Roane State
COMMUNITY COLLEGE

Cyber Incident Response Plan

Prepared by:

Tim Carroll
Assistant Vice President and Chief Information Officer
Information Technology
September 2016

Version 1.0

Executive Summary

The State of Tennessee, Treasury Department, Division of Risk Management and Claims Administration, has purchased Cyber Liability Insurance Coverage to protect State Agencies and Departments including Roane State Community College as part of the Tennessee Board of Regents. This Cyber Incident Response Plan[1] (CIRP) supports this protection with a plan for discovery, investigation, response and remediation. It includes procedures for technical staff and users for detailing, communicating, responding to, and reporting security incidents. This plan is an extension of information security practices, where potential incidents are identified and passed to this plan for further review and processing.

A security incident refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include but are not limited to unauthorized access, malicious code, network probes and denial of service attacks. *(See Appendix C for a glossary of terms.)*

The CIRP will assist with decision making, internal and external coordination, unity of effort, and minimization of reputational and financial losses. The CIRP provides operational instructions for the discovery of a cyber-breach, the investigation and remediation process, the assembly of the internal response team, determining the escalation level, contacting law enforcement, the utilization of vendors, the notification process, establishing a call center and post incident lessons learned.

Cyber incidents can be accidental or malicious actions or events that have the potential of causing unwanted effects on the confidentiality, integrity and availability of State information and IT assets. Cyber incidents include, but not limited to, theft or loss of physical equipment, illegal access to systems or information, and failing to protect and secure electronic Personal Identifiable Information (PII) and/or Personal Health Information (PHI). These situations cause institutions to face unnecessary expense in productivity, significant damage to systems and damage to reputation.

The goal of this CIRP is to assist Roane State Community College with managing a cyber-security event or incident for the purpose of mitigating damages, increasing the confidence and trust of all stakeholders and to reduce the recovery time and costs of a cyber-security breach. The CIRP will assist with decision making, internal and external coordination, unity of effort, and minimization of reputational and financial losses for an organization achieved through the implementation of procedures outlined in this plan. The CIRP provides operational instructions for the discovery of a cyber-breach, the investigation and remediation process, the assembly of the internal response team, determining the escalation level, contacting law enforcement, the utilization of vendors, the notification process to TBR, establishing a call center and post incident lessons learned.

[1] Plan based on Example Document, “Cyber Incident Response Plan”, by State of Tennessee, Treasury Department Division of Risk Management Claims Administration. The Tennessee Board of Regents Cyber Incident Response Plan has been incorporated into this plan.

Effective planning must incorporate coordination across all business functions, for example, organizational communications among leadership, regulatory affairs, legal, compliance and audit and operational functions. Internal coordination, combined with easily accessible documentation of CIRP, ensures that all levels of an organization can react with greater alertness during an incident.

Mandatory requirements are in **bold**.

Document Control

Document Version

Version No.	Version Date	Author	Summary of Changes
1.0	9/7/2016	Tim Carroll	Initial Document

Official Approvals

Original Signed-

____

Dr. Chris Whaley Date
President, Roane State Community College

____

Danny Gibbs Date
Executive Vice-President, Business and Finance, Roane State Community College

Approval Dates

This plan and all updates have been reviewed and approved on the dates listed below:

Name	Title	Date of Approval	Version No.
Dr. Chris Whaley	President	13-Feb-17	1.0
Danny Gibbs	Executive Vice-President Business and Finance	13-Feb-17	1.0
Tim Carroll	Assistant Vice President and Chief Information Officer	13-Feb-17	1.0

Record of Distribution

A hard copy of the plan is kept in the Information Technology office. Electronic copies of this plan are kept on the Information Technology SharePoint Policies and Procedures site under Section 1. General (100), and on Office 365 Information Technology Disaster Recover Site. The plan and all updates should be distributed electronically to the following who will distribute to additional staff as necessary:

Office	Date of Distribution
President	13-Feb-17
Executive Vice President, Business and Finance	13-Feb-17
Assistant Vice President & CIO, Information Technology	13-Feb-17
Vice President, Academic Services	13-Feb-17
Vice President, Institutional Effectiveness and Research	13-Feb-17
Vice President, Workforce Development and Student Affairs	13-Feb-17
Executive Director Oak Ridge Branch Campus and Community Relations	13-Feb-17
Director, Internal Audit	13-Feb-17
Chief of Police	13-Feb-17
Help Desk	13-Feb-17

Acronyms Used in this Document

Below are commonly used acronyms found in this document. Appendices B and C provide further definitions and explanations for some of these terms.

CIO – Chief Information Officer

CIRP – Cyber Incident Response Plan

EMT – Executive Management Team

FERPA - Family Educational Rights and Privacy Act

IDPS - Intrusion Detection/Prevention Systems

IL – Incident Lead

IRS - Incident Response Support-Treasury

IRT – Incident Response Team

IRT PC – Incident Response Team Primary Contact

NTTS – Networking, Telecommunications & Technical Services

PCI – Payment Card Industry

PCI DSS – Payment Card Industry Data Security Standard

PHI – Personal Health Information

PII – Personally Identifiable information

PIO – Public Information Officer

RSCC – Roane State Community College

PR – Public Relations

SSN – Social Security Number

STS - Strategic Technology Solutions

TBR – Tennessee Board of Regents

Overview

Purpose

The Cyber Incident Response Plan (CIRP) is required in order to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of Roane State Community College’s Computer Resources and securing Personally Identifiable Information (Pll) and Protected or Personal Health Information (PHI). This adverse event may be malicious code attack, unauthorized access to Roane State Community College’s systems, unauthorized use of Roane State Community College’s services, general misuse of systems, and failure to secure PPI and PHI information and other information classified as sensitive under the institution’s data classification policy and procedures.

Goals

The goals of this CIRP are to assist Roane State with managing a cybersecurity event or incident including:

- mitigating damages,
- minimizing disruption to academic, business, network operations and other college processes
- increasing the confidence and trust of all stakeholders
- reducing the recovery time and costs of a cyber-security breach
- allowing for legal (to include criminal and/or civil) actions against perpetrators
- providing accurate reports and useful recommendations

Scope

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

Document Review and Revision Schedule

This document will be reviewed annually for informational updates for names, titles, and contact information and will be reviewed annually for procedural, policy and other updates.

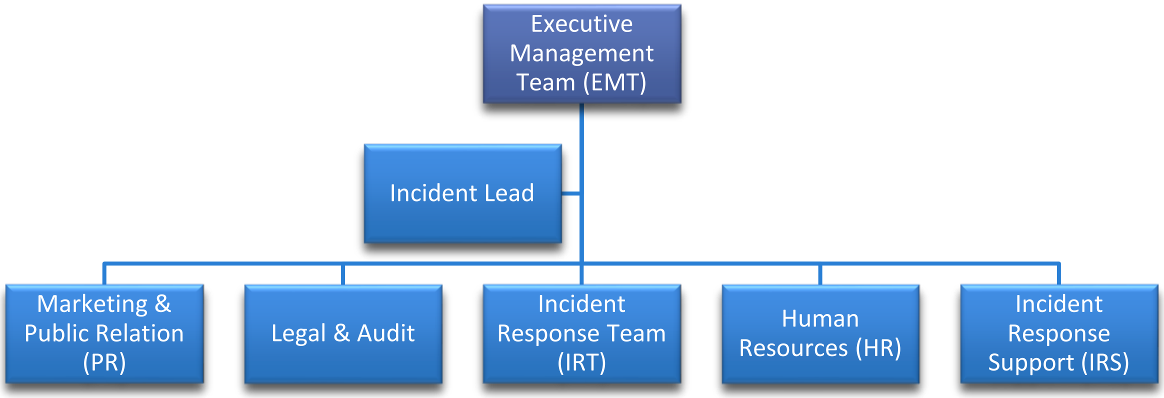
Incident Response Team

The Assistant Vice President of Information Technology and Chief Information Officer, or designee, is responsible for maintaining and overseeing the incident response process and assigning members to the Incident Response Team. The Incident Response Team has the authority to monitor suspicious activity and to disconnect equipment that are in violation of College, campus, state or federal regulations.

The Incident Response Team is accountable to the CIO for the investigation, declaration, analysis, and disposition of an incident. The membership of the Incident Response Team is dependent on the type of incident and the means necessary to mitigate its effect on the confidentiality, integrity or availability of information resources.

To adequately respond to an intrusion or incident, predetermined teams will participate depending on the incident characteristics. As the situation develops and the impact becomes more significant, the various teams will be called to contribute.

See Appendix A: Incident Response Teams Contact List *for list of names and contact numbers for team members.*


Executive Management Team (EMT)
Incident Lead
Marketing & Public Relation (PR)
Legal & Audit
Incident Response Team (IRT)
Human Resources (HR)
Incident Response Support (IRS)

Purpose

The purpose of Roane State Community College Incident Response Team (IRT) is to:

- Protect Roane State Community College information assets.
- Provide subject matter expertise with managing and handling incidents.
- Determine the extent to which the incident poses problems related to identity theft, loss of individuals' privacy or confidentiality or the security of Roane State Community College information and systems.
- Manage activities to recover from the breach and mitigate the resulting damage, including decisions relating to external breach notification.
- Implement the response plan, engage the proper resources and track the efforts and the progress of containing the breach.
- Prevent the use of Roane State Community College systems in attacks against other systems (which could cause us to incur legal liability).
- Minimize the potential for negative exposure with Roane State Community College’s reputation and regaining and building public trust.

Goals

The objectives of Roane State Community College Incident Response Team are to:

- Contain and minimize threat.
- Determine the source of the incident.
- Identify key tasks, manage timelines and document all response efforts from beginning to end.
- Assign and establish team roles and responsibilities, along with specifying access credentials.
- Determine how the incident occurred.
- Avoid escalation and further incidents from specific breach.
- Limit immediate incident impact to customers and partners.
- Summarize the steps needed to assess the scope of a breach.
- Assess the impact and damage in terms of financial harm, reputational harm or other harm.
- Recover from the incident.
- Outline the budget and resources needed to handle a breach.
- Find out how to avoid further exploitation of the same vulnerability.
- Recommend updates to policies and procedures as needed.
- Ensure contact lists remain updated and team members remain ready to respond.
- Analyze response efforts post-breach to better prepare Roane State and the Incident Response Team for the next incident.

Incident Response Team Responsibilities

Incident Response Team Members should be responsible for the following areas:

- Determining the tools and technology utilized in intrusion detection,
- Performing appropriate pre-incident activities (e.g. monitoring network activity, vulnerabilities, logs, etc.)
- Defining and classifying incidents,
- Determining if an incident should be investigated and the scope of such an investigation (i.e. law enforcement agencies, forensic work)
- Securing the network
- Conducting follow-up reviews.

See Appendix B: Roles and Responsibilities *for more detail covering the responsibilities of specific personnel.*

Incidents

Common Attack Methods

Events can be detected through automated or manual means. Automated detection capabilities include RSCC's network-based and host-based Intrusion Detection/Prevention Systems (IDPSs) and antivirus/antimalware software. Incidents may also be detected through manual means, such as problems reported by users or observations of abnormal resource utilization, suspicious account activity and log analysis. Additionally, RSCC may receive reports from sources external to the College that have detected issues and reported the activity. Although incidents occur in many ways, this plan focuses on the procedures to handle incidents that use the following common attack vectors:

- **Theft or Loss of Physical Equipment** - A data breach can occur with the theft or loss of physical equipment which stores data, such as laptop computers or memory storage devices.

- **Illegal Access to the Systems or Information** - A data breach can occur through malicious code delivered via external/removable media or email, denial of service attacks, unauthorized access, and unlawful access to personally identifiable information or Pll data by technological means such as hacking into existing computer systems or hijacking computers with viruses, worms or Trojans. Once inside a system, a cyber-criminal can steal data, infect it or overload computer systems.

- **Insiders** - A data breach can be committed by current employees, ex-employees or even through social engineering where an employee is tricked into providing access or unauthorized release of sensitive information either within or outside of the State such as, but not limited to, phishing, spear phishing, hacking into social networks, and other socially-engineered activities.

- **Oversight** - A data breach can occur when no one thought the information needed to be protected and no precautions were taken to safeguard the data in the first place.

Response Stages

The defined stages of response include:

1. Preparation
2. Incident Discovery/Detection
3. Triage and Analysis
4. Eradication and Recovery
5. Initial Notification
6. Follow-Up

Preparation

Knowing how to respond to an incident BEFORE it occurs can save valuable time and effort in the long run through the practice of table top exercises and annual training. A review of existing information system(s) and data identifies where personally identifiable information (Pll), protected health information (PHI) and other sensitive information resides. This can be done by the following:

- Documenting what Pll, PHI and other information classified as sensitive under the institution's data classification policy and procedures is maintained by your organization, where it is stored (including backup storage and archived data), and how it is kept secure;
- Conducting regular risk assessments and evaluating privacy threats for your organization, as well as any contractors, vendors, and other business partners;
- Reviewing who is approved for access to Pll, PHI and/or other sensitive information and checking user activity status to determine which accounts should be deactivated after a pre-determined period of inactivity;
- Reviewing separation of duties to help ensure integrity of security checks and balances as employees should only have access to information related to their job function;
- Implementing mitigation controls designed to prevent and detect unauthorized access, theft or misuse of Pll, PHI and/or other sensitive data, which includes hard copy files;
- Implementing security controls, such as encryption of sensitive data in motion and at rest (where feasible);
- Regularly reviewing and keeping up-to-date your data destruction policies, to minimize the risk of data breaches through unauthorized access to archived media or computers that are no longer in use; and
- **Annual reviewing and updating this response plan and annually conducting table top exercises that include the Executive Management Team.**

Incident Discovery/Detection

It is important that anyone who reports a security incident provides as much relevant information as possible. Based upon the type of the incident, notifications need to go to the appropriate people in the Incident Classification Chart. Additionally, the Incident Response Team will identify the appropriate technical teams that are needed to assist with the analysis phase of the incident.

Observing one of the following events is generally inconclusive. However, a combination of any the following activities can represent a security event and should be investigated:

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

Any event, suspected or known, that involves PII should be reported.

Triage and Analysis

This involves limiting the scope and magnitude of an incident because some incidents may involve malicious code and these types of incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment. This involves the containment of stolen or unauthorized access to electronic stored data or dissemination of information to an external database. During this phase of the incident handling, it is important to initially identify the criticality of the incident (this may be changed during the analysis phase). This will be done by the Incident Lead and Incident Response Team.

The Incident Lead and Incident Response Team should consider and determine that an incident may have a state-wide impact. The Incident Lead and Incident Response Team will undertake appropriate root cause analysis and actions to minimize the risk to state's core business operations. In addition, the IRT will utilize the evidence handling and forensics processes outlined in Appendix H: Data Exposure Standard Operating Procedure (SOP). The college may need to hire a Certified Forensics Investigator or turn the incident over to law enforcement depending on the magnitude of the event.

Eradication and Recovery

Restoring a system to its normal business status is essential. Once a restore or recovery has been performed, it is important to verify that the restore operation was successful and that the system is back to its normal condition or the breached data has been contained.

- A computer forensic examination of all loss of data shall be conducted to determine all possible external electronic storage locations.

- This computer forensic examination shall also verify if the breached data has or has not been disseminated to any other known or unknown external electronic location.
- The Incident Lead shall document all ongoing events, all people involved and all discoveries into a timeline for evidentiary use.
- The Executive Management Team will determine if external notification process shall be activated (affected individuals, affected businesses, local law enforcement, FBI and/or contracted cyber response vendors).
- To determine whether notification of a breach is required, the likely risk of harm caused by the breach and then the level of risk must be assessed.
- A wide range of harm should be considered, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach. Removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators or dismissing employees.
- Determine whether PII was accessed as well has how many records or individuals were compromised.

Initial Notification

Identify whether or not an incident has occurred. If one has occurred, the incident response team (IRT) can take the appropriate actions.

If the initial cyber incident is determined to be moderate or high, the Executive Management Team shall notify and activate appropriate segments of the Incident Response Team and determine if Tennessee Bureau of Investigation involvement is warranted. **Agencies shall report actual or suspected data breaches and significant cyber security incidents within 24 hours of discovery to the Tennessee Board of Regents. TBR will notify the State Comptroller, the State Treasurer, and the Treasury Department, Division of Risk Management Claims Administration.**

Depending on the totality of the circumstances, notification to the State Attorney General, the Executive Branch, and other agencies as applicable, and, if determined, members of the General Assembly will be determined by TBR. **All Departments are still subject to audit by the Comptroller of the Treasury authorized by Tennessee Code Annotated, Section 8-4-109(a)(2).**

- **The highest appointed official in the Executive Management Team will notify the State of Tennessee Board of Regents Chancellor.**

- The internal notification process shall include details of the incident, initial risk rating (Low, Moderate, High or Very High), as well as the actions that have been taken to respond to the incident thus far.

- Upon discovery, the Incident Lead of the Incident Response Team shall report actual or suspected breaches, significant breaches of departmental data or significant cyber security incidents to the Executive Management Team and as soon as possible to the Tennessee Board of Regents. TBR will then notify, as appropriate, the Department of Treasury, Division of Risk Management Claims Administration, with a brief status report of what has occurred as determined by Incident Response Team. The Incident Response Team will work with the Executive Management Team to record the incident information and the details of the breach in the Cyber Incident Investigation Report Form. *(See* Appendix C: Glossary of Terms *for a glossary of terms.)*

In preparing for initial notification, consider the following:

- ✓ How difficult is it to contain the incident?
- ✓ How fast is the incident spreading?

Note: For individual instances of malware, the Incident Response Team should not be activated.

Follow-Up

The Incident Response Team and the Executive Management Team should hold a "lessons learned" meeting with all involved parties after a major incident and, optionally, after lesser incidents as resources permit. This meeting provides a chance to review what occurred, what was done to intervene, and how well intervention worked.

This follow-up can also support any efforts to prosecute those who have broken the law.
This includes, but not limited to, changing Roane State policies as appropriate. After an incident is resolved, all incidents that have reached a severity of Level 4 or higher (see next section for incident classification scheme) will be reviewed and a final incident report will be compiled to ensure that all existing processes were followed and were adequate.

- Schedule a lessons-learned meeting with Incident Response Team and Executive Management Team to discuss any identified improvements to the response plan and the processes to the response that worked well during the incident.
- Determine if other external services, such as law enforcement, insurance company, or cyber vendors, should be considered to assist with future cyber breaches and incidents.
- What is the estimated financial impact to Roane State Community College?
- Will this affect Roane State's image or public trust negatively?
- Maintain logbook of events and develop an investigation report.
- The investigation report will include, describe and answer the following:
    - The description of the data lost, including the amount and its sensitivity or classification level and description of any hardware damaged or lost.
    - For cyber security incidents, the nature of the cyber threat (e.g., Advanced Persistent Threat, Zero Day Threat and data exfiltration).
    - Nature and number of persons affected (e.g., employees, external customers, students, citizens, vendors) and if the incident disrupted ongoing operations.
    - Likelihood data is accessible and usable from unauthorized personnel or cyber criminals.

- Likelihood the data was intentionally targeted.
- Evidence that the compromised data is actually being used to commit identity theft.
- Strength and effectiveness of security technologies protecting data.
- Likelihood the breach may lead to harm and the type of harm. Such harm may include confidentiality or fiduciary responsibility, blackmail, disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty.
- Ability to mitigate the risk of harm.

Incident Classification

Classification of an incident is perhaps the most critical decision in the incident handling process. An incident will be classified as one of six (6) severity levels. These severity levels are based on the impact to Roane State and can be expressed in terms of financial impact, impact to services and/or performance of Roane State mission functions, impact to image or impact to public trust. All security incidents are classified by the actual and potential impacts on day-to-day activities of the college.

Severity	Description	Sensitive Data involved FERPA HIPPA PII PCI	Image and/or Trust	Services Impacted	Multiple Systems Impact
6 – Very High	Multiple systems inoperable or taken offline preventing the performance of daily duties impacting the servicing of customers, or **<u>confirmed</u>** data breach or system compromise of more than one application, system or area, or involving sensitive application or system data.	**X**	**X**	**X**	**X**
5 – High	Single system inoperable or taken offline, preventing the performance of daily duties impacting the servicing of customers, or **<u>confirmed</u>** data breach or system compromise of a single application, system or area involving non-sensitive application or system data.		**X**	**X**	**X**
4 - Moderate	Server(s) is operable with minor damage. Minor damage to facility or business areas which prevents the performance of daily duties which impact the servicing of customers, or **<u>unconfirmed</u>** suspected data or system compromise.			**X**	**X**
3 - Low	Server operable with no significant degradation of performance or more than five end user sites affected by the same MINOR severity event.				**X**
2 - Minor	More than five workstations blocked for reimaging.				**X**
1 – Very Minor	Single workstation blocked for reimage. No data compromise.				

6 – High

Incident Notification

The criticality review must occur within all phases and, as the criticality changes, appropriate notifications need to be made. This criticality review must occur within all phases and, as the criticality changes, appropriate notifications need to be made.

- Incidents suspected or confirmed incidents determined to be MINOR and above: The Incident Response Team Primary Contact will be notified.
- Incidents classified LOW and above will be escalated by the Incident Response Team Primary Contact to the Incident Lead.
- Incidents determined to be MODERATE and above will be escalated by the Incident Lead to the Executive Management Team. At the Executive Management Team's discretion, notification will be given to the Tennessee Board of Regents Chancellor and CIO. TBR will then, as appropriate, notify the Legislative Branch, Treasurer, Comptroller, Secretary of State, Attorney General, and the Executive Branch.

Severity	Minimum Notifications					
Notification	EMT	IL	PIO	Legal/HR /Audit	IRT	IRS
6 – Very High	X	X	X	X	X	X
5 – High	X	X	X	X	X	X
4 - Moderate	X	X	X		X	X
3 - Low		X			IRT Primary Contact	
2 - Minor					IRT Primary Contact	
1 – Very Minor						

There may be times when other notifications need to take place, and the Notification Target is only the minimum notification requirement. The STS and TBR Command Centers are responsible for maintaining up-to-date contact lists. The CIO or designee will contact them to initiate any required contacts that are not already available.

- STS (615) 741- 1001 or (800) 342-3276, option 3
- TBR Chief Information Officer (615) 366-4451

The Incident Response Team shall assess data breaches and incidents involving Pll, PCI, PHI, FERPA, federal tax information, business intelligence information or all other data breaches and incidents with support from Treasury Department, Division of Risk Management Claims Administration. The assessment will be based on the details included in the incident report and will assign an initial potential impact level of Low, Moderate or High. The potential impact levels describe the worst case potential impact on the organization, individual person, employee, or vendor of the breach/cyber incident.

Any data breaches or incidents which involve Institutional Student Information Record (ISIR) data of FASFA Filing Status Information are required to be reported within one (1) business day after the college learns of such an incident to: US Department of Education, Federal Student Aid, 830 First Street, NE, Union Center Plaza, Room 32E1, Washington, DC 20202 or via email to FAFSACcompletion@ed.gov. Additional information can be found in the Student Aid Internet Gateway (SAIG) Participation Agreement form.

The Executive Management Team shall determine, as the incident has more impact (severity level increases), the escalation process that will be invoked to involve appropriate resources.

> *Incidents should be handled at the lowest escalation level that is capable of responding to the incident, with as few resources as possible, to reduce the total impact, and to keep tight control.*

Escalation Considerations

The Executive Management Team will consider several characteristics of the incident before escalating the response to a higher level and prior to the Executive Management Team determining the severity of the data breach.

The following considerations should be answered:

- How widespread is the incident and what is the impact to operations?
- How difficult is it to contain the incident and how fast is the incident spreading?
- What is the estimated financial impact?
- Should law enforcement be notified?

- Will this affect Roane State’s public image negatively?

This table defines the escalation levels with the associated team involvement.

Severity	Minimum Notifications
6 – Very High	EXECUTIVE MANAGEMENT TEAM INCIDENT LEAD INCIDENT RESPONSE TEAM IRS (Incident Response Support-Treasury) PIO/Media Communications (PR) Legal/HR/Audit/Compliance
5 – High	EXECUTIVE MANAGEMENT TEAM INCIDENT LEAD INCIDENT RESPONSE TEAM IRS (Incident Response Support-Treasury) PIO/Media Communications (PR) Legal/HR/Audit/Compliance
4 - Moderate	EXECUTIVE MANAGEMENT TEAM INCIDENT LEAD INCIDENT RESPONSE TEAM IRS (Incident Response Support-Treasury) PIO/Media Communications (PR)
3 - Low	INCIDENT LEAD INCIDENT RESPONSE TEAM PRIMARY CONTACT
2 - Minor	INCIDENT RESPONSE TEAM PRIMARY CONTACT
1 – Very Minor	No Notification

Team Responsibilities at each Escalation Level

6 – High

The Roane State nagement Team and Incident Response Team will determine the appropriate cou n, including notification to affected individuals, the resources needed, and any appropriate remedy options. The Executive Management Team and Incident Response Team shall notify the State of Tennessee Division of Risk Management Claims Administration (DRMCA) for insurance purposes. The Executive Management Team and/or Incident Response Team may request additional support from DRMCA upon request

Escalation Level 1 – Very Minor	
Normal Operations	Monitor all known sources for alerts or notification of a threat. Single workstation blocked for reimage. No data compromised. **NO NOTIFICATION REQUIRED.**

Escalation Level 2 – Minor	
Incident Response Team – Primary Contact	▪ Verify that an incident has actually occurred. This activity typically involves the unit systems administrator and end user, but may also result from proactive incident detection work of the Security Office or central IT operations. If it is determined that an incident has occurred, inform appropriate authorities. ▪ Monitor all known sources for alerts or notification of a threat. More than five workstation blocked for reimage. No data compromised. ▪ Determine if the Incident Lead needs to be contacted to escalate to Levels 3, 4, 5, or 6.

Escalation Level 3 - Low	
Incident Response Team - Primary Contact	▪ Conduct a thorough assessment of the type and scope of data exposed following applicable laws, regulation, and policy. ▪ Determine initial defensive action required. ▪ Prepares the Incident Report Form if not already completed.

Incident Lead	▪ Notify the Incident Lead. ▪ Server operable with no significant degradation of performance, or more than five end user sites affected by the same minor severity event. ▪ Take steps to remove the cause of the exposure, reduce the impact of the exposure of the sensitive data, and restore operations if the incident compromised or otherwise put out of service a system or network, and ensure that future risk of exposure is mitigated. ▪ Based upon the incident classification, determine if an "Executive Communications Team" needs to be formed. ▪ Receive and track all reported potential threats. ▪ Escalate Incident Response to appropriate Escalation Level if a report is received indicating that the threat has manifested itself. ▪ Determine relevant assignment of tasks for personnel to conduct the assessment the data breach has been confirmed. ▪ Alert IT organizations and applicable support organizations of the potential threat and any defensive action required. ▪ Alert the Executive Management Team and the Communication Team of the potential threat if determined the incident needs to escalate to Levels 4, 5, or 6. ▪ Alert Legal, Audit and Compliance of the potential threat if determined the incident needs to escalate to Levels 5 and 6. ▪ Notify the Incident Response Support Team (DRMCA) of the potential threat if determined the incident needs to escalate to Levels 4, 5, or 6.

Escalation Level 4 - Moderate	
Executive Management Team (EMT)	▪ Assume responsibility for directing activities in regard to the incident. ▪ Determine whether Escalation Level 4 is appropriate or escalate to Level 5, or possibly Level 6. ▪ Determine when the risk has been mitigated to an

	acceptable level. ▪ President determines when internal notification process should be activated. ▪ President determines if Tennessee Bureau of Investigation notification process should be activated. ▪ Determine when the breach of data has been either contained or mitigated to an acceptable level through the activation of the computer forensic examination. ▪ Determine if external notification process shall be activated (affected individuals, affected businesses, local law enforcement, FBI and/or contracted cyber response vendors). ▪ Ensure a computer forensic examination of all loss of data will be conducted to determine all possible external electronic storage locations. ▪ Determine risk of harm caused by the breach and then the level of risk must be assessed to escalate to Levels 5 or 6. ▪ **Determine if notice to individuals whose data may have been exposed by the incident is addressed. Swiftness in notifying those affected by a breach of personally identifiable information (Pll), as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.**

Escalation Level 4 - Moderate	
Incident Lead ***Note:*** *The chronological log will be used to support possible follow up on legal action as determined by Roane State General Counsel, and President.*	▪ **Notify the Executive Management Team of the manifestation of the threat.** ▪ **Notify the Incident Response Team of the incident.** ▪ **Receive status from the Technical Assessment Team and report to the Executive Management Team.** Start a chronological log of events.
Incident Response Team -Technical Assessment and Support	▪ **Determine best course of action for containment of the incident.** ▪ **Report actions taken and status to the Incident Lead.** ▪ **Report actions taken and status to the Incident Response Coordinator.** ▪ Prepares the Incident Report Form if not already completed. ▪ Report actions taken, number of personnel involved etc. to Incident Coordinator for the chronological log.
Communication Team/PIO ***Note:*** *The Communication and Executive Management Teams should consider notifying the public media as soon as possible after the discovery of a breach. However, if possible, the incident response plan and notification content should be developed prior to notifying the media.*	▪ Message the employee population informing them of the incident if deemed appropriate by the Executive Management Team. ▪ Message the employee population of any action they need to take as determined by the Technical Assessment and Support Team and directed by the Executive Management Team. ▪ Determine, with Legal, Audit and Compliance, the specific legal obligations and timeline for notification. ▪ Assist the Executive Management Team with determining if or when the data breach should be released to affected individuals and/or the media. ▪ Notification content should focus on providing information, including links to resources, to aid the public in its response to the breach.

Escalation Level 4 - Moderate	
Communication Team/PIO *(continued)*	▪ Notification may be delayed upon the request of law enforcement. ▪ To the extent possible, prompt public media disclosure is generally preferable because delayed notification may erode public trust.
Incident Response Support (IRS) – Risk Management Claims Administration - Treasury	▪ Obtain copy of initial investigation report from the Incident Lead or the Executive Management Team. ▪ Notify State of Tennessee's insurance broker and insurance carrier. ▪ Submit the initial investigation report to insurance carrier and broker. ▪ Determine if a recommendation to activate cyber response vendors is needed to the Incident Lead or the Executive Management Team. ▪ Respond to any request for assistance from the Incident Lead or the Executive Management Team.

Escalation Level 5 - High	
Executive Management Team	▪ Direct the Incident Response Support Team to: ○ Set up communications between all Executive Team Managers and the Technical Support Team. ○ Establish and assume occupancy of the command center. ○ Initialize an incident voice mail box where status messages can be placed to keep Roane State personnel updated. ▪ President determines if Tennessee Bureau of Investigation (TBI) notification process should be activated. In some circumstances, the President, Executive Team Managers, and TBI may consider delaying external notification to affected individuals and media if a notification would seriously impede the investigation of the breach or the affected parties. However, any delay should not worsen risk or harm to any affected individual. ▪ Alert the Extended Team of the incident notifying them of the Severity Level. ▪ Determine when external notification process shall be activated (affected individuals, affected businesses, local law enforcement, FBI, and/or contracted cyber response vendors). ▪ Determine when a computer forensic examination of all loss of data will be conducted to determine all possible external electronic storage locations. ▪ Determine when the risk has been mitigated to an acceptable level. ▪ Provide status updates from the President to the leadership hierarchy within Roane State. ▪ Ensure that all needed information is being collected to support legal action or financial restitution.

Escalation Level 5 - High	
Executive Management Team *(continued)*	▪ Determine if the information that has been lost or stolen is properly protected by encryption and has been validated by the Technical Assessment Team. If it is determined that the data is encrypted, the risk of compromise may be low to nonexistent. ▪ Determine if and when the cyber vendor's call center and monitoring services will be used for the data breach/cyber incident. ▪ **Determine if notice to individuals whose data may have been exposed by the incident is addressed. Swiftness in notifying those affected by a breach of personally identifiable information (PlI), as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint.**
Incident Lead	▪ Continue maintaining the chronological log of event. ▪ Post numbered status messages in the incident voice mail box for updating executive management. ▪ Continue to have oversight over the tasks and progress of the Technical Assessment and Support Team. ▪ Report progress of the Technical Assessment and Support Team to the Executive Management Team.
Incident Response Team – Technical Assessment and Support	▪ Prepares the Incident Report Form if not already completed. ▪ Continue to monitor all known sources for alerts, looking for further information or actions needed to eliminate the threat. ▪ Continue reporting status, actions taken, number of personnel, etc. to the Incident Lead for the chronological log of events. ▪ Monitor effectiveness of actions taken and modify them as necessary. ▪ Provide status updates to the Incident Lead on effectiveness of actions taken and progress in eliminating the threat.

Escalation Level 5 - High	
Legal, Audit and Compliance	▪ Determine, with Communications, the specific legal obligations and timeline for notification. Consult Tennessee Code Annotated, Section 47-18-2107 for specific requirements, and with the Consumer Protection Division of the Attorney General's Office. ▪ Notify the Executive Management Team to determine if or when the data breach notification letter should be released to affected individuals and/or the media. ▪ If the breach involves a state contractor or a public-private vendor operating a system of records on behalf of Roane State Community College, the Legal, Audit, and Compliance Team is responsible for ensuring or determining if any notification and corrective actions needs to be taken by Roane State. ▪ Review contract and outline the roles, responsibilities, and relationships with contractors or vendors, and prepare a summary reflecting cyber insurance requirements within contract. ▪ Work directly with the state-contracted Cyber Coach Attorney and/or obtain an engagement letter with outside counsel or firm that specializes in cyber breaches/ incidents. Consult with Attorney General's Office if an engagement letter is required.
Communication Team/PIO *Note: The Communication and Executive Management Teams should consider notifying the public media as soon as possible after the discovery of a breach. However, if possible, the incident response plan and notification content should be developed prior to notifying the media.*	▪ Message the employee population informing them of the incident if deemed appropriate by the Executive Management Team. ▪ Message the employee population of any action they need to take as determined by the Technical Assessment Team and directed by the Executive Management Team. ▪ Determine, with Legal, Audit and Compliance, the specific legal obligations and timeline for notification.

Escalation Level 5 - High	
Communication Team/PIO *(continued)*	▪ Assist the Executive Management Team with determining if occurrence of the data breach should be released to affected individuals and/or the media and, if so, when to release information. ▪ Notification content should focus on providing information, including links to resources, to aid the public in its response to the breach. ▪ Notification may be delayed upon the request of law enforcement. ▪ To the extent possible, prompt public media disclosure is generally preferable because delayed notification may erode public trust.
Incident Response Support (Risk Management Claims Administration – Treasury)	▪ Obtain a copy of initial investigation report from the Incident Lead or the Executive Management Team. ▪ Notify State of Tennessee's insurance broker and insurance carrier. ▪ Submit the initial investigation report to insurance carrier and broker. ▪ Determine if a recommendation to activate cyber response vendors is needed to the Incident Lead or the Executive Management Team. ▪ Respond to any request for assistance from the Incident Lead or the Executive Management Team.
Human Resources	▪ HR, Legal, Audit and Compliance, and President determine if disciplinary action or termination is warranted if the breach of data/cyber incident was from an internal source.

Escalation Level 6 – Very High

Executive Management Team	▪ Direct the Incident Response Support Team to: ○ Set up communications between all Executive Team Managers and the Technical Support Team. ○ Establish and assume occupancy of the command center. ○ Initialize an incident voice mail box where status messages can be placed to keep Roane State personnel updated. ▪ President determines if Tennessee Bureau of Investigation (TBI) notification process should be activated. In some circumstances, the President, Executive Team Managers, and TBI may consider delaying external notification to affected individuals and media if a notification would seriously impede the investigation of the breach or the affected parties. However, any delay should not worsen risk or harm to any affected individual. ▪ Alert the Extended Team of the incident notifying them of the Severity Level. ▪ Determine when external notification process shall be activated (affected individuals, affected businesses, local law enforcement, FBI, and/or contracted cyber response vendors). ▪ Determine when a computer forensic examination of all loss of data will be conducted to determine all possible external electronic storage locations. ▪ Determine when the risk has been mitigated to an acceptable level. ▪ Provide status updates from the President to the leadership hierarchy within Roane State. ▪ Ensure that all needed information is being collected to support legal action or financial restitution.

Escalation Level 6 – Very High	
Executive Management	• Determine if the information that has been lost or stolen is properly protected by encryption and has been validated by

Team	the Technical Assessment Team. If it is determined that the data is encrypted, the risk of compromise may be low to nonexistent. • Determine if and when the cyber vendor's call center and monitoring services will be used for the data breach/cyber incident. • Determine if notice to individuals whose data may have been exposed by the incident is addressed. Swiftness in notifying those affected by a breach of personally identifiable information (Pll), as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.
Incident Lead	▪ Continue maintaining the chronological log of events. ▪ Post numbered status messages in the incident voice mail box for updating agency executive management. ▪ Continue to have oversight over the tasks and progress of the Technical Assessment Team and the Technical Support Team. ▪ Report progress of both the Technical Assessment Team and the Technical Support Team to the Executive Management Team.
Incident Response Team – Technical Assessment and Support	▪ Prepares the Incident Report Form if not already completed. ▪ Continue to monitor all known sources for alerts, looking for further information or actions needed to eliminate the threat. ▪ Continue reporting status to the Incident Lead for the chronological log of events. ▪ Monitor effectiveness of actions taken and modify them as necessary.

Escalation Level 6 – Very High	
Incident Response Team –	▪ Provide status updates to the Incident Lead on

Technical Assessment and Support (continued)	effectiveness of actions taken and progress in eliminating the threat. ▪ Continue actions to eradicate the threat as directed by the Executive Management Team, the Incident Lead, and the Incident Response Team. ▪ Continue to report actions taken, number of personnel, etc. to the Incident Lead for the chronological log.
Legal, Audit and Compliance	▪ Determine, with Communications, the specific legal obligations and timeline for notification. Consult Tennessee Code Annotated, Section 47-18-2107 for specific requirements, and with the Consumer Protection Division of the Attorney General's Office. ▪ Notify the Executive Management Team to determine if or when the data breach notification letter should be released to affected individuals and/or the media. ▪ If the breach involves a state contractor or a public-private vendor operating a system of records on behalf of Roane State Community College*,* the Legal, Audit, and Compliance Team is responsible for ensuring or determining if any notification and corrective actions needs to be taken by Roane State. ▪ Review contract and outline the roles, responsibilities, and relationships with contractors or vendors, and prepare a summary reflecting cyber insurance requirements within contract. ▪ Work directly with the state-contracted Cyber Coach Attorney and/or obtain an engagement letter with outside counsel or firm that specializes in cyber breaches/incidents. Consult with Attorney General's Office if an engagement letter is required.

Escalation Level 6 – Very High	
Communication Team/PIO *Note:*	▪ Message the employee population informing them of the incident if deemed appropriate by the Executive Management Team.

The Communication and Executive Management Teams should consider notifying the public media as soon as possible after the discovery of a breach. However, if possible, the incident response plan and notification content should be developed prior to notifying the media.	▪ Message the employee population of any action they need to take as determined by the Technical Assessment Team and directed by the Executive Management Team. ▪ Determine, with Legal, Audit and Compliance, the specific legal obligations and timeline for notification. ▪ Assist the Executive Management Team with determining if occurrence of the data breach should be released to affected individuals and/or the media and, if so, when to release information. ▪ Notification content should focus on providing information, including links to resources, to aid the public in its response to the breach. ▪ Notification may be delayed upon the request of law enforcement. ▪ To the extent possible, prompt public media disclosure is generally preferable because delayed notification may erode public trust.
Incident Response Support (Risk Management Claims Administration – Treasury)	▪ Submit updated status reports received from the Incident Lead or the Executive Management Team to insurance carrier. ▪ Determine if a recommendation to activate cyber response vendors is needed to the Incident Lead or the Executive Management Team. ▪ Respond to any request for assistance from the Incident Lead or the Executive Management Team. ▪ Assist the Executive Management Team with setting up cyber vendors call center and monitoring services.
Human Resources	▪ HR, Legal, Audit and Compliance, and President determine if disciplinary action or termination is warranted if breach of data/cyber incident was from an internal source.

Post Incident	
Incident Lead	Prepare a report for Roane State executive management to include: ▪ Estimate of damage/impact; ▪ Action taken during the incident (not technical detail); ▪ Follow-up on efforts needed to eliminate or mitigate the

	vulnerability; - Policies or procedures that require updating; - Efforts taken to minimize liabilities or negative exposure; and - Document lessons learned and modify the Incident Response Plan accordingly. - Update the cyber incident log with incident after action information.
Legal, Audit and Compliance	- Confirm transmission of any notifications determined necessary by law or policy. - Provide the chronological log and any system audit logs requested by law enforcement or prosecutors, if applicable. - Assist with preparing any or all documents, upon request, from law enforcement or prosecutors, if applicable.
Human Resources	- Determine if any additional training regarding Pll, HIPAA, or FERPA is needed for all or certain classes of employees. - Continue with scheduling annual training for Pll, HIPAA, or FERPA for all employees.

Notification Contents

Please note that Legal, Compliance, and Audit divisions should consult Tennessee Code Annotated, Section 47-18-2107 regarding notification requirements.

The notification letter should be provided in writing and should use concise and plain language. The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery.
- A description of the types of personal information involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.).
- A statement regarding whether the information was encrypted or protected by other means when determined such information would be beneficial and would not compromise the security of the system.
- The steps affected parties should take to protect themselves from potential harm, if any.
- The steps being taken to investigate the breach, to mitigate losses and to protect against any further breaches. The inclusion of any details concerning the investigation of the breach should take into consideration whether or not the inclusion of such details would jeopardize an ongoing law enforcement investigation.
- The contact for more information about the incident, including a toll-free call center telephone number, e-mail address, and postal address.
- The notification information should be layered with the most important information up front, and the additional details in a Frequently Asked Questions (FAQ) format, or on the Roane State website. If the Roane State has knowledge that the affected parties are not English speaking, notice should also be provided in the appropriate language(s).

See Appendix D: Sample Notification
(provided by State of Tennessee Treasury Department) for sample of written notifications provided by the State of Tennessee Treasury Department, Division of Risk Management Claims Administration and Appendix F: Sample Call Center FAQ
(provided by the State of Tennessee Treasury Department) for sample answers to Frequently Asked Questions that can be distributed to the Information Center or other call center established after an incident.

Appendices

Appendix A: Incident Response Teams Contact List

Executive Management Team (EMT)

Name	Title	Email	Phone Numbers
Dr. Chris Whaley	President	whaleycl@roanestate.edu	865-882-4501
Tim Carroll	Assistant Vice President & CIO, Information Technology	carrolltd@roanestate.edu	865-882-4618
Danny Gibbs	Executive Vice President, Business and Finance	gibbsdc@roanestate.edu	865-882-4220
Dr. Diane Ward	Vice President, Student Services	wardd@roanestate.edu	865-882-4513
Teresa Duncan	Vice President, Workforce Development & Student Affairs	DuncanTS@roanestate.edu	865-882-4648
Karen Bruner	VP of Institutional Effectiveness and Research, Institutional Effectiveness / Research	BrunnerKL@roanestate.edu	865-882-4606

Incident Lead (IL)

Name	Title	Email	Phone Numbers
Tim Carroll	Assistant Vice President & CIO, Information Technology	carrolltd@roanestate.edu	865-882-4560 865-466-2049 (cell)

Incident Response Team (IRT, Assessment and Technical Support)

Name	Title	Email	Phone Numbers
Peter Souza	Director, Networking, Telecommunications & Technical Support	souzapa@roanestate.edu	865-882-4681
Chris Pankratz	Director, Administrative Systems	PankratzCS@roanestate.edu	865-354-3000 x4262
Allen Foster	Assistant Network and Telecommunications Manager	fostera@roanestate.edu	865-354-3000 x4740
Lyle Fountain	Systems Administrator (NTTS)	FountainLW@roanestate.edu	865-354-3000 x4588
Keri Phillips	Database Administrator	phillipska@roanestate.edu	865-882-4548
Dave Ribes	Help Desk Manager/Sr. Computer Technician	ribesdj@roanestate.edu	865-354-3000 x4617
Elizabeth Hill	Help Desk Specialist	hillae@roanestate.edu	865-354-3000 x4357

Incident Response Support

Name	Title	Email	Phone Numbers
Rodney Escobar	Director of Risk Management and Claims Administration	Rodney.Escobar@tn.gov	615-741-9957

Communications

Name	Title	Email	Phone Numbers
Owen Driskill	Executive Director Oak Ridge Branch Campus and Community Relations	driskillo@roanestate.edu	(865) 354-3000 x2301

Legal, Audit and Compliance

Name	Title	Email	Phone Numbers
Cynthia Cortesio	Director, Internal Audit	cortesiocl@roanestate.edu	865-882-4529
Louis P. Svendsen	University Council	lou.svendsen@tbr.edu	615-366-3909
Jon Calisi	TBR Technical Contact	Jon.calisi@tbr.edu	(615) 366-4456

Human Resources

Name	Title	Email	Phone Number
Odell Fearn	Director, Human Resources	fearnao@roanestate.edu	865-354-3000 x4212

Law Enforcement Notification List

Name	Title	Email	Phone Numbers
Tom Stufano	Chief of Police	stufanotj@roanestate.edu	865 882 4512
Knoxville Consolidated Facility	Tennessee Bureau of Investigation		865-549-7800
Edward W. Reinhold	Knoxville FBI Office	knoxville@ic.fbi.gov	865-544-0751

Appendix B: Roles and Responsibilities

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

Tim Carroll, Assistant Vice President and Chief Information Officer
Information Technology
carrolltd@roanestate.edu
865-882-4560

Communications Officer/Public Information Officer (PIO) – The Communications Officer will coordinate communication for both internal and external audiences and determine proper delivery mechanism(s). The content will be created with consultation from the Incident Response Team, Executive Management Team and other subject matter experts. The Communications Office is typically the director of Marketing and Communications.

Executive Management Team (EMT) – The executive management team is comprised of the senior leadership for Roane State Community College. Directory information listed in Appendix

Help Desk – The RSCC Help Desk is the first level of interaction for users experiencing IT issues which can also include security events. It is the Help Desk'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 appropriate technician, server administrator and/or the director of Networking, Telecommunications and Technical Support. The Help Desk shall instruct the user not to reboot, disconnect, or otherwise alter the system when a confirmed incident has been discovered.

Human Resources (HR) – The director of Human Resources will work with Legal, Audit and Compliance if required if incidents at Level 5 and higher require personnel action or training.

Incident Lead – The incident lead is an individual appointed the college president to direct and manage the internal response team, as well as to act as the go-between for the Executive Management Team. In the event of an event escalated to Level 3 or higher, the Incident Lead will coordinate with the Incident Response Team Primary Contact and the Incident Response Team (IRT) to review the incident and respond according to the specific SOP. The Incident Lead will coordinate the response with system administrators, the Help Desk, Networking, Telecommunications and Technical Support, Administrative Systems, 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). If the event is escalated to a Level 4 or higher, the Incident Lead will notify the Executive Management Team. The Incident Lead is typically the CIO.

Incident Response Team Primary Contact – The Incident Response Team Primary Contact is responsible for the gathering of all necessary information pertaining to a security incident and for the tracking and reporting of specific incidents. The primary contact is the communication liaison between the affected groups and the Incident Lead. The Incident Response Team Primary Contact is typically the Director of Networking, Telecommunications and Technical Support.

Incident Response Team (IRT) – This team is comprised of operational and technical employees who undertake the actions required to mitigate the threat and investigate computer security events and incidents. These can be system administrators, database administrators, network engineers, or application administrators/programmers.

Incident Response Support (IRS) – This group is comprised of State subject matter experts who provide guidance, advice and support for cyber incidents categorized at level 4 or higher.

Incident Response Team Primary Contact (IRC) – The Primary Contact is responsible for gathering all of the necessary information pertaining to a security incident and for the tracking and reporting a security incident and for the tracking and reporting of specific incidents. The Primary Contact is usually the Chief Information Officer or senior Information Technology executive for the college.

Legal, Audit and Compliance – The legal, audit and compliance team is comprised of the Roane State director of Internal Audit and the Executive Director of Equity and Compliance. They will coordinate and communicate with TBR and Treasury personnel as needed.

Networking, Telecommunications and Technical Support (NTTS) – The team will work in conjunction with the Incident Lead 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, running malware and other detection software, re-imaging machines, restoring backups and other activities. The NTTS Operations Manager and Network Manager are responsible for monitoring the systems within their areas to identify unusual behavior or symptoms, which may indicate a security incident.

Technicians – The technicians are usually the first level of interaction for users experiencing issues which may include cyber security events. It is the technician's responsibility to evaluate information from users to, first, determine if an incident has occurred or is in progress. If true, they should advise users on the handling of the incident to mitigate loss or exposure of PII or data. Technicians should immediately report all cyber security incidents to their immediate supervisor and the Chief Information Officer or Senior Information Technology executive at the college. Depending on the type of incident, they should instruct the user or users to not reboot or delete data until a forensic examination can be performed. Individual computers may need to be disconnected from the network to prevent further damage to the network.

Users – Refers to all students, faculty, staff and others while accessing, using, or handling Roane State Community College information technology resources. "Others" include, but are not limited to, subcontractors, visitors, visiting scholars, potential students, grant and contract support personnel, media representatives, guest speakers, and non-College entities granted access. Users are responsible for monitoring unusual system behavior, which may indicate a security event. Users must be able to recognize the indications of a security event as outlined in the incident verification section of this document. Users are responsible for reporting events to their computer technician, the Help Desk or Networking, Telecommunications and Technical Support immediately. The user must not reboot, disconnect, or otherwise alter the system when an event has been discovered, unless directed otherwise by a member of the Incident Response Team. Otherwise, collection of valid evidence can be negatively impacted by losing critical information stored in system memory.

Appendix C: Glossary of Terms

Advanced Persistent Threat (APT) – An advanced persistent threat is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to your network or organization. An APT uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term.

Breach – The term "breach" is used to include the loss control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where any person that is not authorized and does not have an authorized purpose to have access or potential access to information, whether physical or electronic. It includes both intrusions (from outside the organization) and misuse (from within the organization). Malware infections will be considered a breach ONLY if it is widespread and infects computers where repairs or replacement costs exceed $25,000, or where data is known to have been compromised.

Business Identifiable Information (BII) – Business identifiable information is information about a company or other business entity that could be used to commit or facilitate the commission of fraud, deceptive practices or other crimes. Examples include, but are not limited to, bank account information, trade secrets, and confidential or proprietary business information.

Command Center –For the purposes of this document, the command center is the central point of contact which any member of the respective government sector (STS/ TBR) can contact to report a cyber-security incident.

Chain of Custody – A method of documenting the possessions of an item from the time of collection to its final disposition. It includes details as to who, when, where and what was done with or to the item.

Cyber Security Event – A Cyber Security event is an observable change that adversely impacts the established security behavior of an environment or system.

Cyber Security Incident – An accidental or malicious violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices that can cause actual or potential threats to the confidentiality, integrity, and availability of State data and information technology assets. Incidents can include computer intrusions, denial-of-service attacks, insider theft of information, copyright violations, and any activity that requires support personnel, system administrators, or computer crime investigators to respond.

Data Exfiltration – Data exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various different techniques, typically by cybercriminals, over the internet or other network.

Denial of Service (DoS) – A DoS is a type of attack that attempts to prevent a system from performing its normal functions or, more frequently attempts to prevent authorized users from accessing a system.

Distributed Denial of Service (DDoS) – A DDoS is a type of DoS attack in which multiple compromised systems are used to target a single system or network.

Event – An observable occurrence in a system and/or network. It may be an early indication that a cyber-incident is occurring.

Free Application for Federal Student Aid (FASFA) – The application for federal student aid completed by the student and then provided to the college(s) selected by the student in the form of an Institutional Student Information Record (ISIR).

Harm – For the purposes of this document, harm means any adverse effects that would be experienced by an individual or organization (e.g., that may be socially, public trust, physically or financially damaging) whose information was breached, as well as any adverse effects experienced by the organization that maintains the information.

Identity Theft - Identity theft is the act of obtaining or using an individual's identifying information without authorization in an attempt to commit or facilitate the commission of fraud or other crimes. The resulting crimes usually occur in one of the following ways. Identity thieves may attempt to:

- Gain unauthorized access to existing bank, investment or credit accounts using information associated with the person.
- Withdraw or borrow money from existing accounts or charge purchases to the accounts.
- Open new accounts with a person's identifiable information without that person's knowledge.
- Obtain driver's licenses, social security cards, passports or other identification documents using the stolen identity.

Imminent threat – a situation in which the agency has a factual basis for believing that a specific incident is about to occur. For example, the agency receives a bulletin from Microsoft warning of operating system vulnerabilities that must be patched immediately.

Inappropriate usage – entails the use of resources in ways other than their intended purpose or which have not been approved. Examples include, but are not limited to, any illegal use of State computer systems; using State computer systems to conduct personal business, and sending communications that violate established conduct policies. Applicable RSCC policies include:

- GA-18-01 Ethical and Responsible Use of Computer Resources
- GA-18-03 Electronic Information Systems (Email)
- GA-18-05 Use of Email as Official Correspondence

- GA-18-07 Mobile Device Policy (iPads and other Mobile Devices)
- GA-18-08 Data and Personally Identifiable Information (PII) Security
- GA-18-09 Strong Password
- GA-18-10 Information Technology Security Program
- Procedures, Guidelines and Other documents supporting policies located in Information Technology SharePoint Policies and Procedures site.

Incident – Also known as a security incident. See definition below.

Incident Response – A structured, documented process used to respond to a security incident such as cyber-attacks and system compromises. The response includes multiple phases which are discovery/detection, triage/analysis, eradication, recovery and reporting.

Indicator – A sign that an incident may have occurred or may be occurring. Examples include anti-virus/malware alerts, unusual network traffic, unusual filenames in the system directory and failed login attempts in system logs.

Malware – short for malicious software, malware is software that enters a computer system without the user's knowledge or consent and then performs an unwanted, and usually harmful, action. Examples include, but are not limited to, worms, viruses, key- loggers, rootkits and Trojans.

Out-of-Bounds Communication – Use of not-technical methods to communicate information. Examples include in person conversations, phone calls and paper reports.

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

PII-Personally Identifiable 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:

1) Social security number;
2) Driver license number; or
3) 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.

Precursor – A sign that an incident may occur in the future. This could include item such as web server log entries, announcements of a new exploit or threat from a person or group.

Security Incident – An adverse event in an information system, and/or network, or the threat of an occurrence. Such events can include, but are not limited to, unauthorized access, denial of service attacks, malicious code, network probes, social engineering and insider theft of information.

Social Engineering – The process of obtaining information from people, frequently through deceptive practices, to find and gather information about personnel or technology. This can occur in person, phone calls, faxes, email or standard mail.

Users – All students, faculty, staff and others who use, access or handle any of the college's information technology resources. Others include, but is not limited to, vendors, contractors, and visitors.

Unauthorized access – This occurs when individuals or systems are able to access data, resources or environments without explicit approval from the owner.

Unauthorized Release of Data that is Protected by State or Federal Statute or Regulation – An unauthorized release of data is a communication or physical transfer of confidential information to an unauthorized recipient. Examples include, but are not limited to, a user inadvertently sends a confidential file to an email list, a poorly written application allows users to gain access to sensitive information, and an unencrypted computer or data storage device with confidential information on it is lost or stolen.

Threat – Any potential source that may exploit a vulnerability or misuse access privileges to cause a security incident.

Vulnerability – A weakness in a technology resource such as a system, application or network device that could be exploited to gain access to college information or systems.

Zero Day Threat – A Zero-Day Threat is a computer threat that exposes undisclosed or unpatched computer vulnerabilities. Zero-day attacks can be considered extremely dangerous because they take advantage of previously unknown vulnerabilities for which no solution is currently available.

Appendix D: Sample Notification
(provided by State of Tennessee Treasury Department)

SAMPLE WRITTEN NOTIFICATION

DATA ACQUIRED: Social Security Number (SSN)
(Note: Do not insert actual SSN)

Dear:

We are writing to you because of a recent security incident at Roane State Community College. [Describe what happened in general terms, what kind of Pll was involved, and what you are doing in response.]

Roane State Community College takes the security of personal information very seriously, and we continue to work closely with the appropriate authorities to continue to monitor this situation. In addition, the Roane State Community College has taken immediate steps to strengthen its internal controls, and established safeguards to prevent a similar breach.

Roane State is notifying you, with this letter, so that you can take actions, along with efforts, to minimize potential harm. Roane State Community College has also advised the three (3) major credit reporting agencies, in the United States, about this incident and have given those agencies a report, alerting them of this incident.

Even though the Roane State is not aware that any of the personal information has been used for identity theft or other criminal activity, Roane State has taken the added precaution of hiring the identify theft prevention firm [Name of Vendor] to provide you with one (1) year of identity protection services, and the optional credit monitoring services, all free of charge.

However, Roane State also encourages you to protect yourself from the possibility of identity theft. We recommend that you complete a Federal Trade Commission ID Threat Affidavit. This added step will assist you with legally notifying your creditors that your identity may have been compromised. Any debts or newly opened lines of credit incurred, after that date, will not be assigned to you.

We also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the numbers below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them, with instructions on how to get a free copy of your credit report from each.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289

Roane State Community College believes you should closely monitor your credit report and place a fraud alert on your credit file. If you do find suspicious activity on your credit report or have reason to believe your information is being misused, please call your local law enforcement agency for assistance. You may also file a complaint with the Federal Trade Commission by visiting www.ftc.gov/bcp/edu/microsites/idtheft or calling 1-877-ID-THEFT (438-4338).

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the Identity Theft website of the Federal Trade Commission.

In closing, Roane State Community College also encourage you to access the following resources and review the enclosed brochure about identity theft from [Name of Vendor]:

- Federal Trade Commission's website provides information about the three (3) major credit reporting agencies and identity theft consumer alerts: www.ftc.gov/bcp/conline/pubs/alerts/infocompalrt.htm
- Identity Theft Resource Center: www.idtheftcenter.org
- Privacy Rights Clearinghouse: www.privacyrights.org

One of the top priorities of the Roane State Community College is protecting the personal information that flows through our various programs that we are responsible for administering.

Sincerely,

[Name and Title]

Appendix E: General Guidelines for the Establishment of a Call Center

In the event of a significant data breach involving Pll, the following guidance is provided to help with the determination of whether to establish a call center. The purpose of a call center is to provide individuals a number to call to obtain further information regarding the data loss and possible action they may want to take to lessen the incident's impact on their personal lives.

The decision to establish a call center should be based on several considerations:

- If the breach affects a large number of individuals and those individuals are not easily identifiable or easily contacted, establishment of a call center should be considered to allow those potentially impacted to call and obtain additional information regarding the breach.
- Each situation will be unique and the decision to establish a call center must be based on individual circumstances. The main concern should be sharing of information with those affected and how they may obtain assistance.

Once a decision is made to establish a call center, there are several options:

- Contract with external cyber vendor to obtain call center and monitoring services.
- Establish an internal, fully-supported and staffed call center. A thorough description of the data level incident and set of frequently asked questions (FAQs) will also be required for call center to refer to when fielding calls.

Suggested items to consider based on the nature of the breach would include, but are not limited to, the following:

- Using existing TBR or affiliated institution personnel to staff the call center and monitoring services, if external vendor services are not used.
- Ensuring training of call center operators.
- Pre-stage FAQs using the samples provided in Appendix F.
- Ability to adjust staffing in response to call volume.
- Daily hours of operations.
- Cost of service.
- Call logging.
- Establish reporting requirements such as dropped calls or wait time, number of callers, etc.
- Advertising call center numbers and making data breach information readily available to those affected (e.g., employees, external customers, students, citizens, vendors).
- Quality assurance checks of call center effectiveness.

Appendix F: Sample Call Center FAQ
(provided by the State of Tennessee Treasury Department)

Example Question	Example Answer
How can I tell if my information has been compromised?	At this point, there is no evidence that any missing data has been used illegally. However, Roane State is asking each individual to be extra vigilant and to carefully monitor bank statements, credit card statements, and any statements relating to recent financial transactions. If you notice unusual or suspicious activity, you should report it immediately to the financial institution involved.
What is the earliest date at which suspicious activity might have occurred due to this data breach?	The information was stolen from an employee of Roane State Community College during the month of [MONTH]. It is likely that individuals may notice suspicious activity during the month of [MONTH].
I have not noticed any suspicious activity in my financial statements, but what can I do to protect myself from being victimized by credit card fraud or identity theft?	Roane State Community College strongly recommends that individuals closely monitor their financial statements, and contact Human Resources for updates regarding this incident. Additional information may be found at www.roanestate.edu/[TBD[2]]
Should I reach out to my financial institutions or will Roane State Community College do this for me?	Roane State Community College does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts unless you detect suspicious activity. If so, you will need to report it.
Where should I report suspicious or unusual activity?	The Federal Trade Commission (FTC) Identity Theft website (http://www.consumer.ftc.gov/features/feature-0014-identity- theft) recommends the following steps if you detect suspicious activity: • Place an Initial Fraud Alert. • Contact the fraud department of one of the

[2] This site will be set up at the time such an incident should occur.

Where should I report suspicious or unusual activity? ***(continued)***	three major credit bureaus: ○ Equifax: 1-800-525-6285; www.equifax.com: P.O. Box 740241, Atlanta, GA 30374-0241 ○ Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013 ○ Transunion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790 • Order your credit report from the three major credit bureaus above. • Create an Identity Theft Report. • Submit a report about the theft to the FTC online or call the FTC at 1-877-438-4338 (1-866-653-4261 - TTY). When you finish writing all the details, print a copy of the report. It will be called an Identity Theft Affidavit. Bring your FTC Identity Theft Affidavit when you file a police report. • File a police report with your local police department or the police department where the theft occurred, and get a copy of the police report or the report number. Your FTC Identity Theft Affidavit and your police report make an Identity Theft Report. • Consider whether you need an Extended Fraud Alert. If you have created an Identity Theft Report, you can get an extended fraud alert on your credit file. When you place an extended alert, you can get two free credit reports within 12 months from each of the three nationwide credit reporting companies, and the credit reporting companies must take your name off marketing lists for prescreened credit offers for five years, unless you ask them to put your name back on the list. The extended alert lasts for seven years. • Consider whether you need a Credit Freeze. You may choose to put a credit freeze on your file, but a credit freeze may not stop misuse of your existing accounts or some other types of identity theft. Also, companies that you do business with would still have access to your credit report for some purposes. A fraud alert will allow some

Where should I report suspicious or unusual activity? ***(continued)***	creditors to get your report as long as they verify your identity. This measure is only recommended if you have confirmed your identity has been stolen. • Close any accounts that have been tampered with or opened fraudulently.
Where can I get further, up-to- date information?	Roane State Community College has set up a special website which features up-to-date news and information. Please visit www.roanestate.edu/[TBD[3]]
Does the data breach affect only certain individual?	It potentially affects a large population of individuals. We urge everyone possibly affected to be extra vigilant and monitor their financial accounts.
What is Roane State Community College doing to ensure that this does not happen again?	Roane State Community College is working with the law enforcement to investigate the data breach and to develop safeguard against similar incidents. Roane State Community College has directed all employees to complete our Security Awareness Training courses. Appropriate law enforcement agencies, Roane State Community College have launched full-scale investigations into this matter.
What additional information will I receive regarding this incident?	You will receive a Notification Letter from Roane State Community College mailed to you by our vendor, *[Nome of Cyber Vendor]* ID on , (DATE). This letter will include a toll-free telephone number to the *[Name of Cyber Vendor]* call center for any questions and information regarding consumer identity protection, credit monitoring, and identity theft insurance services being provided free through *[Nome of Vendor],* You will be automatically enrolled in the consumer identity protection services. In addition, free optional credit monitoring services with three national credit bureaus and identity theft insurance is also available to those who

[3] This site will be set up at the time such an incident should occur.

	register for these services. Roane State Community College encourages you to take advantage of these free services
Has the problem been contained?	Roane State Community College believes this is an isolated incident and it does not appear that the file has been disseminated to other people or sources.

Appendix G: Collection and Preservation of Evidence

When a security incident involves legal action against a person or organization, or a personnel action against an Institutional employee, evidence must be collected, preserved, and presented to conform to the rules for evidence specified in the relevant jurisdiction(s). The following procedures help ensure the chain of evidence needed for legal proceedings:

1. When collecting evidence, follow all appropriate Institutional policies and procedures
2. Document all actions taken in the collection and preservation of the evidence
    a. For data stored on electronic media make a mirror image or copy of the media
    b. Have an independent person witness the imaging/copying process.
    c. Law enforcement should be involved if the incident involves a high profile or sensitive criminal case
    d. Document all actions taken during the imaging/copying process to include:
        i. Date
        ii. Time
        iii. Location the image/copy was made
        iv. Who performed the actions
        v. Who witnessed the actions
        vi. The tools and programs used.
    e. Label the original media and store it along with the log of the imaging/copying process in a secure location.
3. Perform all forensics work:
    a. Only on the image or copy
    b. Do not modify or place the original at risk
    c. Additional images or copies of the original should be created for use if needed
4. For paper-based documents, keep the original in a secure location and log the following:
    a. Who found the document
    b. Where it was found
    c. Date and time it was found
    d. Who witnessed the discovery

Depending on the nature of the incident, appropriate evidence handling techniques will be utilized such as those defined in NIST Special Publication on Computer Security Incident Handling Guide #800-61 and NIST SP 800-86, Guide to Incident Response. The primary reason for gathering evidence during an incident is to resolve an incident, but it may also be needed for legal proceedings. The extent of the forensics will vary depending on the type of incident and the potential for law enforcement involvement. It may be necessary for the institution to hire a certified forensic specialist depending upon the nature and extent of the incident and the college should work with law enforcement and Risk Management to make this decision.

If a certified forensic investigator is not necessary, the following actions should be taken:

- All evidence should be accounted for at all times. A chain of custody form as found in Appendix I will be started for any systems being confiscated with signatures anytime the custody is changed.
- A detailed log should be kept for all evidence, including the following:
    - Identifying information (including location, serial number, model number, hostname, IP address) for the equipment.

  - Name, title and phone number of each individual who collected or handled the equipment.
  - Date and time for each occurrence of evidence.
  - Location where evidence was stored. Confiscated equipment will be stored in the closet of the Vice President for Technology when feasible.
  - Photographs of the screen showing any messages (error, threat or compromise) should be taken.
  - Disk images will be taken of the compromised system on read-only media.
  - The volatile data should be collected before shutting the system down. This includes:
    - Current running processes
    - Network connections (netstat)
    - Arp tables (arp -a)
    - List of open files
- All equipment in the area of compromise should be labelled. Care should be taken to include all removable media.
- Photographs of the area should be taken before the equipment is moved and should show the location of the labelled equipment and what is connected to the system.
- Confiscated equipment will be held in the closet of the Vice President for Technology when feasible. Another location will be determined if needed.
- If equipment can't be taken out of service or physically moved, the Vice President for Technology will consult law enforcement to decide the best course of action if needed.
- The following actions should be avoided:
  - Shutting down or rebooting the victim's computer.
  - Assuming that some components of the victim's computer may be reliable and usable.

Chain of Custody Form

Roane State Community College

Chain of Custody Form

Item Number(s): ______________________

To be completed by initial collector:
Evidence collected by (name): ____

Date/Time Collected: ________________________________

Evidence Description: ____

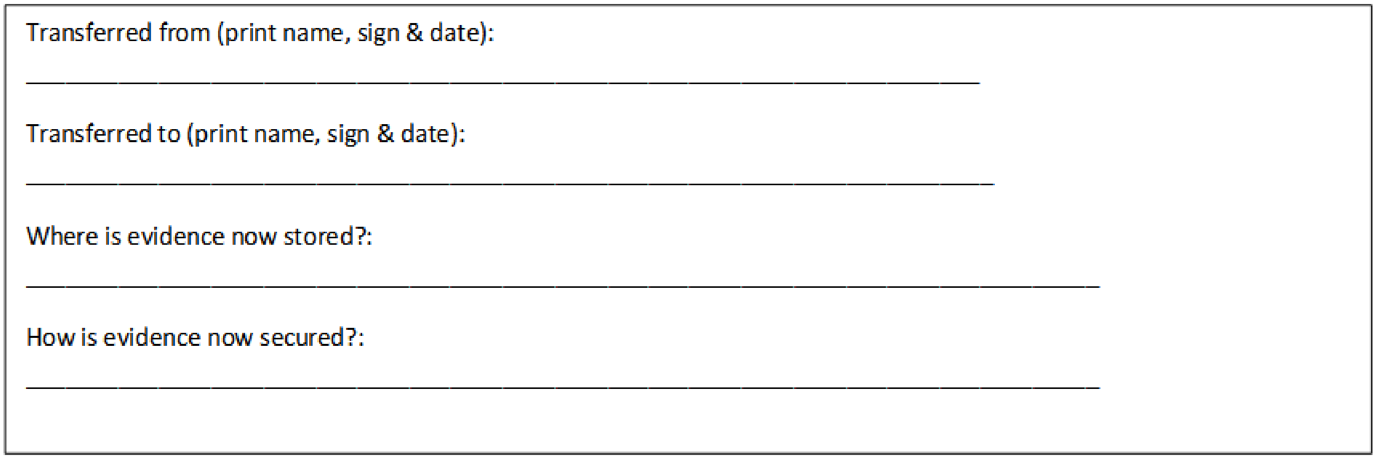
____

Where is evidence initially stored? ____

How is evidence initially secured? ____

Collector signature: ____ Date: _______________________

(Attach documentation to describe the collection method and preservation of application software/utility to view the evidence.)



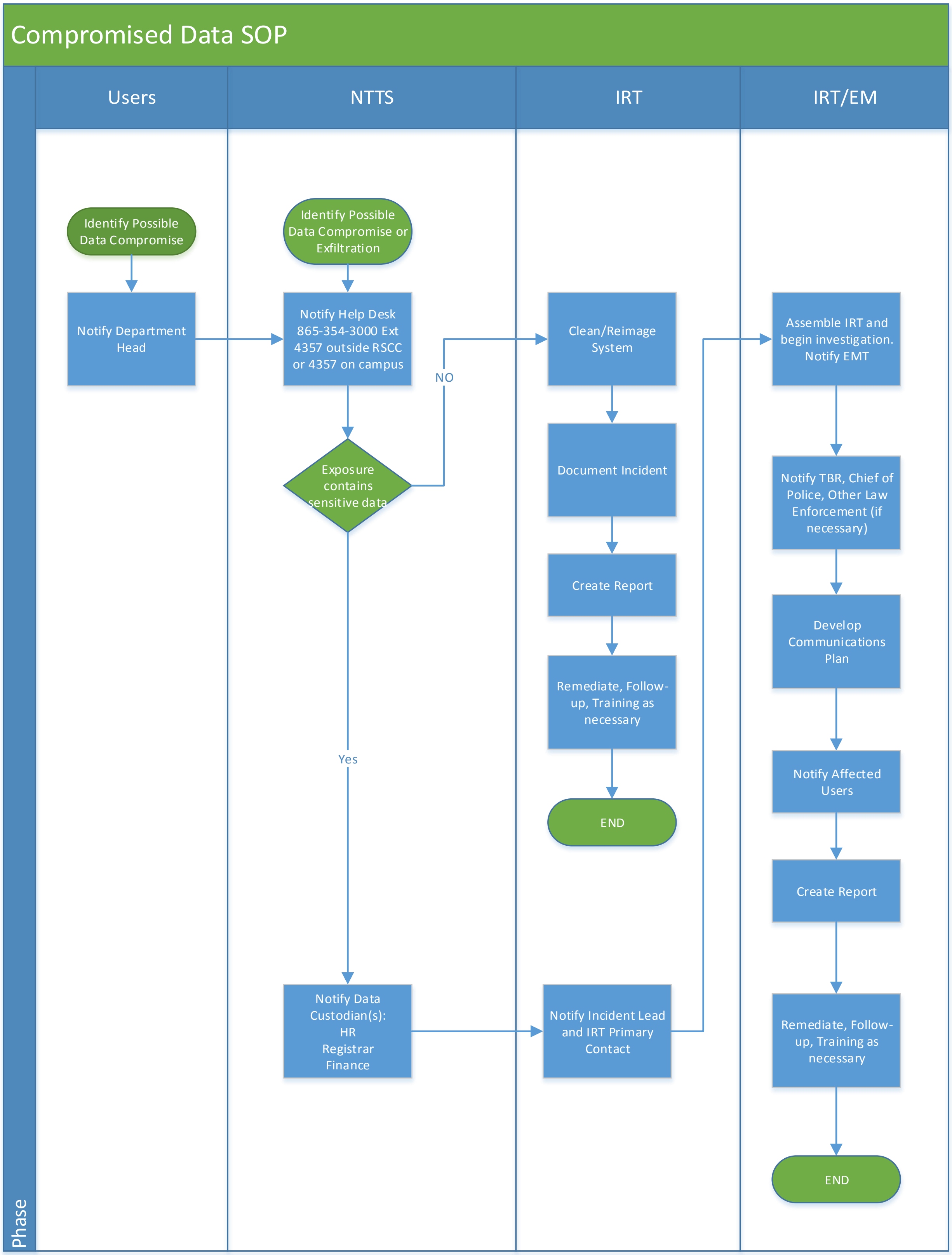
Transferred from (print name, sign & date):
____

Transferred to (print name, sign & date):
____

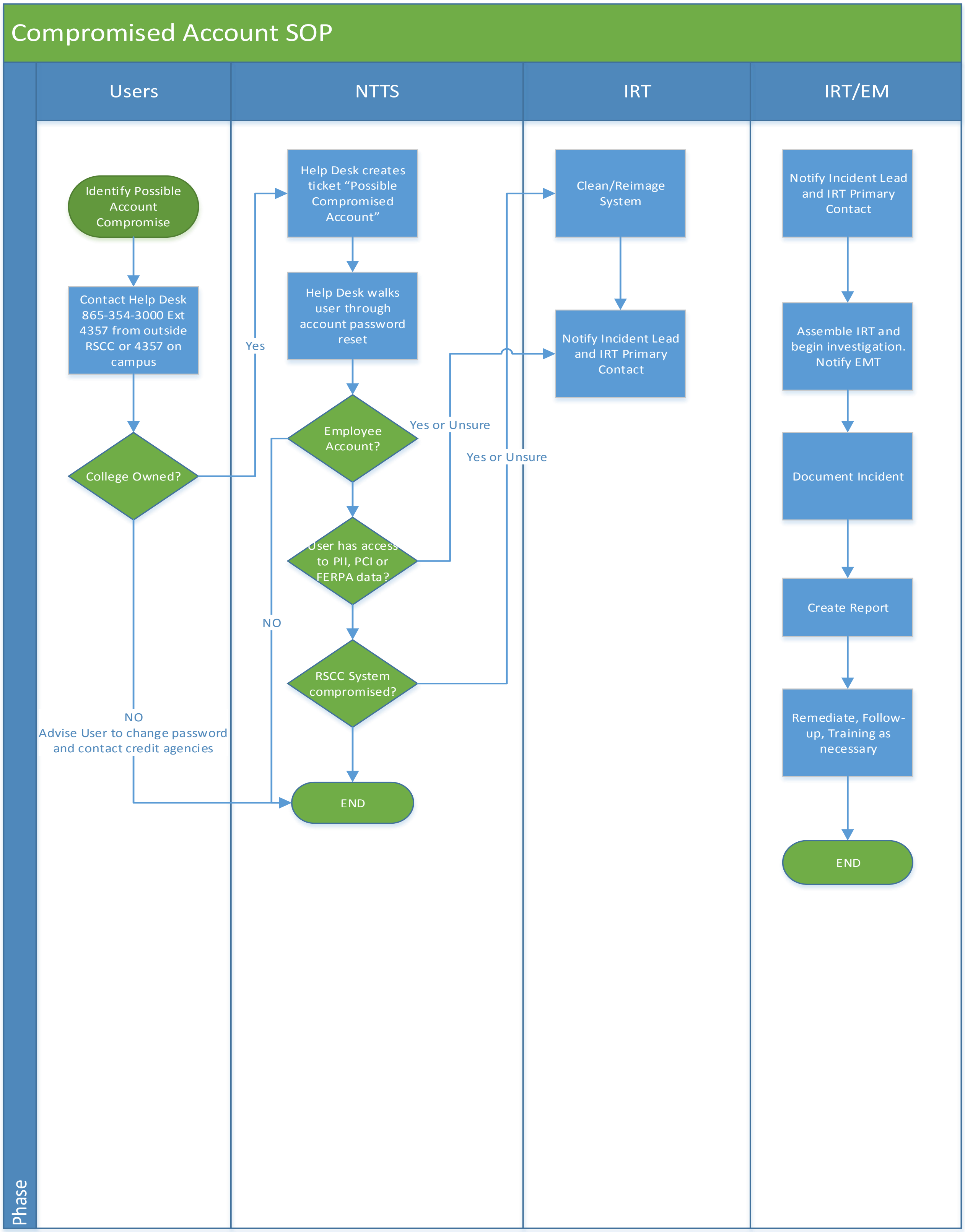
Where is evidence now stored?:
____

How is evidence now secured?:
____

Appendix H: Data Exposure Standard Operating Procedure (SOP)

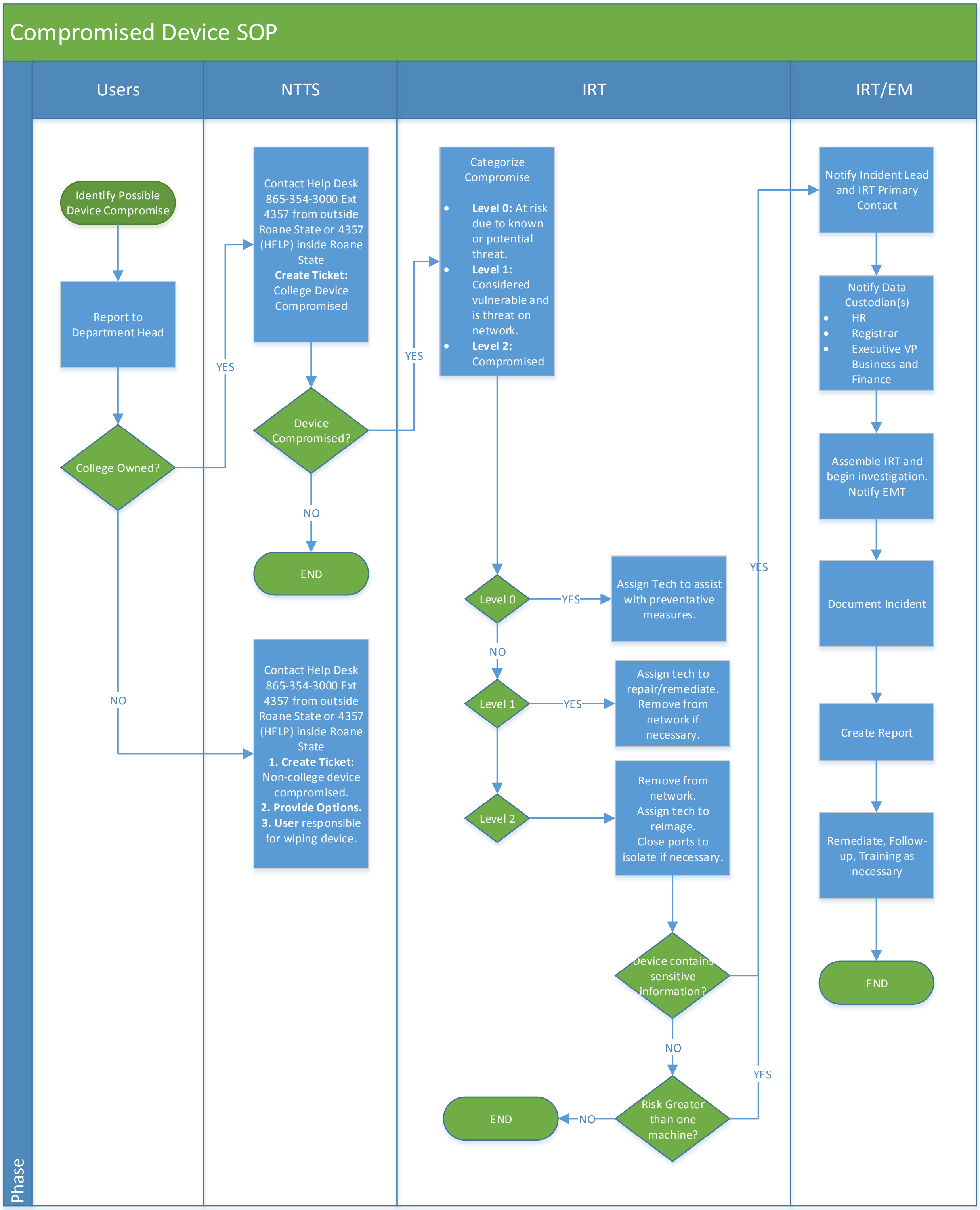

Compromised Data SOP
Users
NTTS
IRT
IRT/EM
Phase
Identify Possible Data Compromise
Notify Department Head
Identify Possible Data Compromise or Exfiltration
Notify Help Desk 865-354-3000 Ext 4357 outside RSCC or 4357 on campus
Exposure contains sensitive data
NO
Yes
Notify Data Custodian(s): HR Registrar Finance
Clean/Reimage System
Document Incident
Create Report
Remediate, Follow-up, Training as necessary
END
Notify Incident Lead and IRT Primary Contact
Assemble IRT and begin investigation. Notify EMT
Notify TBR, Chief of Police, Other Law Enforcement (if necessary)
Develop Communications Plan
Notify Affected Users
Create Report
Remediate, Follow-up, Training as necessary
END

Appendix I: Compromised Account Standard Operating Procedure (SOP)



Compromised Account SOP
Phase
Users
NTTS
IRT
IRT/EM
Identify Possible Account Compromise
Contact Help Desk 865-354-3000 Ext 4357 from outside RSCC or 4357 on campus
College Owned?
Yes
NO
Advise User to change password and contact credit agencies
Help Desk creates ticket "Possible Compromised Account"
Help Desk walks user through account password reset
Employee Account?
Yes or Unsure
NO
User has access to PII, PCI or FERPA data?
RSCC System compromised?
Yes or Unsure
END
Clean/Reimage System
Notify Incident Lead and IRT Primary Contact
Notify Incident Lead and IRT Primary Contact
Assemble IRT and begin investigation. Notify EMT
Document Incident
Create Report
Remediate, Follow-up, Training as necessary
END

Appendix J: Compromised Device Standard Operating Procedure (SOP)


Compromised Device SOP
Users
NTTS
IRT
IRT/EM
Phase
Identify Possible Device Compromise
Report to Department Head
College Owned?
YES
NO
Contact Help Desk 865-354-3000 Ext 4357 from outside Roane State or 4357 (HELP) inside Roane State **Create Ticket:** College Device Compromised
Device Compromised?
YES
NO
END
Contact Help Desk 865-354-3000 Ext 4357 from outside Roane State or 4357 (HELP) inside Roane State **1. Create Ticket:** Non-college device compromised. **2. Provide Options. 3. User** responsible for wiping device.
Categorize Compromise
• **Level 0:** At risk due to known or potential threat.
• **Level 1:** Considered vulnerable and is threat on network.
• **Level 2:** Compromised
Level 0
YES
Assign Tech to assist with preventative measures.
NO
Level 1
YES
Assign tech to repair/remediate. Remove from network if necessary.
Level 2
Remove from network. Assign tech to reimage. Close ports to isolate if necessary.
Device contains sensitive information?
YES
NO
Risk Greater than one machine?
YES
NO
END
Notify Incident Lead and IRT Primary Contact
Notify Data Custodian(s)
• HR
• Registrar
• Executive VP Business and Finance
Assemble IRT and begin investigation. Notify EMT
Document Incident
Create Report
Remediate, Follow-up, Training as necessary
END

Appendix K: Cyber Incident Reporting Form

A electronic version of this form is stored on the Information Technology Team Site on SharePoint (https://sharepoint.roanestate.edu/sites/IT/IncidentResponse/Forms/AllItems.aspx). The electronic form is to be used for reporting, it is provided in this document for information purposes only.

Cyber Incident Investigation Report Form

Incident Detector's Information:

Name: ______________________________ Title: ______________________________

Phone: ______________________________ Cell: ______________________________

E-mail: ____

Detector's Signature: ____

Incident Summary:

Incident Detection
Date and Time Detected: ____

Detection Method and/or
Location: ____

Additional Information:
____
____

Incident Type

- □ Malicious Code
- □ Unauthorized Access
- □ Denial of Service
- □ Unauthorized Use
- □ Espionage
- □ Probe
- □ Hoax
- □ Other:

Key fingerprint =

Roane State

Incident Survey:

Campus or Site: ______________________________

Specific Location(s)
of affected systems: ______________________________

Describe affected information system(s) (one form per system is recommended):

Hardware Manufacturer: ______________________________
Serial Number: ______________________________
Property Tag Number (if applicable): ______________________________

Is the affected system connected to a network?

- ☐ YES
- ☐ NO

System Name: ______________________________
MAC Address: ______________________________
System Network Address: ______________________________

Describe the physical security of the location of affected information systems
(locks, security alarms, building access, etc):

Incident Containment

Isolate affected Systems:

Incident Response Team Primary Contact approved removal from network?

☐ YES

☐ NO

If YES, date and time systems were removed: ____

If NO, state the reason: ____

Backup affected systems:

System backup successful for all systems

☐ YES

☐ NO

Name of persons who did backup: ____
Date and time backups started: ____
Date and time backups complete: ____
Backup files secured:

☐ YES

☐ NO

Backup Storage Location: ____

Signature:____

Date: _________________________

Incident Eradication

Name of persons performing forensics on systems: ____________________________________

Was the vulnerability identified?

□ YES
□ NO

Describe:

What was a validation procedure used to ensure problem was eradicated:

Communication Log

Date: ____________ Time: ______ •am • pm	Method (email, phone, etc): _____________
Initiator Name: ________________________ Initiator Title: _________________________ Initiator Organization: __________________ Initiator Contact Info: ___________________	Receiver Name: ______________________ Receiver Title: ________________________ Receiver Organization: _________________ Receiver Contact Info: ___________________
Details:	

Date: ____________ Time: ______ •am • pm	Method (email, phone, etc): _____________
Initiator Name: ________________________ Initiator Title: _________________________ Initiator Organization: __________________ Initiator Contact Info: ___________________	Receiver Name: ______________________ Receiver Title: ________________________ Receiver Organization: _________________ Receiver Contact Info: ___________________
Details:	

Date: ____________ Time: ______ •am • pm	Method (email, phone, etc): _____________
Initiator Name: ________________________ Initiator Title: _________________________ Initiator Organization: __________________ Initiator Contact Info: ___________________	Receiver Name: ______________________ Receiver Title: ________________________ Receiver Organization: _________________ Receiver Contact Info: ___________________
Details:	