Purpose Statement

The Tuskegee University (TU or the University) Information Security Incident Response Policy establishes responsibilities associated with the coordination of the University's [illegible] 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

- 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

	providing such Information.
Personnel	Tuskegee employees (part and full time) and Students
Security Event	An identified occurrence of a system, servi or network state indicating a possible exploitation of a Security Vulnerability or Security Weakness.
Security Incident	A single or series of unwanted or unexpect 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 ar 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

In the detection phase, the SIRT, 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

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

(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, 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

(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

TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION

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

TUSKEGEE UNIVERSITY

OFFICE OF INFORMATION TECHNOLOGY

1200 Old Montgomery Road Room 70-408 John A. Kenney Hall Tuskegee, Alabama 36088 ä334 727 8350
www.tuskegee.edu

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.

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

1. To the extent known, detail of the:

a. Security Incident (date, time, place, duration, etc.);

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.

ii) 2())3(E)D6Tj EMC /P <</MCV04 Tc 0.4cumeenec-.dthII -10((MCV

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 4(po)]TJ 0 -12(e)6(r) (c)6 1(h)e1(es)-WillD1-12(2)(0)79>0TF4(x)-6(2ik)ts4(er)4(4(p)/6(e)a(r