Information Security

Incident Response Policy & Process

Policy & Process Document

Policy Version 1.7, Process Version 2.8, Date: 9/6/2021

Updated security definitions and policies to align with changes in legal, regulatory, and compliance requirements, as well as best practice improvements.

iCIMS CISO must approve any changes to this document.

I. Contents

1. Document Purpose

1.1. This document defines the policy and process for addressing Security and Privacy Incidents through appropriate Incident Response.

1.2. This document applies to all Personnel and supersedes all other policies relating to the matters set forth herein.

2. Terms & Definitions

Term/Acronym	Definition
Abnormal Activities	Unsuccessful attacks that appear particularly significant based on iCIMS understanding of the risks it faces.
Data Breach	A Security or Privacy Incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, PII or Personal Data transmitted, stored or otherwise processed, or as otherwise defined under applicable legislation, regulation, or similar jurisdictional requirements.
Data Controller	Means the person or organization that determines the purpose and means of the Processing of Personal Data.
Escalation	The engagement of additional resources to resolve or provide the status regarding an incident.
GCO	General Counsel's Office
Incident Record	Created at the time a Security or Privacy Incident is initially recognized. Contains all relevant information pertaining to the Security or Privacy Incident.
Incident Response / Incident Management	Process for detecting, reporting, assessing, responding to, dealing with, and learning from incidents.
Information Security	Preservation of confidentiality, integrity, and availability of information and the equipment, devices or services containing or providing such Information.
Personal Data	Means any information relating, directly or indirectly, to an identified or identifiable PII Principal or individual, where such information is protected under applicable data protection or privacy law.
Personal Identifiable Information (PII)	Any information that (a) can be used to identify the PII Principal or individual to whom such information relates, or (b) is or might be directly or indirectly linked to a PII Principal or individual.
Personnel	iCIMS employees (part and full time) and interns.
PII Principal *(also known as Data Subject)*	A natural person to whom the PII relates.
Privacy Event	A situation where PII or Personal Data is potentially processed in violation of one or more relevant data protection or privacy safeguarding requirements.
Privacy Incident	A situation where PII or Personal Data is processed in violation of one or more relevant data protection or privacy safeguarding requirements.
Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy, a possible exploitation of a Security Vulnerability or Security Weakness or a previously unknown situation that can be security relevant.
Security Incident	A single or series of unwanted or unexpected Security Events that compromise business operations with an impact on Information Security.
Security or Privacy Incident Response Team (SIRT)	A predefined group of individuals needed and responsible for responding to an incident, managed by the Information Security Department. During an incident, the SIRT is responsible for communication with and coordination of other internal and external groups.
Sensitive Personal Information (SPI)	A form of Personal Data and means any information revealing a PII Principal's genetic or biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation and lifestyle, or criminal convictions or offenses
Security Vulnerability	A weakness of an existing asset or control that can be exploited by one or more threats.

Term/Acronym	Definition
Security Weakness	A weakness that results from the lack of an existing, necessary control.
Subscriber Data	Refer to iCIMS Subscription Agreement.
Third Parties	Consultants, vendors, partners, or other contractors of iCIMS that are provided information by iCIMS on a need-to-know basis subject to confidentiality obligations.

3. Policy Scope

The objective of this policy is to ensure a consistent and effective approach to the management of Security and Privacy Incidents, including the identification and communication of Security and Privacy Events and Security Weaknesses.

4. Incident Response Policy

The Incident Response policy is as follows:

- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to Security and Privacy Incidents.

- The objectives for Security and Privacy Incident management should be agreed upon with management, and it should be ensured that those responsible for Security and Privacy Incident management understand the organization's priorities for handling Security Incidents.

- Security and Privacy Events should be reported through appropriate management channels as quickly as possible.

- Personnel and contractors using the organization's information systems and services are required to note and report any observed or suspected Security Weakness or Vulnerability in systems or services.

- Security and Privacy Events should be assessed, and it should be decided if they are to be classified as Security or Privacy Incidents.

- Security and Privacy Incidents should be responded to in accordance with documented Incident Response procedures.

- Knowledge gained from analyzing and resolving Security and Privacy Incidents should be used to reduce the likelihood or impact of future incidents.

- Procedures should be defined and applied for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

- Awareness should be provided on topics such as:

    - The benefits of a formal, consistent approach to Incident Management (personal and organizational)
    - How the program works, expectations
    - How to report Security and Privacy Incidents, who to contact
    - Constraints imposed by non-disclosure agreements.

- Communication channels should be established well in advance of a Security or Privacy Incident. Include all necessary parties in relevant communication:

    - SIRT members
    - Senior Management
    - iCIMS Personnel

- In the event a Security or Privacy Incident, Data Controllers, government bodies, PII Principals, and other necessary parties should be notified in a reasonable timeframe, and in compliance with regulatory and other applicable requirements and guidance.

- At no time should investigations into Security or Privacy Events or Incidents be unreasonably obstructed.
    - Any obstruction of an investigation into a Security or Privacy Event or Incident must immediately be reported to senior leadership for resolution.
    - Obstruction of an investigation may result in disciplinary action, up to and including termination.

5. Process Purpose

5.1. The purpose of this process is to define the Incident Response procedures followed by iCIMS in the event of a Security and Privacy Incident. This document is a step-by-step guide of the measures Personnel are required to take to manage the lifecycle of Security and Privacy Incidents within iCIMS, from initial Security and Privacy Event and Incident recognition to restoring normal operations. This process will ensure that all such Security and Privacy Incidents are detected, analyzed, contained and eradicated, that measures are taken to prevent any further Security and Privacy Incidents, and, where necessary or appropriate, that notice is provided to Personnel, and/or affected parties and law enforcement authorities, if necessary.

5.2. This process applies to all Personnel and supersedes all other procedures, practices, and guidelines relating to the matters set forth herein.

6. Scope

This document covers the Incident Response process for all identified Security and Privacy Incidents. This incident response process is based off 800-61 Rev. 2.

The following activities will be covered:

- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-Incident Activities

The Incident Response process is considered complete once Information confidentiality, integrity, and/or availability are restored to normal and verification has occurred.

7. Overview

7.1. Roles and Responsibilities

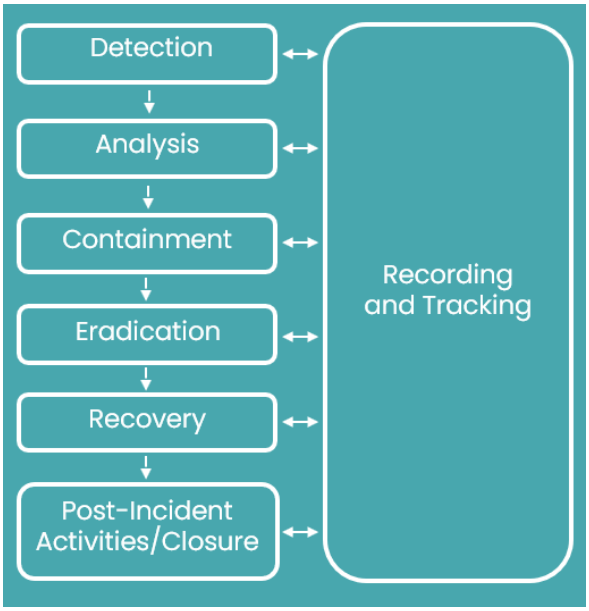
Individuals needed and responsible for responding to a Security or Privacy Incident make up the SIRT. Core members will include the following:

- CISO (SIRT Primary Lead)
- VP, Legal & Compliance, Deputy General Counsel (SIRT Secondary Lead)
- Data Protection Officer (DPO)
- Security team staff
- Privacy team staff
- Information owner

Other groups and/or individuals that may be needed include:

- Senior Leadership
- General Counsel's Office (GCO)
- Human Resources (Talent)
- End User Support
- CTS or Labs Staff
- Building and/or facilities management staff
- Other Personnel involved in the Security or Privacy Incident or needed for resolution
- Contractors (as necessary)
- Communications Resources

Incident Response Process



7.2. Detection Phase

In the Detection Phase the SIRT, or an internal or external entity, identifies a Security or Privacy Event that may be the result of a potential exploitation of a Security Vulnerability or a Security Weakness, or that may be the result of an innocent error.

Immediately upon observation or notice of any suspected Security or Privacy Event, Personnel shall use reasonable efforts to promptly report such knowledge and/or suspicion to the Information Security Department at the following address:

- Email: InformationSecurity@icims.com

A Privacy Event shall also be reported to the following address:

- Email: privacy@icims.com

A Security or Privacy Event may be discovered in many ways, including the following:

- Observation of suspicious behavior or unusual occurrences.
- Lapses in physical or procedural security.

- Information coming into the possession of unauthorized Personnel or Third Parties.
- Information inappropriately exposed on a publicly facing website.

To assess whether a Security or Privacy Event must be reported, Personnel shall consider whether there are indications that:

- Information was used by unauthorized Personnel or Third Parties.
- Information has been downloaded or copied inappropriately from iCIMS' computer systems or equipment.
- Equipment or devices containing Information have been lost or stolen;
- Equipment or devices containing Information have been subject to unauthorized activity (e.g., hacking, malware).
- Personal Data has been inappropriately disclosed, accessed or transferred.

In addition, the following situations shall be considered for Security or Privacy Event reporting:

- Ineffective security controls.
- Breach of information integrity, confidentiality or availability expectations.
- Human errors (innocent or otherwise).
- Non–compliance with policies or standards.
- Breaches of physical security arrangements.
- Uncontrolled systems changes.
- Malfunctions of software or hardware.
- Access violations.

Even if Personnel are not sure whether a Security or Privacy Event is an actual Security or Privacy Incident, they are still required to report it as provided herein, as it is better to be cautious than to be compromised.

The SIRT will usually require the reporter to supply further information, which will depend upon the nature of the Security or Privacy Event. However, the following information normally shall be supplied:

- Contact name and information of person reporting the Security or Privacy Event.
- Date and time the Security or Privacy Event occurred or was noticed.
- Type and circumstances of the Security or Privacy Event.
- The type of data, information, or equipment involved.
- Location of the Security or Privacy Event, data or equipment affected.
- Whether the Security or Privacy Event puts any person or other data at risk; and
- Any associated ticket numbers, emails or log entries associated with the Security or Privacy Event.

SIRT Primary Lead, or the SIRT Secondary Lead if the Primary Lead is unavailable, will ensure that the SIRT is promptly engaged once such notice is received. The following actions will also be taken:

1. The SIRT, under the leadership of the SIRT Primary Lead, shall use reasonable efforts to analyze the matter within four (4) hours of notice and decide whether to proceed with the Analysis Phase of the Incident Response Procedures.
    a. Determination to initiate the Analysis Phase must be made quickly so that Personnel can make an initial determination as to the urgency and seriousness of the situation.
2. Upon making the decision to begin the Analysis Phase, if the SIRT suspects that the Security or Privacy Event may result in damage to the reputation of iCIMS or legal liability, the GCO shall initiate a legal assessment of actual or potential legal issues.

7.3. Analysis Phase

The initial response to detection of a Security or Privacy Event is typically the Analysis Phase. *In this phase the SIRT determines whether a Security or Privacy Event is an actual Security or Privacy Incident.* To determine if a Security or Privacy Event is a Security or Privacy Incident the following considerations apply:

1. Leverage diagnostic data to analyze the Security or Privacy Event using tools directly on the operating system or application. This may include, but not be limited to:
    (i) Taking screenshots, memory dumps, consult logs and network traces.
    (ii) Performing analysis on the information being collected.
    (iii) Analyzing the precursors and indications.
    (iv) Looking for correlating information; and
    (v) Performing research (e.g., search engines, knowledgebase).

2. Identify whether the Security or Privacy Event was the result of an innocent error, or the actions of a potential attacker. If the latter, effort shall be made to identify who the potential attacker may be, by processes such as:
    (i) Validating the attacker's IP address.
    (ii) Researching the attacker through search engines.
    (iii) Using incident databases.
    (iv) Monitoring attacker communication channels, if possible; and
    (v) In unique cases, and with the approval of legal counsel, potentially scanning the attacker's system.

If the SIRT has determined that a Security or Privacy Event has triggered a Security or Privacy Incident, senior leadership will be notified and the appropriate SIRT team members will be engaged accordingly and the SIRT will begin documenting the investigation and gathering evidence. The type of Security or Privacy Incident is based on the nature of the event. Example types are listed as follows:

1. Data exposure.
2. Unauthorized access/Inappropriate role-based access.
3. Distributed Denial of Service/ Denial of Service (DDoS/DoS).
4. Malicious code.

5. Improper usage.
6. Scans/Probes/Attempted access.

If it is determined that a Security or Privacy Incident has not been triggered, additional activities noted under '7.7. Post-Incident Activities' may be initiated under the direction of the SIRT.

The Security or Privacy Incident's potential impact on iCIMS and/or its subscribers shall be evaluated and the SIRT shall assign an initial severity classification of low, medium, high, or critical to the Security or Privacy Incident. To analyze the situation, scope, and impact, the SIRT shall:

1. Define and confirm the severity level and potential impact of the Security or Privacy Incident.
2. Identify which resources have been affected and forecast which resources will be affected.
3. Estimate the current and potential effect of the Security or Privacy Incident.

The SIRT shall attempt to determine the scope of the Security or Privacy Incident and verify if the Security or Privacy Incident is still ongoing.

Scoping the Security or Privacy Incident may include collecting forensic data from suspect systems or gathering evidence that will support the investigation. It may also include identifying any potential data theft or destruction. New investigative leads may be generated as the collected data is analyzed.

If the Security or Privacy Incident involves malware, the SIRT shall analyze the malware to determine its capabilities and potential impact to the environment. Based on the evidence reviewed, the SIRT will determine if the Security or Privacy Incident requires reclassification as to its severity or cause (e.g., whether it was originally thought to be the action of a malicious actor but turned out to be an innocent error, or vice versa).

As indicated above, a Security or Privacy Incident may require evidence to be collected. The collection of such evidence shall be done with due diligence and the following procedures shall apply:

1. Gathering and handling of evidence (forensics) shall include:
    (i) Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, and IP address of a computer).
    (ii) Name, title, and phone number of everyone who collected or handled the evidence during the investigation.
    (iii) Time and date (including time zone) of each occurrence of evidence handling.
    (iv) Locations where the evidence was stored, and conditions of storage (e.g., locked spaces, surveilled spaces); and
    (v) Reasonable efforts to create two backups of the affected system(s) using new, unused media — one is to be sealed as evidence and one is to be used as a source of additional backups.
2. To ensure that evidence is not destroyed or removed, where any Personnel are suspected of being responsible for a Security or Privacy Incident, iCIMS shall, consistent with its procedures, use reasonable efforts to place monitoring and forensics agents and/or confiscate all computer/electronic assets that have been assigned to the individual.
    (i) This task may be done surreptitiously and shall be completed as quickly and in as non-intrusive a manner as possible.
    (ii) The SIRT shall consider restricting access to the computers and attached peripherals (including remote access via VPN, secure remote system access, etc.) pending the outcome of its examination.
3. Where applicable, and depending upon the seriousness of the Security or Privacy Incident, items and areas that shall be secured and preserved in an "as was" condition include:
    (i) Work areas (including wastebaskets).
    (ii) Computer hardware (keyboard, mouse, monitor, CPU, etc.).
    (iii) Software.

(iv) Storage media (disks, tapes, removable disk drives, CD ROMs, USB flash drives, etc.).

(v) Documentation (manuals, printouts, notebooks, notepads).

(vi) Additional components as deemed relevant (printer, cables, etc.).

(vii) In cases of damage, the computer system and its surrounding area, as well as other data storage devices, shall be preserved for the potential collection of evidence (e.g., fingerprinting).

(viii) If the computer is "Off", it shall not be turned "On". For a stand-alone computer system, if the computer is "On", the Information Security and IT Departments are to be contacted.

4. It is important to establish who was using the computer system at the time of the Security or Privacy Incident and/or who was in the immediate area. The SIRT shall obtain copies of applicable records (e.g., access logs, swipe card logs, closed circuit television ("CCTV") recordings) as part of the investigation.

5. Based on the severity level and the categorization of the Security or Privacy Incident, the proper team or Personnel shall be notified and contacted by the SIRT.

6. Until the SIRT, with the approval of iCIMS senior management, makes the Security or Privacy Incident known to other Personnel, the foregoing activities shall be kept confidential to the extent possible.

If it is determined that a Security or Privacy Incident has occurred and may have a significant impact on iCIMS or its subscribers, the SIRT shall determine whether additional resources are required to investigate and respond to the Security or Privacy Incident. The extent of the additional resources will vary depending on the nature and significance of the Security or Privacy Incident.

Abnormal Activities Notification:

The SIRT recognizes that there may be many attempts to gain unauthorized access to, disrupt or misuse information systems and the information stored on them, and that many of these attempts will be thwarted by iCIMS' information security program. In general, the SIRT will not report unsuccessful attacks to customers, Data Controllers, government bodies, or PII Principals. For example, the SIRT would generally *not* be required to report

to a Data Controller or customer if it makes a good faith judgment that the unsuccessful attack was of a routine nature.

However, the SIRT will take reasonable steps to notify customers or Data Controllers of any identified Abnormal Activities. For example, in making a judgment as to whether an unsuccessful attack shall be reported, iCIMS might consider whether handling the attack required measures or resources well beyond those ordinarily used, like exceptional attention by senior personnel or the adoption of extraordinary non-routine precautionary steps. In cases of identified Abnormal Activities, the Data Controller or customer would be notified by means agreed upon by iCIMS and the Data Controller or customer within twenty-four (24) hours upon iCIMS becoming aware of the Abnormal Activity.

Data Breach Notification:

If it is determined during the Analysis Phase that a Security or Privacy Incident has occurred that constitutes a Data Breach, with notification obligations based on applicable legislation, regulation, or similar jurisdictional requirements, then notification of such Data Breach shall be handled by the SIRT and provided to the impacted parties by email, telephone, or other appropriate means agreed upon by iCIMS and the applicable party, or by means stipulated under applicable data protection or privacy law, within twenty-four (24) hours upon iCIMS SIRT becoming aware of the Data Breach. Additional activities noted under '7.7. Post-Incident Activities' may also be initiated under the direction of the SIRT.

When determining the parties to be notified of such Data Breach, the SIRT will analyze the impacted parties (customers, Data Controllers, PII Principals, Third Parties, government bodies) and determine the applicable relationships between the parties (controller, joint controller, processor and/or subprocessor), the applicable contractual obligations, and the applicable laws, regulations, or like jurisdictional requirements. Based on this analysis, iCIMS will notify applicable parties as follows based on iCIMS role as a:

- Controller - Notify the applicable government body, and if the Data Breach is likely to result in a high risk to the rights and freedoms of PII Principals, notify the PII Principals.
- Joint Controller – Notify the other controller and the applicable government body, and if the Data Breach is likely to result in a high risk to the rights and freedoms of PII Principals, notify the PII Principals.
- Processor - Notify the controller.
- Sub-processor - Notify the processor, and where appropriate and feasible, the controller.

7.4. Containment Phase

The Containment Phase mitigates the root cause of the Security or Privacy Incident to prevent further damage or exposure. This phase attempts to limit the impact of a Security or Privacy Incident prior to an eradication and recovery event. During this phase, the SIRT may implement controls, as necessary, to limit the damage from a Security or Privacy Incident. If a Security or Privacy Incident is determined to be caused by innocent error, the Eradication Phase may not be needed. For example, after reviewing any information that has been collected investigating the Security or Privacy Incident the SIRT may:

1. Secure the physical and network perimeter.
    i. For example, shutting down a system, disconnecting it from the network, and/or disabling certain functions or services.
2. Connect through a trusted connection and retrieve any volatile data from the affected system.
3. Determine the relative integrity and the appropriateness of backing the system up.
4. If appropriate, back up the impacted system.
5. Change the password(s) to the affected system(s). Personnel, as appropriate, shall be notified of the password change.
6. Determine whether it is safe to continue operations with the affected system(s).
    i. If it is safe, allow the system to continue to function, in which case the SIRT will:

a. Update the Incident Record; accordingly, and

b. Move to the Recovery Phase.

ii. If it is not safe to allow the system to continue operations, the SIRT will discontinue the system(s) operation and move to Eradication Phase.

iii. The SIRT may permit continued operation of the system under close supervision and monitoring if:

1. Such activity will assist in identifying individuals responsible for the Security or Privacy Incident.

2. The system can run normally without risk of disruption, compromise of data, or serious damage; and

3. Consensus has been reached within the SIRT before taking the supervision and monitoring approach.

7. The final status of this stage shall be appropriately documented in the Incident Record.

8. The SIRT shall apprise senior management of the progress, as appropriate.

During the Analysis and Containment Phases, the SIRT shall keep notes and use appropriate chain of custody procedures to ensure that the evidence gathered during the Security or Privacy Incident can be used successfully during prosecution, if appropriate.

7.5. Eradication Phase

The Eradication Phase is the phase where vulnerabilities causing the Security or Privacy Incident, and any associated compromises, are removed from the environment. An effective eradication for a targeted attack removes the attacker's access to the environment all at once, during a coordinated containment and eradication event. Although the specific actions taken during the Eradication Phase can vary depending on the Security or Privacy Incident, the standard process for the Eradication Phase shall be as follows:

1. Determine the symptoms and cause related to the affected system(s).

2. Eliminate components of the Security or Privacy Incident. This may include deleting malware, disabling breached user accounts, etc.

3. Strengthen the controls surrounding the affected system(s), where possible (a risk assessment will be performed, if needed). This may include the following:
    i. Strengthening network perimeter defenses.
    ii. Improving monitoring capabilities or scope.
    iii. Remediating any security issues within the affected system(s), such as removing unused services or implementing general host hardening techniques.
    iv. Conduct a vulnerability assessment to verify that all the holes/gaps that can be exploited have been addressed.
4. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
5. Update the Incident Record with the information learned from the vulnerability assessment, including the cause, symptoms, and method used to fix the problem with the affected system(s).
6. If necessary, escalate to higher levels of support to enhance capabilities, resources, or time-to-eradication.
7. Apprise senior management of progress, as appropriate.

After iCIMS has implemented the changes for eradication, it is important to verify that cause of and individual(s) causing the Security or Privacy Incident is fully eradicated from the environment. The SIRT shall also test the effectiveness of any security controls or changes that were made to the environment during containment and eradication.

7.6. Recovery Phase

The Recovery Phase represents the SIRT's effort to restore the affected system(s) to operation after the problems that gave rise to the Security or Privacy Incident, and the consequences of the Security or Privacy Incident, have been corrected. Recovery events can be complex depending on the Security or Privacy Incident type and can require full project management plans to be effective.

Although the specific actions taken during the Recovery Phase can vary depending on the identified Security or Privacy Incident, the standard process to accomplish this shall be as follows:

1. Execution of the following actions, as appropriate:
    - Installing patches.
    - Rebuilding systems.
    - Changing passwords.
    - Restoring systems from clean backups.
    - Replacing affected files with clean versions.
2. Determination whether the affected system(s) has been changed in any way.
    a. If the system(s) has been changed, the system is restored to its proper, intended functioning ("last known good").
        i. Once restored, the system functions are validated to verify that the system/process functions as intended. This may require the involvement of the business unit that owns the affected system(s).
        ii. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline), it shall be restored and validated, and the system(s) shall be monitored for proper behavior.
    b. If the system(s) has not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
3. Implementation of additional monitoring and alerting may be done to identify similar activities.
4. Update the Incident Record with any details determined to be relevant during this phase.
5. Apprise senior management of progress, as appropriate.

7.7. Post-Incident Activities

In addition to the Data Breach and Abnormal Activities notification requirements identified in the analysis phase above, and after verification of a successful containment and any necessary eradication, the SIRT shall take the following post-incident activities, as may be necessary:

II. Communications

A. Notification

After consulting with senior management, when warranted or required by judicial action, applicable law, regulation, or like jurisdictional requirement, iCIMS shall use reasonable efforts to provide notice to Personnel and/or affected parties about a Security or Privacy Incident or Data Breach involving the Personal Information and/or Subscriber Data of such stakeholders. For example:

1. Where it has been determined, or the SIRT and senior management reasonably believe, that there has been unauthorized access to or release of unencrypted Subscriber Data.
2. Where a Security or Privacy Incident has compromised the security, confidentiality, or integrity of Subscriber Data.

Upon deciding to notify and prior to notifying law enforcement or other governmental authority (if necessary), the SIRT (in consultation with senior leadership), shall use reasonable efforts to provide notice and disclosure to Personnel and/or affected parties within twenty-four (24) hours and, subject to applicable law, regulation, or like jurisdictional requirement prior to notification of law enforcement personnel. Delayed notification may nonetheless occur in instances where it is required mandated or authorized by applicable law, regulation, or court of competent jurisdiction. For example, notification disclosure might be delayed if notice would impede a criminal investigation or if time is required to restore reasonable integrity to iCIMS's information systems.

Notification of a Data Breach or Abnormal Activities will occur within twenty-four (24) hours of identification, as noted in the 'Abnormal Activities Notification' and 'Data Breach Notification' sections above in alignment with regulatory and contractual requirements.

If appropriate, the SIRT may:

    1. Prepare a general notice and arrange for providing the notice to Personnel and/or affected parties.
2. Prepare a FAQ based on the notice and arrange to have it posted to the iCIMS website after the notice has been sent.
3. Identify a point a contact for Personnel and/or affected parties to contact if further information is sought; and
4. Establish a toll-free number for use by stakeholders.

iCIMS' objective is to provide notice in a manner designed to ensure that Personnel and/or affected parties can reasonably be expected to receive the disclosure.

The form and content of the notification may either be by letter (first class mail) or by email sent to an address where Personnel and/or affected parties can reasonably be expected to receive the disclosure or other, similar means.

The notification, in clear and plain language, may contain the following elements:

1. A description of the Security or Privacy Incident or Data Breach that includes as much detail as is appropriate under the circumstances.
2. The type of information that was impacted (e.g., number of individuals or records concerned) subject to unauthorized access and any foreseeable, likely consequences.
3. Measures taken by iCIMS to protect the Information of Personnel and/or affected parties from further impact.
4. A contact name and toll-free number that Personnel and/or affected parties may use to obtain further information.
5. A reference to the page on the iCIMS website where updates may be obtained.
6. A reminder to guard against possible identity theft by being vigilant with respect to banking or credit activity for twelve to twenty-four months.
7. Contact information for national credit reporting agencies.

8. Other elements as may be required by applicable law or whose inclusion the SIRT may otherwise consider appropriate under the circumstances.

B. Cooperation with External Investigators

If the SIRT considers it appropriate to inform law enforcement authorities or to retain forensic investigators or other external advisors, the following information shall be collected to provide to such authorities or investigators:

1. To the extent known, details of the:
    a. Security or Privacy Incident (date, time, place, duration, etc.).
    b. Person(s) under suspicion (name, date of birth, address, occupation/position, employment contracts, etc.).
    c. Computer and network log files pertaining to the Security or Privacy Incident(s).
    d. "Ownership" details of any Information that is allegedly stolen, altered, or destroyed.
    e. The access rights to the computer system involved of the person(s) under investigation.
    f. Information obtained from access control systems (e.g., computer logs, CCTV, swipe card systems, attendance logs, etc.); and
    g. Any action taken by the IT department in relation to the computer systems concerned, including the date and time.
2. A copy of applicable iCIMS Data Privacy and Security Statement ("Statement") in force at the time of the incident (if applicable); and
3. Any other documentation or evidence relevant to the internal investigation of the Security or Privacy Incident.

C. Information Sharing and Media Relations

Security or Privacy incident-specific information (e.g., dates, accounts, programs, systems) must not be provided to any unknown individuals making such requests by telephone or email. Any release of Security or Privacy incident-specific information shall only be to individuals previously identified by the SIRT. All

requests for information from unknown individuals shall be forwarded to the SIRT. If there is any doubt about whether information can be released, contact the GCO.

Contact with law enforcement authorities shall only be made by the GCO in consultation with the SIRT and senior management.

In the event of a Security or Privacy Incident, where members of the media make inquiries, Personnel are to be made aware that all requests for the release of information, press releases, or media interviews must be submitted to the GCO.

The GCO, in consultation with the SIRT and senior management, shall determine whether it is appropriate to issue a media statement, hold a press briefing, or schedule interviews.

If Sensitive Personal Information has been compromised and a significant number of individuals, as identified by the SIRT, are affected and/or suspected of being affected, the GCO, upon consultation with outside counsel and subject to applicable law, shall use reasonable efforts to contact applicable consumer reporting agencies prior to sending notices to the affected Personnel and/or affected parties.

Certain jurisdictions where iCIMS does business, or where iCIMS' stakeholders reside, mandate different disclosure or notification obligations. Additionally, advice from both inside and outside counsel is required before communication occurs with credit reporting agencies.

D. External Incident Communications

After a Security or Privacy Incident, information may be required to be shared with outside parties, following emergency response procedures as necessary, including:

- Law enforcement/incident reporting organizations
- Affected external parties
- The media
- Other outside parties

1. iCIMS will seek to ensure its obligations are fulfilled by quickly and professionally taking control of communication early during major events. Accordingly, the SIRT will:
    - Designate a credible, trained, informed spokesperson to address the media.
    - Determine appropriate clearance and approval processes for the media.
    - Ensure the organization is accessible by media so they do not resort to other (less credible) sources for information.
    - Emphasize steps being taken to address the Security or Privacy Incident.
    - Tell the story quickly, openly, and honestly to counter falsehoods, rumors, or undue suspicion.
2. When publicly disclosing information of a Security or Privacy Incident, the following shall be considered:
    - Was Personal Data compromised?
    - Was Subscriber Data compromised?
    - Were legal and/or contractual obligations invoked by the Security or Privacy Incident?
    - What is the organization's strategy moving forward?

E. Internal Incident Communications

1. Where warranted, the SIRT will ensure that open communication is maintained within the organization to ensure relevant parties are informed of facts, reminded of responsibilities, and capable of dismissing rumors and speculation.
2. Aggregate documentation from post-mortem/follow-up reviews into the Security or Privacy Incident record and create a formal report of the Security or Privacy Incident to share with senior management, as necessary.

III. Follow Up

The Follow-up Phase represents the review of the Security or Privacy Incident to look for "lessons learned" and to determine whether the process that was followed could have been improved in any way.

Security or Privacy Events and Security or Privacy Incidents shall be reviewed after identification resolution to determine where response could be improved.

The SIRT will meet to review the Security or Privacy Event, or Security or Privacy Incident record created, as necessary, and perform the following:

i) Determine the root cause of the Security or Privacy Incident and what shall be done to ensure that the root cause has been addressed.

ii) Create a "lessons learned" document and include it with the Incident Record.

iii) Evaluate the cost and impact of the Security or Privacy Event or Incident to the organization using applicable documents and any other resources.

iv) Determine what could be improved.

v) Communicate these findings to senior management for approval, as necessary, and for implementation of any recommendations made post-review of the Security or Privacy Event or Incident.

vi) Carry out recommendations approved by senior management while ensuring that sufficient time and resources are committed to this activity.

vii) Close the Security or Privacy Event or Incident.

A. Retention and Review of Security or Privacy Incident Record & Documentation

It shall be the responsibility of the SIRT to investigate the Security or Privacy Incident and establish an incident record. The incident record shall be verified during the follow up process to ensure that it documents:

1. Relevant factual information or evidence.
2. Consultations with Personnel and external advisors; and
3. Findings resulting from the collection of factual information or evidence obtained.

The rationale for the creation of an incident record is that law enforcement authorities may be informed of Security or Privacy Incidents or iCIMS may take legal action if individuals causing a Security or Privacy Incident can be identified. The implications of each Security or Privacy Incident are not always discernible at the start of, or even during, the course of a Security or Privacy Incident. Accordingly, it is important that information is documented, and associated information system events are logged.

The incident record may be in written or electronic form. If it is maintained in an electronic form, appropriate protections must be applied to guard against the alteration or deletion of the incident record.

The information to be reported will vary according to the specific circumstances and availability of the information, but may include:

1. Dates and times when incident-related events occurred.
2. Dates and times when incident-related events were discovered.
3. Dates and times of incident-related conference calls.
4. A description of the Security or Privacy Incident, including the systems, programs, networks or types of Information that may have been compromised.
5. Root cause(s) of the Security or Privacy Incident(s), if known, and how they have been addressed.
6. An estimate of the amount of time spent by Personnel working to remediate incident-related tasks.
7. The amount of time spent by Third Parties working on incident-related tasks, including advice from outside counsel.
8. The names and contact information of all individuals providing information in connection with the investigation.
9. The information analyzed to determine notification obligations, including the names of the impacted parties, the relationships between the parties, the applicable contractual obligations, and the applicable laws, regulations, or like jurisdictional requirements.
10. Measures taken to prevent future Security or Privacy Incidents, taking into consideration root causes, along with any remediation costs incurred by iCIMS; and

11. If applicable, the date and time of law enforcement involvement.

All Personnel have an affirmative obligation to use reasonable efforts to respond to all inquiries for information and cooperate in all investigations. Obstruction of Security or Privacy Event and Security or Privacy Incident investigations may lead to disciplinary actions, up to and including termination.

Review of the incident record and documentation shall include the following:

1. Review tracked documents of the Security or Privacy Incident to evaluate the following:
    - The causes of the nonconformity.
    - Whether similar nonconformities exist or could potentially occur.
    - The effectiveness of the corrective action taken; and
    - The effectiveness of the Incident Response process.
2. Learn from Security or Privacy Incidents and improve the response process. Security or Privacy Incidents must be recorded, and a post incident review conducted. Identify the impact of Security or Privacy Incidents and outline pain points for future security investments. The following details must be retained:
    - Types of Security or Privacy Incidents
    - Volumes of Security or Privacy Incidents and malfunctions
    - Costs incurred during the Security or Privacy Incidents, where possible.

B. Retention and Review of Data Breaches Record & Documentation

It shall be the responsibility of the iCIMS Privacy, under SIRT oversight, to notify impacted parties about a Data Breach and to establish a record of the Data Breach with sufficient information to provide a report for regulatory and/or forensic purposes. The Data Breach record shall be verified during the follow up process to ensure that it documents:

- A description of the Security Incident and/or Privacy Incident.

- The time period.
- The consequences of the Security or Privacy Incident.
- The name of the reporter.
- To whom the Security or Privacy Incident was reported.
- The steps taken to resolve the Security or Privacy Incident (including the person in charge and the data recovered); and
- The fact that the Security or Privacy Incident resulted in unavailability, loss, disclosure, or alternation of Personal Data and/or PII.

C. Periodic Evaluation of the Program

The processes surrounding incident response shall be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to Security or Privacy Events and Incidents, as well as the training of the general population regarding the organization's expectation of them, relative to security responsibilities.

Security or Privacy Events and Incidents shall be recorded for tracking, analysis, and reporting purposes. The following metrics shall be considered to assess the overall Security or Privacy Incident management program:

- Overall reduction in time spent responding to Security or Privacy Incidents.
- Reduction of impact of certain Security or Privacy Incidents.
- Overall occurrence of Security or Privacy Incidents.
- Mean time to analysis (MttA)
- Mean time to resolution (MttR)