Levels (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 (24x7)	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 plan.
	High	1 business hours	
	Medium	2 business hours	
	Low	8 business hours	
Containment	Emergency	3 hours (24x7)	Containment is the successful implementation of mitigating controls to prevent any possibility of propagation.
	High	5 hours (24x7)	
	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 be assigned responsibilities as outlined below. This team may be supplemented with additional members as warranted by the specific circumstance of the incident.
- The following table notes the individuals and roles comprising the Incident Response Team (IRT).

Position	Roles	Primary	Secondary
Security Steering Group	CIO, & Designees, CISO	**Dickie Howze**	Neal Underwood
Incident Management Team Lead (IMTL)	CISO	**Dustin Glover**	TBD
Incident Management Team (IMT)	CISO, Data Center Operations (DCO), Applications and Data Management (ADM), Network Services (NS), End User Computing (EUC), Agency Relationship Management (ARM)	**Derek Williams** - DCO, **Matt Andresen** - ADM, **Jane Patterson** - NS, **Jeremy Deal** - EUC, **David Moore** - ARM	Joe Lee - DCO, Catherine Shain - NS, TBD
IMT - Incident Response Manager	IRM – Incident Response Team Lead	Appointed by IMTL	Appointed by IMTL
IMT – Legal	Subject Matter Expert in Legal and Compliance	**Veronica Sizer**	TBD
IMT - Public Relations	Subject Matter Expert for Public Communications	TBD	TBD
IMT - Human Resources	Subject Matter Expert in HR Area	**Ron Jackson**	TBD
IRT - Incident Handler	Lead IRT Resource – Assigned permanently until 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 Relations 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, and identified by ARM	As Applicable	As Applicable
IRT - Specialists / SMEs	Subject Matter Experts 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.

- **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 Manger 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 Plan.
  - Presents incident response report and lessons learned to IMT Leader and SSG members.

- **Incident Handler**
  - Assigned as a dedicated resource until Incident has successfully completed all phases.
  - Follows Incident Response Plan 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.

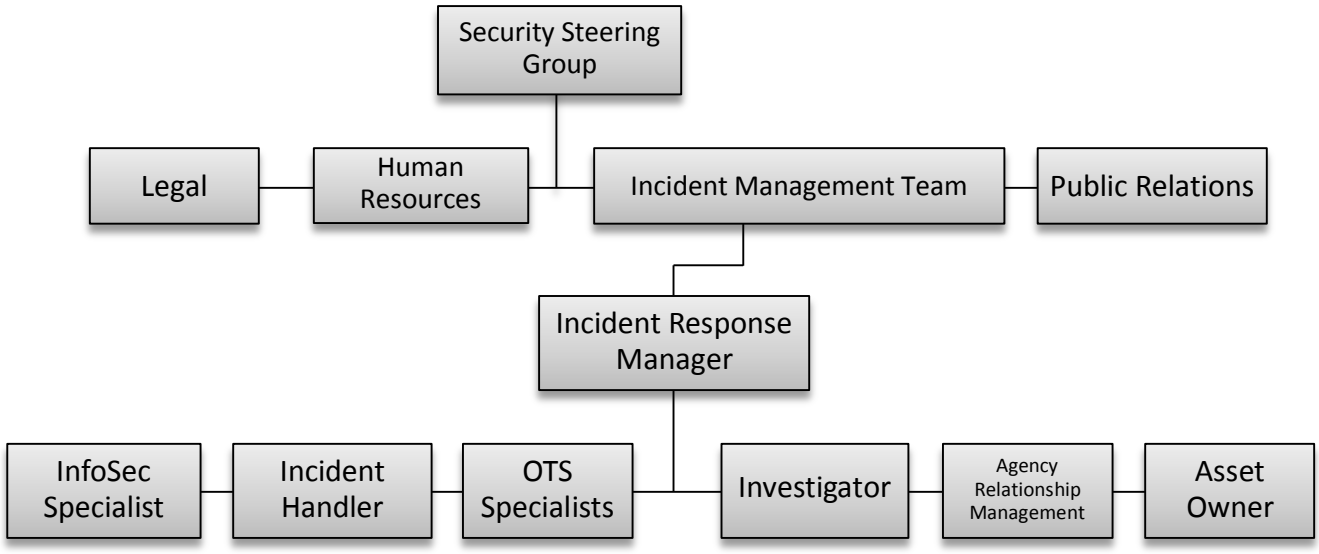
- **Technical or Process Specialists/Representatives**
  - Provide support to lMT or lRT when resolving incidents.
  - Maintain information systems in a good condition per company policy and best practices.
  - Report any additional information as applicable to incident.
  - Not authorized to share details 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 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



Communications

Timely, accurate, and consistent notification is a critical operational requirement of any Incident Management effort 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 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

Depending on the Agency and Restricted Data elements impacted by the Incident, an Agency may have very specific regulatory, legal, or contractual obligations initially notify a Federal Department or Partner.

Notification may be required even prior to confirmation of unauthorized access or disclosure.

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 incident response efforts.**

Breach Notifications (cont.)

- 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 within the Contacts table **located within the last section of this document.**
- 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 maybe required.

Required when:

- 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 on incident response procedures.

Testing

- The incident response plan 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 as a result 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 plan?
    - 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?

Contacts (External)

Agency	Name	Phone	Email
Law Enforcement			
FBI – Cyber Intrusion (P)			
FBI – Cyber Intrusion (S)			
LA-SAFE (Fusion Center)			
LA State Police			
LA Office of Inspector General			
Federal Agencies			
IRS (P)			
IRS (S)			
TIGTA (P)			
TIGTA (S)			
SSA (P)			
SSA (S)			
SSA (T)			

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

Contacts (Internal)

Name	Title	Phone	Email
Dickie Howze	CIO		
Neal Underwood	Dep. CIO		
Dustin Glover	CISO		
Derek Williams	DCO – Director		
Jane Patterson	NS – Director		
Jeremy Deal	EUC – Director		
Michael Andresen	ADM – Director		
David Moore	ARM – Director		

Incident Response Plan - Revision and Review Log

Name	Title	Date	Action
Dustin Glover	CISO	2014 – 09-17	Initial Draft for Information Security Workgroup
Dustin Glover	CISO	2015 – 06-30	Update format in preparation for adding as Appendix Item within the Information Security Policy.
Dustin Glover	CISO	2015 – 07-29	Review document and updated with initial Contacts and title updates
Dustin Glover	CISO	2015 – 12-04	Removed 'Draft'