The University of Tennessee, Knoxville Incident Response Plan

Prepared by:

The University of Tennessee, Knoxville
Office of Information Technology (OIT)
Information Security Office

Contents

Document Control

Version No.	Version Date	Author	Summary of Changes
1.0	2014-07-01	Bob Hillhouse	Final Version

Approvals

Digitally signed by Joel E. Reeves
DN: cn=Joel E. Reeves, o=University of Tennessee, ou=OIT, email=joel.reeves@utk.edu, c=US
Date: 2014.07.01 07:57:21 -04'00'

July 1, 2014

Joel E. Reeves, Jr.
Assistant Vice-Chancellor & CIO

Date

Robert A Hillhouse

2014-07-01

Robert A. Hillhouse
Associate CIO & Chief Information Security Officer

Date

Name	Title	Date of Approval	Version No.
Joel E. Reeves, Jr.	Asst. Vice-Chancellor & CIO, UT Knoxville		1.0
Robert A. Hillhouse	Associate CIO & Chief Information Security Officer	2014-07-01	1.0

University of Tennessee, Knoxville Incident Response Plan (IRP)

1. Executive Summary

This document implements the requirements stated in The University of Tennessee, Knoxville Information Security Plan regarding the coordination and facilitation of an incident notification and response process. The University of Tennessee, Knoxville (UTK) campus community is required to utilize this process in cases concerning suspected violations of any of the following:

Information Technology Policy IT0110 (AUP)
Fiscal Policy FI0805 – Information Technology Resources
Unauthorized release or exposure of university systems
All applicable laws of the state of Tennessee and the federal government

This document provides specific requirements for dealing with information systems security incidents and suspected information technology resources abuses. This document is meant to provide the UTK information systems support personnel with a systematic approach for handling the discovery of and response to an abuse or security incident. The process is developed to achieve the following goals:

Minimize disruptions to business functions and network operations
Confirm whether an incident or abuse has occurred
Promote the accumulation of accurate information
Establish controls for proper retrieval and handling of evidence
Allow for legal (to include criminal and/or civil) actions against perpetrators
Provide accurate reports and useful recommendations

This document contains references to the processes for dealing with security incidents and/or resource abuses from any source connected to or transmitting information using UTK information technology resources.

The University of Tennessee, Knoxville is committed to preserving the confidentiality, integrity and availability of its information resources. The University of Tennessee, Knoxville adopts and implements this Security Incident Response Plan as a means of minimizing the effects of a security incident and restoring information technology services.

This document must be reviewed annually by the UTK Chief Information Officer or his designee.

2. Scope

This process applies to all users (including but not limited to, staff, faculty, students, contractors, consultants, and visitors) while using UTK information systems resources. All users are required to be advised of this plan and comply with this process.

See Appendix A for a glossary of terms.

3. Roles and Responsibilities

3.1. Reporting and Contact Information

The following is the point of contact for information regarding the Incident Response Plan:

Name:	**Bob Hillhouse**
Title:	**Associate CIO & Chief Information Security Officer**
Email:	**security@utk.edu or bob@utk.edu**

3.2. Responsibilities

All users of UTK information resources, system administrators, information systems support personnel, and security support personnel must understand their role in relationship to this process and comply with its requirements.

The UTK Chief Information Officer (CIO) or his designee is responsible for maintaining and overseeing the incident response process and assigning members to the Security Incident Response Team (SIRT) appropriate to the security event. The SIRT is accountable to the CIO for the investigation, declaration, analysis, and disposition of an incident. The membership of the SIRT is dependent on the type of incident and the means necessary to mitigate its effect on the confidentiality, integrity or availability of information resources.

The UTK CIO has the authority to monitor suspicious activity and to disconnect equipment that are in violation of university, campus, state or federal regulations.

See Appendix B for more detail covering the responsibilities of specific personnel.

4. Event Detection and Incident Confirmation Process

Events can be detected through a variety of technical and procedural mechanisms. Technical mechanisms include intrusion prevention/detection systems (IPS/IDS), Security Information and Event Management (SIEM) systems, and firewalls which produce alerts when suspicious network activity is detected. Procedural mechanisms include system log reviews, observations of abnormal resource utilization and suspicious account activity. Additionally, sources external to the university (MS-ISAC, REN-ISAC, DMCA) may detect issues by recognizing unauthorized activity or abnormal behavior on their systems and reporting the activity to the university.

4.1. Incidents that use Common Attack Vectors

Although incidents occur in many ways, this plan focuses on the procedures to handle incidents that use the following common attack vectors:

1. **External/Removable Media** – an attack executed from removable media (e.g., flash drive, CD) or a peripheral device.
2. **Attrition** – An attack that uses brute force methods to compromise, degrade, or destroy systems, networks or services.
3. **Web** – An attack executed from a website or web-based application.
4. **Email** – An attack executed via an email message or attachment.
5. **Improper Usage** – Any incident resulting from the violation of UT Policy IT0110 – The Acceptable Use Policy – by an authorized user, excluding the above categories.
6. **Loss or Theft of Equipment** – The loss or theft of a computing device or media used by the university, such as a laptop or smartphone.
7. **Other** – An attack that does not fit into any of the other categories.

4.2. Incident Verification

A combination of the following activities can represent a security event and thus require action. Although observing one of these symptoms is generally inconclusive, observing one or more of these symptoms in conjunction is motivation for further scrutiny:

a) Unsuccessful logon attempts;
b) Unexplained system crashes;
c) Unexplained poor system performance;
d) Port scanning (use of exploit and vulnerability scanners, remote requests for information about systems and/or users, or social engineering attempts);
e) Unusual usage times (statistically, more security incidents occur during non-working hours than any other time);
f) An indicated last time of usage of an account that does not correspond to the actual last time of usage for that account.

4.3. Incident Prioritization

Incidents are prioritized based on the following relevant factors:

1. **Functional Impact** –the current or future impact of an incident on the university's ability to conduct business.
2. **Informational Impact** – the incident's impact on the confidentiality, integrity, or availability of the university's information resource.
3. **Recoverability Impact** – the effort and the resources required to return the resource to full operation.

5. Incident Response Using Standard Operating Procedures

Unless evidence collection and network monitoring is immediately initiated, critical information may be destroyed before investigators have a chance to review it. Furthermore, UTK information technology support personnel have the responsibility to inform affected individuals/organizations in a timely fashion. All users should report events to the Office of Information Technology (OIT) HelpDesk and to their respective System Administrator (SA). The SA, or the HelpDesk will then gather the necessary information to appropriately record the security event.

The contact number for reporting a security event is:

OIT HelpDesk: (865) 974-9900

5.1. Incidents involving MODERATE systems

It is important to note that a suspected compromise of any system must be reported immediately to the OIT HelpDesk. **The suspected system should not be rebooted, disconnected, or otherwise altered unless directed by a member of the SIRT.**

Systems classified as MODERATE may contain information that includes, but is not limited to, personally identifiable information (PII), or information covered by Payment Card Industry – Data Security Standards (PCI-DSS), Family Educational Rights and Privacy Act (FERPA), and Health Insurance Portability and Accountability Act (HIPAA). Systems classified as MODERATE may also be mission critical from an availability perspective (e.g. DNS servers).

Standard Operating Procedures (SOP), which outline the specific steps to be taken during the incident response stage of a suspected incident or abuse, are listed as appendices to the Incident Response Plan. UTK IT personnel should be familiar with each SOP and adhere to the standards defined within that procedure.

- Appendix C – Data Exposure Incident SOP
- Appendix D – Compromised Device Incident SOP
- Appendix E – Compromised Account SOP

6. Reporting

Depending on the type of incident or abuse, a report will be created by the affected user or their system administrator. If it cannot be determined whether a report is needed, system owners should contact the OIT HelpDesk for guidance. Answers to the following questions should be included in this report:

1. What is the associated monetary cost?
2. Did the incident disrupt ongoing operations?

3. Was any data irrecoverably lost, and, if so, what was the value of the data?
4. Was any hardware damaged?
5. Was there unauthorized access to information classified as MODERATE?

Incident reports must be disseminated to the parties involved and the support personnel for their records. A copy of each report shall be forwarded to the UTK ISO for review, storage, and reporting.

Analyzing the cost of the incident - Work should be conducted within the organization to quantify the personnel time required for dealing with the incident (including time necessary to restore systems).

Deriving a financial cost associated with an incident will help those who may be prosecuting any suspected perpetrators, and will aid in the justification of funding for future security initiatives.

7. Follow-up

Performing follow-up activity is one of the most critical actions in responding to incidents. This helps the UTK campus improve their incident handling processes as well as aid in the continuing support of any efforts to prosecute those who have broken the law or abused any UTK information technology resources. If it cannot be determined whether a follow-up is needed, information owners should contact the OIT HelpDesk for guidance. Follow-up actions include the following:

a) Define the "lessons learned"
b) Analyze what has transpired and what was done to intervene.
c) Was there sufficient preparation to prevent the incident?
d) Did detection occur promptly? If not, why?
e) Could additional tools have helped the detection and recovery process?
f) Was the incident sufficiently contained?
g) Was communication adequate, or could it have been better?
h) What practical difficulties were encountered?

The follow-up phase ensures continuing improvement to the quality of the IRP. Every effort should be made to complete follow-up documentation within 90 days of closing an incident.

Appendix A- UTK Information Technology Security Glossary of Terms

Acceptable Use Policy (AUP) – The University of Tennessee Information Technology Policy IT0110 – Acceptable Use of Information Technology Resources implements the general principles established by UT Fiscal Policy FI0805 regarding the appropriate use of information systems equipment, software, and networks. This policy applies to all users (including but not limited to, staff, faculty, students, contractors, consultants, and visitors) while using UTK information systems resources.

Applicable Laws of the State of Tennessee and the Federal Government – Any laws in the state of Tennessee or from the federal government that apply to security and information technology, information technology resources, or electronic information transmission technologies.

Computer System – An electronic device that uses common storage and executes code for designated data manipulation that is user-written. This includes all portable devices including, but not limited to, laptop computers, personal digital assistants, and all mobile email devices.

Security Incident Response Team (SIRT) – The Security Incident Response Team supports the operations of the Knoxville Area Campus through mitigation of all incidents adversely impacting the confidentiality, integrity, availability, and accountability of information technology resources.

Electronic Information – Refers to information in electronic form and the information technology resource on which the information resides. This does not apply to information in paper form.

Event – An occurrence that has not been verified as a security incident.

Family Educational Rights and Privacy Act (FERPA) – The Family Educational Rights and Privacy Act of 1974, commonly referred to as the Buckley Amendment, protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

Gramm-Leach-Bliley Act (GLBA) – Requires financial institutions to protect the confidentiality and integrity of their customer's information.

Health Insurance Portability and Accountability Act (HIPAA) – Creates a standard for healthcare providers and institutions to protect the confidentiality and integrity of personal health information.

Incident Response – The documented process used by information technology professionals in response to information technology resource compromises, vulnerabilities, and attacks.

Information Security Office (ISO) – The entity that is responsible, under the campus Chief Information Officer (CIO), for the information technology security oversight and administration of the Information Security Program for the University of Tennessee, Knoxville.

Information Systems Support Personnel – In this document, applies to all system administrators, HelpDesk personnel, Desktop Support, the ISO, and any individual at The University of Tennessee, Knoxville campus that support information technology resources.

Information Technology Resources – Includes any computers, computer systems, network devices, telephony systems, or software applications supported by UTK.

NetReg – NetReg is the Office of Information Technology process used to register computer systems on The University of Tennessee, Knoxville network and enable DHCP/DNS services. It can also be used to temporarily "terminate" network access in a majority of the cases.

Payment Card Industry-Data Security Standards (PCI-DSS)- The PCI-DSS provides an actionable framework for developing a payment card security process—including prevention, detection, and appropriate reaction to security incidents.

Security Incident – A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Incidents can include computer intrusions, denial-of-service attacks, insider theft of information, copyright violations, and any unauthorized or unlawful activity that requires support personnel, system administrators, or computer crime investigators to respond.

Standard Operating Procedure (SOP) – The Standard Operating Procedure (SOP) implements the general principles established by the Incident Response Plan (IRP) regarding the specific steps which UTK personnel must follow when responding to an abuse or incident.

System Administrators (SA) – The University of Tennessee, Knoxville campus employees that are responsible for Information Systems (including the security controls for the system) within a department or group.

Users – Refers to all students, faculty, staff and others while accessing, using, or handling the University of Tennessee, Knoxville's information technology resources. "Others" includes, but is not limited to, subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities granted access.

Appendix B- UTK Information Technology Security Glossary Definition of Responsibilities

Desktop Support Services –Desktop Support Services provides direct interactive support for users experiencing security incidents that do not have a SA in place or require additional expertise. Desktop Support Services personnel shall instruct the user not to reboot, disconnect, or otherwise alter the system when a confirmed event has been discovered, unless directed by a member of the SIRT. Otherwise, collection of valid evidence is negatively impacted by losing critical information stored in system memory. Users/SAs can contact the OIT HelpDesk to report when a machine has been cleaned or rebuilt.

HelpDesk – The OIT HelpDesk is the first level of interaction for users experiencing security events. It is the OIT HelpDesk's responsibility to coordinate incoming information on a per user basis, advise individual users on handling individual security events or incidents, and forward information relating to an event or incident to The University of Tennessee, Knoxville ISO. The OIT HelpDesk shall instruct the user not to reboot, disconnect, or otherwise alter the system when a confirmed incident has been discovered, unless directed by The University of Tennessee, Knoxville ISO (or designated SIRT Team member) or the incident is unlikely to be prosecuted and additional forensic information gathering is unnecessary. Otherwise, collection of valid evidence can be negatively impacted by losing critical information stored in system memory.

Incident Analyst – Responsible for performing the analysis of a particular incident. This shall include determining the cause of the incident, the impact to the campus, and the recommended response. This task will usually be assigned to a member from The University of Tennessee, Knoxville ISO or designee.

Incident Investigator – Responsible for the gathering of all necessary information pertaining to the abuse and/or security incident and for the tracking and reporting of specific incidents. Establishes and maintains open channels of communication between the affected groups and The University of Tennessee, Knoxville ISO. This will typically be someone from OIT HelpDesk, OIT Desktop Support Security, Network Services Security, and/or The University of Tennessee, Knoxville ISO.

Information Security Office (ISO) – The University of Tennessee, Knoxville Information Security Office (ISO) is responsible for coordinating information security efforts within the University of Tennessee, Knoxville campus. In addition, the ISO is accountable for actively monitoring key intrusion detection and intrusion prevention systems, assisting in vulnerability assessments, and overseeing forensic investigations. When necessary, the UTK ISO or CIO will mobilize the Security Incident Response Team (SIRT) to review the incident and respond according to the specific SOP. The ISO will coordinate the response with system administrators, the OIT HelpDesk, Desktop Support Security, Network Services Security, security personnel, and other agencies as necessary (including but not limited to Campus Police, Student Affairs, Public Relations, Office of the General Counsel, and the Federal Bureau of Investigation). The ISO is also responsible for notifying the Chief Information Officer (CIO) regarding security incidents to obtain additional direction as necessary.

Network Services (NS) – The Network Services team will work in conjunction with the OIT HelpDesk, Desktop Support Security, and the ISO in order to identify, analyze, and respond to suspected and verified security incidents. Such responses may include disabling or re-enabling network ports, port scanning, and altering router access control lists or firewall policies.

OIT Student Security – This is a subgroup of the HelpDesk responsible for disabling, enabling, and/or un-registering hardware addresses in NetReg, investigating security events and incidents, sending requests to NS for ports that are to be disabled/enabled, and tracking security incidents for students. Student Security is also responsible for disseminating incoming information on a per user basis, advising students on handling individual security events, and forwarding information relating to an event to the ISO and the Vice Chancellor for Student Affairs.

Security Analyst – Serves as the technical resource, responsible for proposing countermeasures for hardening various systems and platforms supported within the university. This role will be assigned by the UTK ISO.

SIRT Incident Handler(s) – Responsible for leading a particular incident response operation or effort. This task can be assigned to any member of the SIRT team depending on the nature of the task.

SIRT Team Leader – Responsible for the overall administrative and personnel management of the team. This task will be assigned by the Chief Information Officer, the Information Security Officer, and/or an OIT Director.

System Administrator (SA) – The SA is the first level of interaction for users that are experiencing a security event or incident. It is the system administrator's responsibility to coordinate incoming information, advise users on handling security events, forward information to the UTK ISO, and disseminate information to users and other system administrators as appropriate. The system administrator must not reboot, disconnect, or otherwise alter the system when an event has been discovered, unless directed otherwise by a member of the SIRT or the ISO. Otherwise, collection of valid evidence is negatively impacted by losing critical information stored in system memory. The system administrator is responsible for monitoring the systems within their department to identify unusual behavior or symptoms, which may indicate a security incident. These indications are further outlined in the detection portion of this document.

Users – Responsible for monitoring unusual system behavior, which may indicate a security event. The indications of a security event are further outlined in the incident verification section of this document. Users are responsible for reporting events to their local system administrator, the UTK ISO, the OIT HelpDesk, Desktop Support, or Network Services immediately. The user must not reboot, disconnect, or otherwise alter the system when an event has been discovered, unless directed otherwise by a SA, a member of the SIRT or the ISO. Otherwise, collection of valid evidence can be negatively impacted by losing critical information stored in system memory.

Appendix C – Data Exposure Incident SOP

Responsibilities

Whenever the Office of Information Technology (OIT) is notified of a data disclosure or a potential data exposure, specific steps should take place to work with university officials to determine a course of action to ensure compliance with federal and state regulations. The department responsible for the exposure should inform their department head and respective Vice Chancellor of the incident and work with the Office of General Counsel and the UTK Information Security Office to determine appropriate action(s).

The department responsible for the exposure assumes primary responsibility for dealing with issues of the exposure according to the UTK procedure listed here. They should work with system owners to verify the classification of the data and take responsibility for developing a communications plan that includes any publicity, notification to individuals and others, and necessary remediation.

The group or department responsible for the data exposure is responsible for contacting individuals affected by the exposure and must consult with the UTK Office of Communications, OIT Security Office and the Office of General Counsel to develop a communication plan.

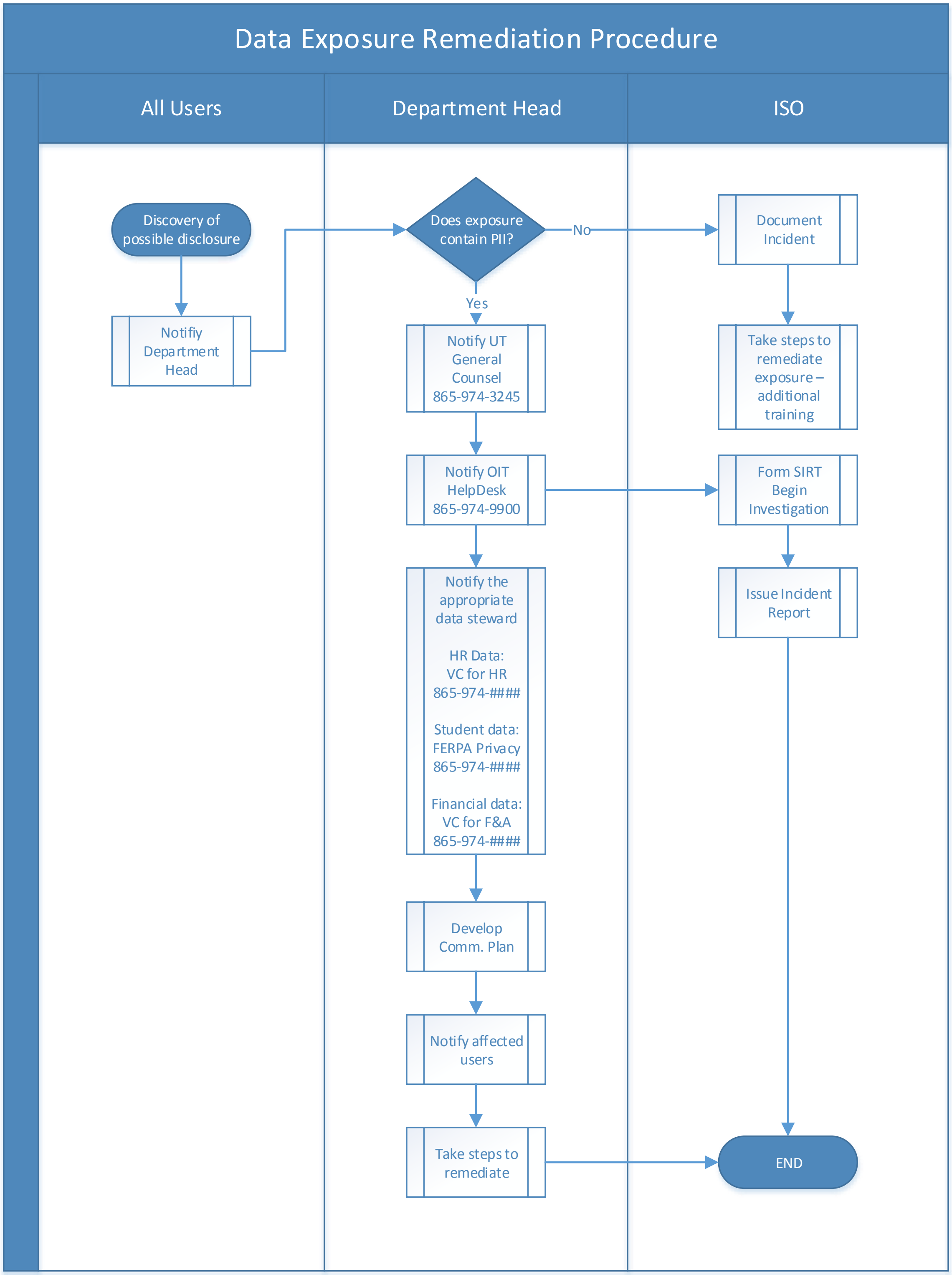
PII-Personally Identifiable Information

Personally identifiable information (PII), including information classified as MODERATE, is covered by The University of Tennessee Data Breach Notification Policy, IT0121. “Personal information” means an individual’s first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted:

(i) Social security number;
(ii) Driver license number; or
(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

“Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Data Exposure Remediation Procedure


Data Exposure Remediation Procedure
All Users
Department Head
ISO
Discovery of possible disclosure
Notifiy Department Head
Does exposure contain PII?
No
Yes
Document Incident
Take steps to remediate exposure – additional training
Notify UT General Counsel 865-974-3245
Notify OIT HelpDesk 865-974-9900
Form SIRT Begin Investigation
Notify the appropriate data steward
HR Data: VC for HR 865-974-####
Student data: FERPA Privacy 865-974-####
Financial data: VC for F&A 865-974-####
Issue Incident Report
Develop Comm. Plan
Notify affected users
Take steps to remediate
END

Notification Examples

Examples of contact letters have been provided below to help guide the process of contacting those who have had their data exposed. The examples use a scenario of data exposures through email and a stolen device. The contact template could easily be changed to reflect a data exposure through a lost digital storage device. Contact the OIT HelpDesk and Office of General Counsel to coordinate a communications plan.

Example of PIRN data exposure through email

<DATE>

<Addressee>

You are receiving this letter because on ***<date>,*** a handling error in our office resulted in a file containing some of your confidential data being sent to an incorrect e-mail address for which we cannot identify the owner.

The data file included the following information from your application to our program:
<List of data elements>

We have no evidence that an unauthorized individual has actually utilized any of this information, and notice was sent to the recipient's address advising that the file was sent in error and requesting that it be destroyed. We are bringing this incident to your attention, in accordance with Tennessee law, so that you can be alert to signs of any possible misuse of your personal identity.

As the situation develops, we will send additional messages regarding any further information which we are able to discover. Please monitor your email in the coming days for messages from our office. We have also changed our handling procedures such that files containing confidential data are transferred through vehicles other than e-mail. If you have any questions, please contact our department at ***<department email***>.

We apologize for this lapse and for any inconvenience it may cause.

Sincerely,

<Signature>

Example of stolen/lost device with PII

<Date>

Dear **<*student name*>:**

The University of Tennessee, Knoxville recognizes the importance of safeguarding your personal information. To that end, we have implemented strict administrative, technical, and physical safeguards to protect that information. However, even the most rigorous safeguards cannot guarantee protection against criminal conduct. University of Tennessee, Knoxville officials have been notified of the theft of a laptop computer that contained a file that held some of your personal information. Specifically, the file contained **<*list of items*>** from several years ago.

Although we believe this theft was directed at the hardware, and not the contents, we wanted to act preemptively to notify you of this situation and inform you of the risk. We do not have evidence that anything has been done with the information, but we are bringing this incident to your attention so that you can be alert to signs of any possible misuse of your personal identity. We will continue to monitor the situation, and recommend you take precautionary steps to guard yourself against any potential identity theft.

[We have established a website at **<*(URL)*>** to provide you with information].**(Optional)** You may place a fraud alert with credit bureaus and/or periodically run a credit report to ensure accounts have not been activated without your knowledge. If you determine that an account has been fraudulently established using your identity, you should contact law enforcement and the financial agency with which the account was established. The following references provide additional information about identity theft:

- Federal Trade Commission website on identify theft (http://www.consumer.gov/idtheft/)
- Social Security Administration Fraud Line at 1-800-269-0271
- Major Credit Bureau Numbers
    - Equifax 1-800-525-6285
    - Experian 1-888-397-3742
    - Trans Union 1-800-680-7289

As an additional safeguard, you may choose to place a temporary “fraud alert” on your credit report. Fraud alerts can help prevent an identity thief from opening any accounts in your name. You are encouraged to contact the toll-free fraud number of one of the three main consumer reporting companies to place a fraud alert on your credit report. The toll-free number for one of the three, Equifax, is shown above. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report as well

The University of Tennessee, Knoxville is committed to maintaining the privacy of present/past student information and takes many precautions for the security of personal information. Although social security numbers are no longer used for identification purposes in our automated systems, the files on the stolen laptop preceded the new identification policy and most records still contained the social security number. We sincerely regret any inconvenience this incident presents to you.

If you have any questions, please contact our department at <***department email***>.
Sincerely,
<Signature>

Appendix D – Compromised Device Incident SOP

Responsibilities

Whenever The University of Tennessee, Knoxville (UTK) is notified of a device or potential device compromise, specific steps should take place to work with the user and university officials to evaluate the nature of the compromise and ensure compliance with federal and state regulations. This applies to university-owned devices or personal devices accessing university resources.

The actions taken are dependent on factors including the security classification (LOW, MODERATE, HIGH) of the device and the university affiliation of the primary user (e.g. Faculty, Staff, or Student). The department responsible for the compromised device should inform their department head of the incident and work with the Office of General Counsel and the UTK Information Security Office to determine appropriate action(s).

The department responsible for the device or employee who owns the device assumes primary responsibility for dealing with issues of the compromise according to the UTK procedure listed here. They should work with the primary user or owner to verify the classification of the data and take necessary steps for developing a communications plan that includes any publicity, notification to individuals and others, and necessary remediation.

The user, group or department responsible for the compromised device is responsible for contacting individuals affected by any exposure of sensitive data existing on the device (see Appendix C for Data Exposure Incident). Further, they must consult with the UTK Office of Communications, UTK Information Security Office and the UT Office of General Counsel to develop the necessary communication plan.

OIT Procedures for Responding to the report of a compromised device

The following outlines the standard operating procedures that should be followed in response to the report of a compromised device (either personal or university-owned) that could adversely impact the network and/or AUP policy violations. If the device is personally owned, it is up to the owner to see that the issue is addressed. If the device is university-owned, it is up to the department to see that the issue is addressed.

Level 0

Description

Machines at this level are considered at risk. Users will be notified of the potential threat that could lead to a compromise or infection in the future.

Action Taken by OIT

Upon detection, a Footprints ticket will be generated to log the incident and the owner as designated in NetReg will be sent an email informing them of the potential threat.

Action Required by the User

No action required

Examples:

- Potential problems found proactively
- Notification by an outside source (REN-ISAC, MS-ISAC)

Level 1

Description

Machines at this level are considered vulnerable to known exploits and a threat to the network or to other devices. The user must take some action or he will be cut off from the network.

Action taken by OIT

Upon detection, a Footprints ticket will be generated to log the incident and the user will be sent an email with the appropriate instructions on how to correct the problem. If the user does not correct the problem within 24 hours, the NetReg entry will be disabled.

For devices belonging to students:

The ticket will be assigned to OIT_StudentSecurity (students) and set to a status of Pending Infected.

After 24 hours, if this machine shows up again, the ticket status will be changed to Pending 2BDisabled and assigned to OIT_TCSSecurity. The NetReg entry will be disabled and the case will be assigned to OIT_StudentSecurity.

For devices belonging to faculty/staff:

The ticket will be assigned to OIT_DesktopSupportSecurity and set to a status of Pending Infected.

After 24 hours, if this machine shows up again, the ticket status will be changed to Pending 2BDisabled. The NetReg entry will be disabled by Desktop Support Security

Action Required by the User

User must take the action requested within 24 hours.

Examples:

- Patch has not been applied to prevent known exploits (i.e. vulnerabilities like MS04-011 or the HEARTBLEED bug)
- Virus/Worms
- Notification by an outside source (REN-ISAC, MS-ISAC)

Level 2

Description

Machines at this level have been found to be compromised.

Action Taken by OIT

Upon detection, a Footprints ticket will be generated to log the incident and the user will be sent an email letting him know of the problem and the appropriate action that needs to be taken. The user's NetReg entry will be disabled. In addition, the network access will also be blocked (i.e. the network port will be disabled and/or the MAC address will be blocked on wireless).

For devices belonging to students:

The ticket will be assigned to OIT_TCSSecurity. We will immediately disable the entry in NetReg. Network Services will be notified to disable the network port and/or wireless access. Once finished, assign the case to OIT_StudentSecurity. When the student has brought the computer to the Service Center, Student Computer Support or HelpDesk staff can enable NetReg & facilitate the enabling of the network port/wireless access.

For devices belonging to faculty/staff (personal or university-owned):

The ticket will be assigned to OIT_DesktopSupportSecurity. We will immediately disable the entry in NetReg. Network Services will be notified to disable the network port and/or wireless access.

Action Taken by the User

The user must address the compromise and/or problem before OIT will enable the user's NetReg entry and network port.

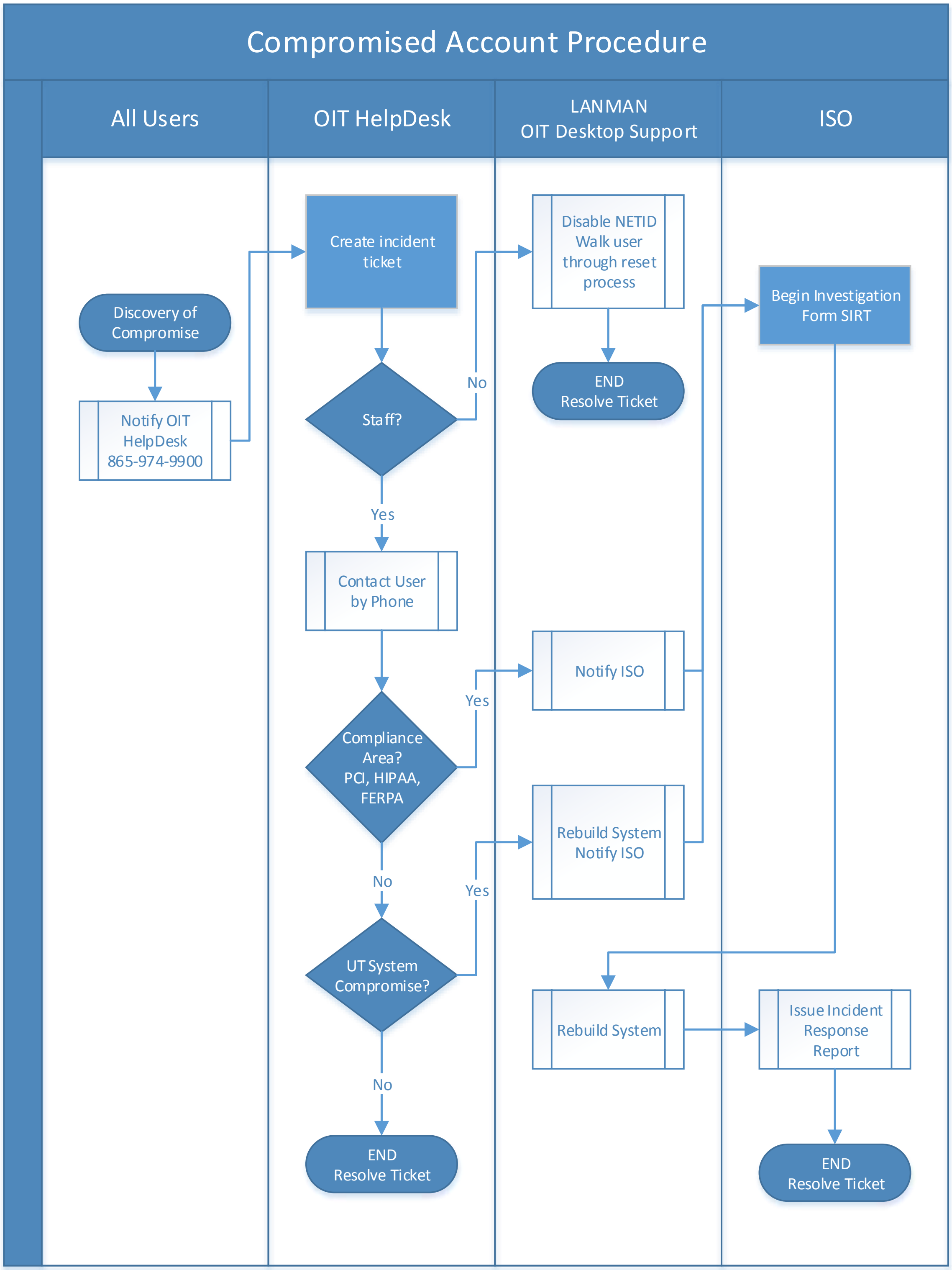
The user must rebuild his/her computer. If this is a university-owned device, the department is responsible for seeing that the machine is rebuilt.

Examples:

- Compromised computers
- Rogue DHCP servers
- Denial of service attacks
- Unauthorized scanning
- Trojans

Notification by an outside source (REN-ISAC, MS-ISAC)

Appendix E – Compromised Account Procedure


Compromised Account Procedure
All Users
OIT HelpDesk
LANMAN
OIT Desktop Support
ISO
Discovery of Compromise
Notify OIT HelpDesk 865-974-9900
Create incident ticket
Staff?
No
Yes
Contact User by Phone
Compliance Area? PCI, HIPAA, FERPA
Yes
No
UT System Compromise?
Yes
No
END Resolve Ticket
Disable NETID Walk user through reset process
END Resolve Ticket
Notify ISO
Rebuild System Notify ISO
Rebuild System
Begin Investigation Form SIRT
Issue Incident Response Report
END Resolve Ticket