## Purpose Statement

The Tuskegee University (TU or the University) Information Security Incident Response Policy establishes responsibilities associated with the coordination of the University's information technology (IT) incident response. The policy is necessary in order to ensure the timely remediation of negative campus IT incidents as well as in post-incident information gathering and reporting of infrastructure-affecting and security-related events.

## Scope

The TU Information Security Incident Response Policy applies to all computer systems and networks connected to the TU network and any remote access (e.g., dial-up connections, VPN connection, etc.) onto the campus network or associated domains

The Incident Response policy is as follows:

- Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to Security Incidents.
- The objectives for Security Incident management should be communicated to University stakeholders and it should ensure that those responsible for Security Incident management understand the organization's priorities for handling Security Incidents.
- Security Events should be reported through appropriate management channels as quickly as possible.
- Personnel and contractors using the University's information systems and services are required to note and report any observed or suspected Security Weakness in systems or services.
- Security Events should be assessed and it should be decided if they are to be classified as Security Incidents.
- Security Incidents should be responded to in accordance with documented Incident Response procedures.
- Knowledge gained from analyzing and resolving Security Incidents should be used to reduce the likelihood or impact of future incidents.
- Procedures should be defined and applied for the identification, collection, acquisition, categorization 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 (Faculty, Staff and Students);
    - How the program works, expectations;
    - How to report Security Incidents, whom to contact;
    - Constraints imposed by non-disclosure agreements.
- Communication channels should be established well in advance of a Security Incident. Include all necessary parties in relevant communication:

- Incident response members
- Senior Management
- Board Members

INCIDENT RESPONSE PROCEDURES

DOCUMENT PURPOSE

1.3. The purpose of this document is to define the Incident Response procedures in the event of a security incident. This document is a step-by-step guide of the measures Faculty and Staff are required to take to manage the lifecycle of Security Incidents at Tuskegee University, from initial Security Incident recognition to restoring normal operating efficiency. This process will ensure that all such Security Incidents are detected, analyzed, contained and eradicated, that measures are taken to prevent any further Security Incidents, and, where necessary or appropriate, that notice is provided to law enforcement authorities, Faculty, Staff, Students and/or affected parties.

1.4. This document applies to all Tuskegee Personnel and supersedes all other procedures, practices, and guidelines relating to the matters set forth herein.

6. TERMS & DEFINITIONS

| Term/Acronym | Definition |
|---|---|
| Escalation | The engagement of additional resources to resolve a Security Incident. |
| Incident Record | Created at the time a Security Incident is initially recognized. Contains all relevant information pertaining to the Security Incident. |
| Incident Response / Incident Management | Process for detecting, reporting, assessing, responding to, dealing with, and learning from Security Incidents. |
| Information Security | Preservation of confidentiality, integrity, and availability of Information and the equipment, devices or services containing or |

| | |
|---|---|
| | providing such Information. |
| Personnel | Tuskegee employees (part and full time) and Students. |
| Security Event | An identified occurrence of a system, service or network state indicating a possible exploitation of a Security Vulnerability or Security Weakness. |
| Security Incident | A single or series of unwanted or unexpected Security Events that compromise business operations with an impact on Information Security. |
| Security Incident Response Team (SIRT) | A predefined group of individuals needed and responsible for responding to a Security Incident, managed by the Information Technology Department. During a Security Incident, the SIRT is responsible for communication with and coordination of other internal groups. |
| Security Vulnerability | A weakness of an existing asset or control that can be exploited by one or more threats. |
| Security Weakness | A weakness that results from the lack of an existing, necessary control. |

## 7. SCOPE

This document covers the Incident Response process for all identified Security Incidents.

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.

## 8. OVERVIEW

### 8.1. Roles and Responsibilities

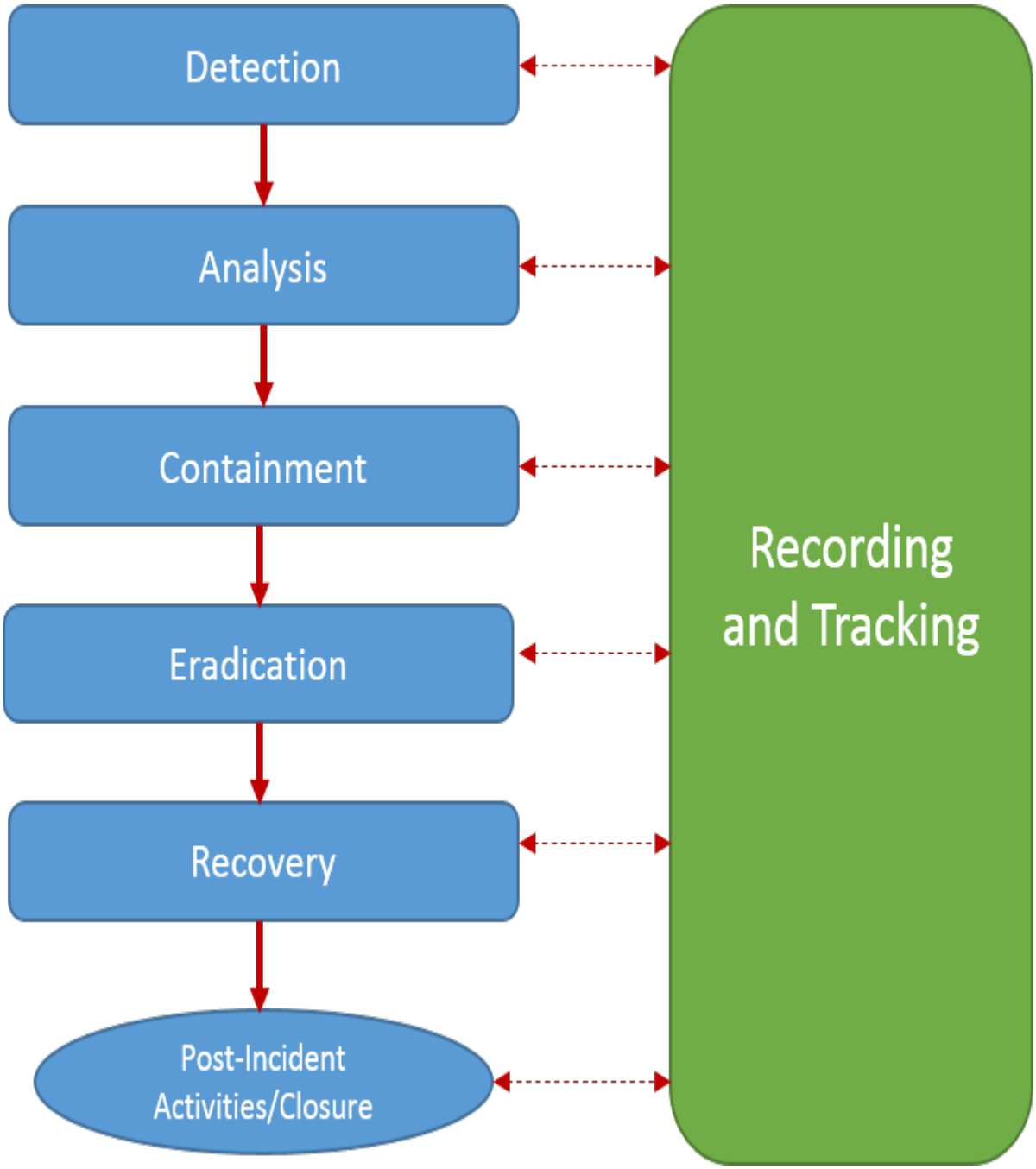
Individuals needed and responsible for responding to a Security Incident make up the SIRT. Core members will include the following:

- Information Security Manager (SIRT Primary Lead)
- Senior Corporate Counsel (SIRT Secondary Lead)
- Security team staff
- Information owner

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

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

## 9. PROCESS




9.1. Detection Phase

In the detection phase, the SIRT or an internal or external entity, identifies a Security Event that is the result of a potential exploitation of a Security Vulnerability or a Security Weakness.

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

Email: InformationSecurity@tuskegee.edu

A Security 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.

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

- Information was used by unauthorized Personnel or Third Parties;
- Information has been downloaded or copied inappropriately from TU 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).

In addition, the following situations should be considered for Security Event reporting:

- Ineffective security controls;
- Breach of information integrity, confidentiality or availability expectations;
- Human errors;
- 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 Event is an actual Security 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 Event. However, the following information should be supplied in all cases:

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

Information Security will ensure that the SIRT is promptly engaged in the event of receiving such notice. The following actions will also be taken:

1. The SIRT, under the leadership of the Information Security Department, must 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 a decision to begin the Analysis Phase, if the SIRT suspects that the Security Event may result in damage to the reputation of TU or in legal liability, the GCO shall initiate a legal assessment of actual or potential legal issues.

9.2. Analysis Phase

The initial response to detection of a Security Event is typically the Analysis Phase. In this phase the SIRT determines whether or not a Security Event is an actual Security Incident. In order to determine whether or not a Security Event is actually a Security Incident the following should occur:

1. Leverage diagnostic data to analyze the Security Event using tools directly on the operating system or application including, but not 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 the potential attacker by:

(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, potentially scanning the attacker's system.

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

1. Data exposure.

2. Unauthorized access.

3. Distributed Denial of Service/ Denial of Service (DDoS/DoS).

4. Malicious code.

5. Improper usage.

6. Scans/Probes/Attempted access.

The Security Incident’s potential impact on TU and/or its stakeholders will be evaluated and the SIRT will assign an initial severity classification of low, medium, high or critical to the Security Incident. To analyze the situation, scope and impact, the SIRT will:

1. Define and confirm the severity level and potential impact of the Security 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 Incident.

4. Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources.

The SIRT will attempt to determine the scope of the Security Incident and verify if the Security Incident is still ongoing. Scoping the Security Incident can include collecting forensic data from suspect systems or gathering evidence that will support the investigation. It will also include identifying any potential data theft or destruction. New investigative leads may be generated as the collected data is analyzed. If the Security Incident involves malware, the SIRT will need to 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 Incident requires reclassification of the severity.

As indicated above, a Security Incident may require evidence to be collected. The collection of such evidence must be approached with due diligence and the following procedures must be adhered to:

1. Gathering and handling of evidence (forensics) should 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

(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 responsible for a Security Incident, TU shall, consistent with its procedures, use reasonable efforts to confiscate all computer/electronic assets that have been assigned to him/her.

(i) This task should be completed as quickly and in as non-intrusive a manner as possible.

(ii) The SIRT should consider restricting access to the computers and attached peripherals (including remote access via modem, secure remote system access, etc.) pending the outcome of its examination.

3. Where applicable, and depending upon the seriousness of the Security Incident, items and areas that should 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, 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, should be preserved for the potential collection of evidence (e.g., fingerprinting);

(viii) If the computer is "Off", it should 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 Incident and/or who was in the immediate area. The SIRT should 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 Incident, the proper team or Personnel will be notified and contacted by the SIRT.

6. Until SIRT makes a conclusive determination, the foregoing activities are to be kept confidential to the extent possible.

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

9.3. Containment Phase

The Containment Phase mitigates the root cause of the Security Incident to prevent further damage or exposure. This phase attempts to limit the impact of a Security 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 Incident. For example, after reviewing any information that has been collected investigating the Security 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 system.

5. Change the password(s) to the affected system(s). Personnel, as appropriate, are to 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 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 should be appropriately documented in the Incident Record.

8. The SIRT apprises senior management of the progress, as necessary.

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 Incident can be used successfully during prosecution, if appropriate.

9.4. Eradication Phase

The Eradication Phase is the phase where vulnerabilities causing the Security 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 Incident, the standard process for the Eradication Phase is as follows:

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

2. Eliminate components of the Security 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 necessary.

After SIRT has implemented the changes for eradication, it should be verified that the Security Incident is fully eradicated from the environment. The SIRT should also test the effectiveness of any security controls or changes that were made to the environment during containment and eradication.

9.5. Recovery Phase

The Recovery Phase represents the SIRT's effort to restore the affected system(s) to operation after the resulting security exposures, if any, have been corrected. Recovery events can be complex depending on the Security 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 Incident, the standard process to accomplish this is 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 should be restored and validated, and the system(s) should 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 implemented 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 necessary.

9.6. Post-Incident Activities

After verification of a successful containment and eradication the SIRT will take the following post-incident activities, as necessary:

Communications

Notification

When warranted, SIRT shall use reasonable efforts to provide notice to Personnel and/or affected parties about a Security Incident involving the Information of such stakeholders:

1. Where it has been determined, or the SIRT and management reasonably believe, that there has been the unauthorized acquisition of computerized data that contains unencrypted Personal Information;

2. Where such acquisition has compromised the security, confidentiality or integrity of Confidential Information; and/or

3. Where required by law or judicial authorization.

Upon making a decision to notify, the SIRT, in consultation with senior management, 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, prior to notification of law enforcement personnel. Delay may nonetheless occur in instances where it is mandated or authorized by applicable law. For example, disclosure might be delayed if notice would impede a criminal investigation or if time is required to restore reasonable integrity to TU information systems.

If appropriate, the SIRT may:

1. Prepare a general notice and arrange for mailing of the notice to Personnel and/or affected parties;

2. Prepare a FAQ based on the notice and arrange to have it posted to the TU 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.

IT's 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 of 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.

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

1. A description of the Security Incident that includes as much detail as is appropriate under the circumstances;

2. The type of information subject to unauthorized access;

3. Measures taken by IT to protect the Information of Personnel and/or affected parties from further unauthorized access;

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 TU website where updates may be obtained;

6. A reminder to guard against possible identify 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.

Cooperation with External Investigators

In the event that 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 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 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 TU Data Privacy and Security Policy (“Policy”) 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 Incident.

Information Sharing and Media Relations

Security 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 Incident-specific information should only be to individuals previously identified by the SIRT. All requests for information from unknown individuals should 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 consultations with the SIRT and senior management.

In the event of a Security Incident, following which 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 Information has been compromised and more than five hundred (500) individuals 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 TU stakeholders reside, mandate different disclosure obligations. Advice from both inside and outside counsel is required before communication occurs with credit reporting agencies.

External Incident Communications

After a Security Incident, information may be required to be shared with outside parties, including:

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

1. TU will seek to minimize damage from the media by quickly and professionally taking control of communication early in the course of major events. Accordingly, the TU 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 Incident;
- Tell the story quickly, openly, and honestly to avoid false fact, rumors, or suspicion.

2. When publically disclosing information of a Security Incident, the following should be considered:

- Was Personal Information compromised?
- Was User data compromised?
- Were legal and/or contractual obligations invoked by the Security Incident?
- What is the organization’s strategy moving forward?

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 Incident Record and create a formal report of the Security Incident to share with senior management, as necessary.

Follow Up

The Follow-up Phase represents the review of the Security Incident to look for "lessons learned" and to determine whether the process that was followed could have been improved in any way. Security Incidents should be reviewed after resolution to determine where response could be improved.

The SIRT will meet to review the Incident Record created during the Security Incident, as necessary, and perform the following:

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

ii) Evaluate the cost and impact of the Security Incident to the organization using applicable documents and any other resources.

iii) Determine what could be improved.

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

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

vi) Close the Security Incident.

Retention and Review of Security Incident Record & Documentation

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

1. All relevant information or evidence;

2. Consultations with Personnel and external advisors; and

3. Findings resulting from the collection of information or evidence obtained.

The rationale for the creation of an Incident Record is based on the fact that law enforcement authorities may be informed of Security Incidents or TU may take legal action if individuals causing a Security Incident can be identified. The implications of each Security Incident are not always discernible at the start of, or even during, the course of a Security 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 Incident, including the systems, programs, networks or types of Information that may have been compromised;

5. Cause(s) of the Security Incident(s), if known;

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. Measures taken to prevent future Security Incidents, along with any remediation costs incurred by TU; and

10. 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.

Review of the Incident Record and documentation should include the following:

1. Review tracked documents of the Security 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 Incidents and improve the response process. Security Incidents must be recorded and a post incident review conducted. Identify the impact of Security Incidents and outline pain points for future security investments. The following details must be retained:

- Types of Security Incidents
- Volumes of Security Incidents and malfunctions
- Costs incurred during the Security Incidents

Periodic Evaluation of the Program

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

Security Incidents will be recorded in a Security Incidents inventory for tracking, analysis, and reporting purposes. The following metrics should be considered to assess the overall Security Incident management program:

- Overall reduction in time spent responding to Security Incidents.
- Reduction of impact of certain Security Incidents.
- Overall reduction of the occurrence of Security Incidents.