

**Technology Services**

 **Incident Response Plan Template**

**Prepared By:**

**[Insert Unit Name]**

# Acknowledgements

This document is the product of a SURA working group created by the SURA IT Committee and comprised of the following individuals: Gary Crane (SURA - Director of IT Initiatives), Hunter Ely (Tulane University - Chief Information Security Officer), David Farris (George Mason University – Director of Safety and Emergency Management), Leo Howell (North Carolina State University – Assistant Director for IT Security & Compliance), Randy Marchany (Virginia Tech - University Information Technology Security Officer), and Russ Ward (University of Alabama in Huntsville (Chief Information Security Officer).

# Forward

This template is intended to be customized to meet an individual institution’s needs. Not all components of this template may be required for all institutions and there will be unique requirements of some institutions that will require additions to this template. This template is intended to provide a starting point for developing and documenting response procedures to various information technology incidents that impact institutional operations, access, or security. This *Technology Services Incident Response Plan* provides for the definition of specific roles and responsibilities for Technology Services personnel to help them manage and respond to foreseeable information technology incidents. Furthermore, this plan describes how Technology Services incidents can be integrated with an institution’s standing operational groups (e.g., Emergency Operations Group, academic units, system/server administrators) and the manner in which incidents should be communicated to end users. The strategies outlined herein are based on industry best practices and are recommended by Southeastern Universities Research Association (SURA) Information Technology group member institutions.

**Future Versions**

Please send suggestions for corrections and expansions to this document to Gary Crane (gcrane@sura.org) for inclusion in future revisions.

#

# Revision Record

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Author | Date | Requester | Description |
| 1.0 |  D. Farris | 3/24/15  |   | Initial Draft |
| 1.1  | G. Crane | 6/2/15 |   | Edits from Tulane added |
| 1.2 | G. Crane | 7/13/15  |   | Convert to Word and format |
| 1.3  | R. Marchany | 9/29/15 |   | Edits added |
| 1.4 | D. Farris | 10/04/15 |   | Formatting, content and edits  |
| 1.5 | G. Crane | 10/19/15 |   | Continued edits |
| 1.6 | D. Farris | 11/04/15 |   | Final Review |

Table of Contents

[Acknowledgements 1](#_Toc434399961)

[Forward 1](#_Toc434399962)

[Revision Record 2](#_Toc434399963)

[Acronyms 6](#_Toc434399964)

[1.0 Introduction 7](#_Toc434399965)

[1.1 Purpose 7](#_Toc434399966)

[1.2 Scope 7](#_Toc434399967)

[2.0 Roles and Responsibilities 8](#_Toc434399968)

[2.1 Technology Services Incident Commander 8](#_Toc434399969)

[2.2 Technology Services Incident Response Team 9](#_Toc434399970)

[2.3 Technology Services EOG Representative/Liaison Officer 10](#_Toc434399971)

[2.4 Institutional Emergency Operations Group 10](#_Toc434399972)

[3.0 Preparation 11](#_Toc434399973)

[3.1 Incident Response Planning 11](#_Toc434399974)

[3.2 Incident Response Plans 12](#_Toc434399975)

[3.3 Training and Exercises 12](#_Toc434399976)

[3.4 Incident Resources 12](#_Toc434399977)

[3.4.1 Personnel Contact Information 13](#_Toc434399978)

[3.4.2 Conference Call and Web Conference Procedures 13](#_Toc434399979)

[3.4.3 Critical Resources 13](#_Toc434399980)

[4.0 Notification Procedures 14](#_Toc434399981)

[4.1 Initial Notification and Incident Reporting 14](#_Toc434399982)

[4.2 Notification Procedures 14](#_Toc434399983)

[4.3 Internal Technology Services Notification 16](#_Toc434399984)

[4.4 Notification to External Server or System Administrators 16](#_Toc434399985)

[4.5 Notification to End Users 16](#_Toc434399986)

[4.6 Notification to Federal and State Agencies 17](#_Toc434399987)

[4.7 Emergency Notification Procedures 17](#_Toc434399988)

[5.0 Response Procedures 18](#_Toc434399989)

[5.1 General Response Procedures 18](#_Toc434399990)

[5.2 Scheduled or Unscheduled System Maintenance/Shutdown Procedures 19](#_Toc434399991)

[5.2.1 Emergency Shutdown Procedures 20](#_Toc434399992)

[5.3 Denial of Service Attack 21](#_Toc434399993)

[5.4 Malicious Web Hack 21](#_Toc434399994)

[5.5 Phishing Attack 22](#_Toc434399995)

[5.6 Compromised Credentials 22](#_Toc434399996)

[5.7 University Closure 22](#_Toc434399997)

[5.7.1 Short Term Non-Emergency Closure 22](#_Toc434399998)

[5.7.2 Emergency or Long-term Closure 23](#_Toc434399999)

[5.7.3 Critical Technology Services Functions 24](#_Toc434400000)

[5.8 Data Center Power or Utility Failure 24](#_Toc434400001)

[5.9 Suspected Data Breach 25](#_Toc434400002)

[5.9.1 Common methods of detecting compromises 25](#_Toc434400003)

[5.9.2 Data Breach Response Actions 26](#_Toc434400004)

[5.9.3 Eradication & Recovery 29](#_Toc434400005)

[5.10 Damage to Technology Services Space and Equipment 30](#_Toc434400006)

[6.0 Disaster Recovery and Business Continuity 30](#_Toc434400007)

[6.1 Disaster Recovery Site Activation 31](#_Toc434400008)

[6.2 Communications 31](#_Toc434400009)

[6.3 Staffing 32](#_Toc434400010)

[6.4 Critical Technology Services Shut Down Procedures 32](#_Toc434400011)

[6.6 Backup & Replication Action Steps 34](#_Toc434400012)

[6.7 Disaster Recovery Business Continuity Site Operations 34](#_Toc434400013)

[7.0 Continuity and Recovery 35](#_Toc434400014)

[7.1 Critical Applications 35](#_Toc434400015)

[7.2 Technology Services Alternate Work Locations 35](#_Toc434400016)

[7.3 Resume Operations at Primary Data Center 36](#_Toc434400017)

[7.3.1 Recovery Team 36](#_Toc434400018)

[7.3.2 Recovery Steps 36](#_Toc434400019)

[8.0 Post-Incident Activities 37](#_Toc434400020)

[8.1 After Action Reporting 37](#_Toc434400021)

[Appendix A: Technology Services Contact List 39](#_Toc434400022)

[Appendix B: University and External Contact List 42](#_Toc434400023)

[Appendix C: Critical Resources Directory 43](#_Toc434400024)

[Appendix D: Incident Response Form 45](#_Toc434400025)

# Acronyms

**CIO** Chief Information Officer

**DRBC**  Disaster Recovery/Business Continuity

**EOC** Emergency Operations Center

**EOG** Emergency Operations Group

**EOP**  Emergency Operations Plan

**IOC** Indication of Compromise

**RTO** Recovery Time Objective

**TLSO** Technology Services Liaison Office

**TSIC** Technology Services Incident Commander

**TSIRT**  Technology Services Incident Response Team

# 1.0 Introduction

This plan outlines incident response procedures that Technology Services will observe whenever an event adversely impacts technology services on [Insert University] campuses or properties occupied by university students, faculty, or staff.

## 1.1 Purpose

The primary purpose of the Technology Services Incident Response Plan is to document an orderly preparation and response strategy to deal with any event that adversely affects Technology Services operations and to integrate the technology services incident response and recovery plan into the institutional Emergency Operations Plan (EOP).

## 1.2 Scope

In the context of this plan, Technology Services incident response priorities are:

1. Identify a Technology Services Incident Response Team (TSIRT).
2. Ensure that TSIRT personnel are integrated into the institutions emergency response plans and procedures.
3. Maintain departmental plans and procedures for emergencies (i.e., disaster recovery site activation, responsibilities of designated/essential personnel, continuity of operations plans, procedures for managing phone, network, server outages, etc.)
4. Communicate impacts, failures, and/or availability of Technology Services infrastructure or services to the appropriate institutional authority in an emergency (e.g., the emergency operations group or equivalent).
5. Ensure that telecommunications, data, network, server, and email systems not hosted at an off-site back-up location operate as long as possible.
6. Work with the university administration to issue emergency communications via SMS, email and telephone emergency broadcast messages or provide technology services to support emergency messaging.
7. Shut down and secure Technology Services computer labs, classrooms, meeting rooms and other campus facilities and offices in the event of a university closure.
8. Ensure that all Technology Services personnel who are identified as designated are aware of this designation and understand their roles and responsibilities in an emergency.
9. Begin recover by assessing any damage to equipment (technology-related and environmental systems-related) and contact support/hardware providers to obtain replacement parts or equipment.
10. Migrate essential services to an off-site back-up service in a timely and orderly fashion if necessary.
11. Restore all operable systems not at the Disaster Recovery Business Continuity (DRBC) to service within two hours after the university reopens.
12. Restore DRBC services to normal operations as soon as practical.

#

# 2.0 Roles and Responsibilities

During a Technology Services incident, the following organizational structure will be adopted to facilitate coordination and communication across Technology Services units and the institution’s emergency operations group.

**Fig. 1** **Example Organization Chart**

## 2.1 Technology Services Incident Commander

The Technology Services Incident Commander (TSIC) is the individual most qualified to respond to or manage a technology services incident. The TSIC may be different for each incident and is appointed by the Chief Information Officer (CIO).

The primary responsibility of the TSIC is overall management of the incident and the university’s response activities. In addition, the TSIC serves as staff to the Emergency Operations Group (EOG). Specific responsibilities related to institutional technical incident response and recovery include:

* Direct and coordinate emergency response preparation steps.
* Convene the TSIRT when necessary and coordinate routine meetings as necessary throughout an incident to manage TSIRT activities and to maintain situational awareness.
* Monitor and coordinate Technology Services activities during and after an incident.
* Monitoring incident progress and consult/liaise with the institutional Emergency Operations Group (EOG) and external authorities as necessary
* Appoint at Technology Services Liaison Officer (TSLO) to communicate ongoing response and recovery operations to the institution’s EOG or Senior Leadership.
* Inform the EOG when Technology Services are compromised, unavailable, or will be resumed.
* Provide other necessary recommendations to the EOG to ensure the safety of personnel and university assets before, during, and after an incident.

|  |  |
| --- | --- |
| Technology Services Incident Type | Incident Commander |
| *Ex. Data Breach* | *Ex. Michael Dell* |
| [Insert Incident Type] | [Insert Position or Name] |
| [Insert Incident Type] | [Insert Position or Name] |
| [Insert Incident Type] | [Insert Position or Name] |
| [Insert Incident Type] | [Insert Position or Name] |
| [Insert Incident Type] | [Insert Position or Name] |
| [Insert Incident Type] | [Insert Position or Name] |

## 2.2 Technology Services Incident Response Team

The TSIRT consists of the following individuals or their delegates:

* [Insert Position or Name]
* [Insert Position or Name]
* [Insert Position or Name]
* [Insert Position or Name]
* [Insert Position or Name]
* [Insert Position or Name]
* [Insert Position or Name]
* [Insert Position or Name]

The TSIRT is responsible for the following:

* Convene at the request of the TSIC or upon notification of a technology services incident
* Coordinate forensic or response activities for all units/personnel under their leadership.
* Report the status of technology services systems or services to the TSIC or other as necessary to facilitate response and recovery procedures.
* Make requests for additional resources and support to the TSIC as necessary.
* Participate in routine meetings of the TSIRT.

## 2.3 Technology Services EOG Representative/Liaison Officer

The TSLO will remain in contact with the TSIC throughout the incident and relay information as necessary to units/groups external to Technology Services (e.g., the institution’s EOG, external stakeholders, clients, end users, etc.). Where possible, the TSLO should also be a standing member of the EOG. Specific responsibilities of the TSLO are:

* Relay information as appropriate and necessary to the institution’s EOG or senior leadership.
* Manage requests for information from the EOG or Senior Leadership.
* Review, edit, coordinate and/or approve all messages to the university community that contain technical information regarding the incident.

## 2.4 Institutional Emergency Operations Group

The EOG is responsible for coordinating university emergency response and recovery operations. Technology Services is represented on the EOG. Upon activation of the EOG, Technology Services will coordinate attendance of one or more Technology Services EOG representatives. The following positions have been identified as Technology Services EOG members.

* [Insert Position]
* [Insert Position]
* [Insert Position]
* [Insert Position]

The EOG will convene in the Emergency Operations Center (EOC), [Insert Primary Location], or if necessary at the alternate EOC located at [Insert Location].

In an emergency and during recovery the institution’s EOG is collectively responsible for the following:

* [Insert roles and responsibilities from the institution’s EOP or Emergency Support Functions (ESF)]
* [Insert roles and responsibilities from the institution’s EOP or Emergency Support Functions (ESF)]
* [Insert roles and responsibilities from the institution’s EOP or Emergency Support Functions (ESF)]
* [Insert roles and responsibilities from the institution’s EOP or Emergency Support Functions (ESF)]
* Etc…

#  3.0 Preparation

The university maintains emergency preparedness and response information for various emergency situations that may occur. The following links provide information on how university employees and departments to prepare for and respond to various types of emergencies.

* [Insert Link to University Local or State Emergency Management Website}
* [Insert Additional Links As Necessary]
* [Insert Additional Links As Necessary]

For more information about university emergency preparedness and response procedures please contact [Insert Office/Department Name] at [Email Address] or [(XXX)-XXX-XXXX].

## 3.1 Incident Response Planning

[Insert Position or Department] is responsible for maintaining incident response plans or coordinating updates to plans by Technology Services departments. Specific responsibilities of [Insert Position or Department] are:

1. Update the *Technology Services Incident Response Plan* each spring.
2. Identify official institutional emergency notification processes that provide information and instructions to faculty, staff, students, and parents during emergency situations.
3. Ensure department equipment inventory lists are current.
4. As necessary, verify department inventory list with University’s Property Management Department.
5. Maintain Purchase Orders or other documentation, if available, that describes Technology Services equipment and indicates the purchase price and purchase date of that equipment for insurance purposes.
6. Update employee contact information regularly.
7. Communicate changes to this plan and associated incident response plans (see section 3.2) as necessary to all affected parties.
8. Conduct training and exercises as necessary to ensure that all individuals identified in incident response plans are capable of carrying out their duties.

## 3.2 Incident Response Plans

Technology services maintains the following incident response plans to support the strategies and incident response procedures outlined in this *Technology Services Incident Response Plan*.

* [*Ex. DRBC Site Activation Procedures, See Appendix ?*]
* [Plan name – description of its purpose and scope, See Appendix ?]
* [Plan name – description of its purpose and scope, See Appendix ?]

## 3.3 Training and Exercises

Technology Services conducts routine training on incident response procedures and holds an annual exercise to test personnel and documented response plans. [Explain how this is accomplished and responsible party]

## 3.4 Incident Resources

The following resources are available to assist Technology Services personnel when responding to immediate hazards associated with an incident.

|  |  |
| --- | --- |
| [Insert Building Name] | [Insert Physical Address] |
| Resource (physical or virtual) | Location (physical/virtual, i.e., URL, shared drive) |
| *Ex. Emergency Go-Kits* | *Ex. Admin Suite, Data Center, Break Room* |
| *Ex. Emergency Procedures Guide* | *Ex. Admin Suite – Emergency Binder* |
| *Ex. First Aid Kit* | *Ex. 3rd Floor Women’s and Men’s Restrooms* |
| *Ex. Hand Held Radio Cache* | *Ex. Tech Services Storage Room Rm. 203* |
| [Insert Name of Resource] | [Insert Location] |
| [Insert Name of Resource] | [Insert Location] |
| [Insert Name of Resource] | [Insert Location] |

*Note: Provide additional tables if Technology Services occupies more than one building*

### 3.4.1 Personnel Contact Information

Technology Services maintains a list of designated/key personnel that may be called upon to respond to an incident. Appendix A provides a list of personnel, titles, home, cell, email, and social media contact information. This is maintained by [Insert Position(s) or Name] and is available [Identify Location]. A university wide emergency contact list is available [Identify Location]. Changes to the list should be communicated to [Insert Position or Name].

### 3.4.2 Conference Call and Web Conference Procedures

In the event that a physical meeting is impractical or impossible, Technology Services maintains a conference call number and web conference capability to facilitate virtual meetings. These systems can be used to coordinate emergency response and recovery procedures and hold virtual TSIRT meetings. In the event that a conference call is needed, the initiator will notify the TSIRT or others as necessary via [Insert Communications Method, e.g., email, SMS] indicating the date, time, and subject of the call.

**Conference Call Web Conference**

Call In Number: (XXX)-XXX-XXXX Conference URL: [Insert URL]

Pin Number: XXX-XXX-XXXX Access: [Insert Access Process]

Leader Code: XXXX

###

### 3.4.3 Critical Resources

A list of critical resources necessary to support, maintain, or recover Technology Services applications and servers is provided in Appendix C. This list identifies the principal hardware/infrastructure necessary to conduct the response procedures outlined in this plan.

# 4.0 Notification Procedures

## 4.1 Initial Notification and Incident Reporting

All users (internal or external) of university information systems must report suspected data breaches, technology system failures, or other Technology Services issue through one of the following means:

* [Insert Incident Reporting Process/Policy]
* [Insert Incident Reporting Process/Policy]
* [Insert Incident Reporting Process/Policy]

Once a Technology Services issue has been reported, a [Insert Process, e.g., ticket, work order, service request] will be generated to track the status of the incident throughout the response process. Depending on the level of risk involved, incidents initially reported to Technology Services may be escalated by any member of Technology Services and require the activation of the TSIRT.

Note: If at any time the TSIRT determines the incident involves criminal or other legal issues (e.g., child pornography), then the appropriate unit, [Insert Unit/Department e.g. Office of General Counsel and/or University Police], must be notified immediately. In the event of a security breach of payment card information, the Office of General Counsel must be contacted immediately.

## 4.2 Notification Procedures

Internal Technology Services communications are necessary to coordinate responses to technology service incidents or conditions affecting technology service availability. Furthermore Technology Services has an obligation to notify end users and systems owners of incidents affecting performance or availability. Incidents should be evaluated on a case by case basis to determine who must be notified and when however in general anticipated technology services incidents should be communicated to the following audiences:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| AudienceIssue | Senior IT Leadership (CIO, DCIO, Ex. Dir) | TSIRT | Specific Technology Services Unit/ Department | All Users or Specific Users | External System Admins |
| Network Outage | X | X | [Insert Unit/Dept.] | X |  |
| Telecommunication Outage | X | X | [Insert Unit/Dept.] |  |  |
| Web Server Outage | X | X | [Insert Unit/Dept.] | X |  |
| Data System Outage | X | X | [Insert Unit/Dept.] |  |  |
| Power Outage Affecting Technology Services |  | X | [Insert Unit/Dept.] |  |  |
| Phishing Attach |  |  | [Insert Unit/Dept.] | X |  |
| Denial of Service | X | X | [Insert Unit/Dept.] | X |  |
| Website Failure | X | X | [Insert Unit/Dept.] |  |  |
| Data Breach | X | X | [Insert Unit/Dept.] |  |  |
| Compromised Credentials |  |  | [Insert Unit/Dept.] | X |  |
| Temporary shutdown of non-critical system |  |  | [Insert Unit/Dept.] | X | X |
| Temporary shutdown of critical system | X | X | [[Insert Unit/Dept.] | X | X |
| [Insert Incident] |  |  | [Insert Unit/Dept.] |  |  |
| [Insert Incident] |  |  | [Insert Unit/Dept.] |  |  |
| Notifications | Yes (Provide Justification) | No (Provide Justification) |
| State/Local Law Enforcement |  |  |
| Federal Law Enforcement |  |  |

## 4.3 Internal Technology Services Notification

In the event that a communication to technology services is warranted to notify personnel of an incident or business continuity event, the following procedures will be followed:

1. Contact [Insert Unit/Position/Name and Backup]
2. [Insert Process]
3. [Insert Process]
4. Etc….
5. Etc….

*Note: consider using a listserv or call tree to identify who may initiate a message, who must draft/edit the message, and who has authority to send messages, who manages responses/questions. This system should be tested on a routine basis and documented in testing and exercises.*

## 4.4 Notification to External Server or System Administrators

Whenever an incident affects external server or system administrators, Technology Services is responsible for providing technical support to mitigate, respond, or recover from the incident. Communications with external server and systems administrators will be conducted by the following units/individuals as directed by TSIRT or the TSIC.

|  |  |  |  |
| --- | --- | --- | --- |
| Server/System | Primary Contact | Alt. Contact | Tech Service Responsible Party |
| *Ex. Cable Television* | *Ex. David Hasselhof 123-456-7890* *thehof@knightrider.com* | *Ex. Barry Allen, 123-456-7890* *flash@toofast.com* | *Ex. Network Services Director* |
| [Insert Server/System] | [Insert Name, Phone, and Email] | [Insert Name, Phone, and Email] | [Insert Technology Services Name/Position] |
| [Insert Server/System] | [Insert Name, Phone, and Email] | [Insert Name, Phone, and Email] | [Insert Technology Services Name/Position] |
| [Insert Server/System] | [Insert Name, Phone, and Email] | [Insert Name, Phone, and Email] | [Insert Technology Services Name/Position] |
| Etc…  |  |  |  |

## 4.5 Notification to End Users

##

TSIRT will determine if end users must be notified of a technology service incident. When a message is warranted the following procedures will be followed.

1. Contact [Insert Unit/Position/Name and Backup]
2. [Insert Process]
3. [Insert Process]
4. Etc.
5. Etc.

*Note: consider who may initiate a message, who must draft/edit the message, and who has authority to send messages, who manages responses/questions. This system should be tested on a routine basis and documented in testing and exercises.*

## 4.6 Notification to Federal and State Agencies

The following incidents must be reported to federal and/or state agencies in accordance with federal, state, or university regulations and policies.

|  |  |  |  |
| --- | --- | --- | --- |
| Incident | Agency | Primary Contact | Alternate Contact |
| *Ex. Data Breach* | *Ex. FBI* | *Ex. Steven Seagal 123-456-7890 sseagal@worstmovie.com* | *Ex. Chuck Norris 123-456-7890 cnorris@roundhouse.com* |
| [Insert Incident] | [Insert Agency] | [Insert Contact Name, Number, and Email] | [Insert Contact Name, Number, and Email] |
| [Insert Incident] | [Insert Agency] | [Insert Contact Name, Number, and Email] | [Insert Contact Name, Number, and Email] |
| Etc… |  |  |  |

When contacting the agency, the following information should be provided:

1. Description of the incident to include date and time first discovered;
2. Current status of the incident (e.g., on-going, contained, etc.);
3. List of agencies involved or notified;
4. Actions taken to notify affected parties;
5. Potential or know compromised personally identifiable information;
6. Financial information (user or institution);
7. Federally regulated information and intellectual property subject to export controls;
8. Sensitive research data;
9. Etc.;
10. Etc.; and
11. Etc.

## 4.7 Emergency Notification Procedures

Emergency situations that impact the university will be distributed by [Insert Alert System Name]. Upon notification of an emergency or situation that impacts Technology Services (e.g., power outage, utility failure, fire, etc.) general emergency response procedures will be observed as directed by emergency notifications, emergency response personnel, or guidance provided in university emergency response plans and procedures. Should Technology Services need to initiate an emergency notification to the university community; the following procedures will be followed.

1. Contact [Insert Unit/Position/Name and Backup]
2. [Insert Process]
3. [Insert Process]
4. Etc.

# 5.0 Response Procedures

Upon receipt of information indicating a potential threat or an event that seriously damages Technology Services assets, a meeting of the TSIRT (called at the discretion of the TSIC or TSIRT member) will be convened either in person or electronically in order to coordinate the department's preparation, response, and recovery procedures to an impending or occurring emergency.

In order to facilitate effective communication to Technology Services staff, each director/supervisor will be responsible for contacting his or her staff regarding required activities. Each director/supervisor will designate an alternate member of their staff to act as the contact person should the director not be available. Use the Incident Response Form (see Appendix D) to document the impact, response actions, resolution, and prevention steps of each incident.

## 5.1 General Response Procedures

 The following procedures will be followed whenever an event occurs that impacts or has the potential to impact Technology Services:

1. The director/unit that identifies an issue or potential issue will convene TSIRT.
2. The TSIC will initiate an Incident Response Form (see Appendix D).
3. TSIRT will determine the impact/potential impact of the event and make the following recommendations:
	1. Notify additional units/personnel within Technology Services (see section 4.0);
	2. Conduct a forensic investigation of incident;
	3. Notify system administrators and or server owners of the incident;
	4. Take impacted hardware or applications off line until service can be restored; and
	5. Notify end users of the impact or potential impact of technology services incidents (see section 4.0).
4. Under the direction of the TSIC and TSIRT, Technology Services will coordinate an appropriate response to resolve service interruptions, respond to cyber threats, or modify operations (e.g., restrict access, initiate continuity procedures, or suspend operations) as necessary.

## 5.2 Scheduled or Unscheduled System Maintenance/Shutdown Procedures

The following steps will be taken when Technology Services determines that routine maintenance, upgrades, repairs, or other services are required that impact system operations or end user access to information technology systems. TSIRT will assign a project manager to oversee the shutdown, maintenance/repair, and restoration of services. The project manager will be responsible for the following:

1. Identify the affected systems, applications, owners, and end users.
2. Notify the EOG if the outage is anticipated to have a significant or widespread impact on university operations.
3. Draft and distribute communications to systems owners and end users that:
	1. Identifies the issue;
	2. Relays the approximate time or date range that services will be unavailable;
	3. Identifies the service(s) that will be unavailable during the outage and potential impacts or alternate processes; and
	4. Approximate date and time that services will be restored.
4. If necessary, coordinate with [Insert Institutional Communications Department] to notify affected parties and end users.

**Fig. 2: System Maintenance Notification and Coordination Chart**

### 5.2.1 Emergency Shutdown Procedures

In the event that a technology service must be suspended or shut down due to an emergency (cyber threat, physical threat, manmade threat, or natural disaster) the following procedures will be followed.

1. Activate the TSIRT to coordinate Technology Services shutdown procedures.
2. Transfer critical operations to the DRBC site if possible.
3. Notify all affected parties impacted by the shutdown.
4. Take protective measures to secure hardware, data, and equipment (e.g., secure files, protect equipment from weather or damage, and relocate equipment if necessary).
5. Notify Technology Services personnel of alternate work locations, telework procedures, or modified operating schedules.

The following systems may be shut down in an emergency. Critical functions (see section 5.7.3) must remain in service to the extent possible.

|  |  |  |
| --- | --- | --- |
| Service Area | Shut Down Lead | Shut Down Alternate |
| *Ex. Data Center* | *Ex. Director of Data Center Operations* | *Ex. Assist. Dir. Data Center Operations* |
| [Insert Service Area] | [Insert Name or Position] | [Insert Name or Position] |
| [Insert Service Area] | [Insert Name or Position] | [Insert Name or Position] |
| [Insert Service Area] | [Insert Name or Position] | [Insert Name or Position] |
| [Insert Service Area] | [Insert Name or Position] | [Insert Name or Position] |
| [Insert Service Area] | [Insert Name or Position] | [Insert Name or Position] |
| [Insert Service Area] | [Insert Name or Position] | [Insert Name or Position] |
| Etc… |  |  |

**5.3 Denial of Service Attack**

In the event that a denial of service attack is identified, the following procedures will be followed.

* 1. *Ex. Technology Services will initiate a university wide notification to all system/end users.*
	2. [Insert Process]
	3. [Insert Process]
	4. [Insert Process]
	5. [Insert Process]
	6. [Insert Process]

**5.4 Malicious Web Hack**

In the event that the institutions website must be shut down or relocated to an alternate site, [Insert Technology Services Department/Unit Name] is responsible for conducting the following steps:

* 1. [Insert Process]
	2. [Insert Process]
	3. [Insert Process]
	4. [Insert Process]
	5. [Insert Process]

**5.5 Phishing Attack**

* 1. *Ex. Technology Services will initiate a university wide notification to all system/end users.*
	2. [Insert Process]
	3. [Insert Process]
	4. [Insert Process]
	5. [Insert Process]
	6. [Insert Process]

**5.6 Compromised Credentials**

* 1. *Ex. Technology Services will initiate a university wide notification to all system/end users.*
	2. [Insert Process]
	3. [Insert Process]
	4. [Insert Process]
	5. [Insert Process]
	6. [Insert Process]

**5.7 University Closure**

During university closures or a modified operating schedule due to severe weather, emergency, holiday, or other event, employees should take actions to protect critical technology services and documents. Directors/supervisors should coordinate staffing as appropriate to support critical business operations.

### 5.7.1 Short Term Non-Emergency Closure

During a non-emergency closure all technology systems should remain fully operational.

All employees are expected to prepare their work area using the procedures below prior to their release from campus/offices. This includes securing critical documents, confidential data, and shutting down non-essential systems. Short term closures are closures precipitated by winter weather, university holidays, or other conditions that do not present a threat to technology services or university infrastructure. During a campus closure, it is expected that the following will occur:

* Normal business and academic activities are suspended.
* Employees will continue to monitor [Insert Emergency Alert Name], the university website, and local media.
* Designated/essential employees are expected to maintain critical technology services for the duration of the closure unless otherwise directed by their supervisor.

### 5.7.2 Emergency or Long-term Closure

During a prolonged university closure due to severe weather, hurricane, flooding, fire, or other regional emergencies or infrastructure damage, employees are expected to do the following to protect hardware, data, and confidential information.

* Secure all critical papers, pictures, books and other loose items in a cabinet, desk or closet.
* Back up computer hard drives. Make two copies. Use CD’s, flash drives, etc.; secure one in the work area and maintain one copy off site in a secure location.
* Unplug all electrical equipment. When unplugging cables for computer equipment, be sure to label the cables to allow for rapid installation after the emergency.
* Move items away from outside windows to an interior area or against an interior wall especially if a tree, bush, or unsecured items are located near the outside windows.
* Pick equipment up off the floor if possible. Cover with plastic and secure with tape or place in a large plastic garbage bag all office equipment, scientific instruments, fine art, antiques and computers, if possible, especially if an outside tree, large bush, or movable items are near the window.
* Close and lock (or secure with tape) all filing cabinets.
* Close and lock all windows, if needed.
* Turn off any natural gas.
* Stow telephones in desks, closets, or cabinets.
* Clean out personal or shared refrigerators and remove trash from building before leaving.
* Take any emergency response procedures, contact lists, and University issued laptops home.
* Take personal items and backup disks home.
* Before leaving, meet with your supervisor, confirm telephone numbers and establish a check in schedule if the event is anticipated to last more than two days.

### 5.7.3 Critical Technology Services Functions

The following critical functions should remain operational and available during an emergency-university or long-term closure to facilitate ongoing critical operations:

|  |  |
| --- | --- |
| Critical Function | Responsible Unit/Department |
| *Ex. Data Network* | *Ex. Network Services* |
| *Ex. Telecommunications* | *Ex. Telecom Administration* |
| [Insert Critical Function] | [Insert Responsible Unit/Department]  |
| [Insert Critical Function] | [Insert Responsible Unit/Department]  |
| [Insert Critical Function] | [Insert Responsible Unit/Department]  |
| [Insert Critical Function] | [Insert Responsible Unit/Department]  |
| [Insert Critical Function] | [Insert Responsible Unit/Department]  |

**5.8 Data Center Power or Utility Failure**

The following procedures will be followed whenever a portion of Technology Services infrastructure is impacted by a utility failure (e.g., power, heating ventilation, or air conditioning).

1. [insert title and name] will determine the extent of the impact of the utility failure
2. [insert title and name] will contact Facility Services to insure that the backup power generators for the Technology Services downtown facility are in automatic mode.
3. Facility Services will coordinate fuel delivery and preventive maintenance of the backup generators. The backup generators will remain on automatic during the storm.
4. If the power or utility failure impacts technology services, the TSIRT will be convened and will follow General Response Procedures outlined in Section 5.1.
5. [Insert Process]
6. [Insert Process]

## 5.9 Suspected Data Breach

The following cyber security data breach procedures are modeled after the [NIST 800-61](http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf) *Computer Security Incident Handling Guide*. This section provides a brief overview of the general actions, including roles and responsibilities that should be taken upon detection or report of a data breach:

1. Monitor systems for breaches or compromised infrastructure; collect reports of data breaches and other malicious acts (e.g., phishing, website hack, etc.)
2. Convene the TSIRT if a breach or security incident is discovered.
3. Identify affected systems, owners, and applications.
4. Preserve all existing data and system configurations using “memory dump’ process.
5. Determine scale/significance of the cyber security incident.
6. Conduct investigative analysis and retain evidence.
7. Engage a third party cybersecurity consultant if necessary
8. Retain evidence.
9. Prioritize the incident
10. Conduct mandatory reporting and notifications.
11. Take actions to contain the incident.
12. Eradicate the threat
13. Recover or restore affected systems and applications

### 5.9.1 Common methods of detecting compromises

The following are common methods of detecting compromised computers:

* Security monitoring
	+ Intrusion detection/prevention system alerts
	+ Vulnerability scan results
	+ Data Leak Prevention tools
	+ Security information and event management alerts
	+ File integrity monitoring alerts
	+ External notifications via [Insert Notification Method, e.g., abuse@university domain.edu]
* Local system administrator monitoring
	+ System performance degradation
	+ Anomalies detected during log monitoring
	+ Abnormal process behavior (e.g., *svcHost.exe* executing from an unexpected directory, svcHost.exe connecting over unusual ports such as port 80).

### 5.9.2 Data Breach Response Actions

***First Responder Actions:*** The actions performed in the early stages of an incident (e.g., unplugging systems from the network, shutting down the system, etc.) often directly impact the ability to efficiently determine the nature and scope of the incident. In order to preserve evidence related to active processes running on the server(s) suspected of being compromised, first responders should perform a “*memory dump*” and store it in the designated location according to the instructions at: [storage location]

***Incident Confirmation & Sensitivity Level Assessment****:* System owners and system administrators will work with [Insert Technology Services Security Department] to confirm that the reported event is an actual cyber security incident. In addition, they will determine the likelihood that sensitive data on the system suspected of being compromised or other connected systems could have been impacted. The following steps are typically performed in the sensitivity level assessment:

* Reviewing previous sensitive data scans of the suspected system or connected system and/or performance of a new sensitive data scan against the affected systems using the university provided sensitive data search tool (e.g., Identity Finder). The instructions for performing the search can be found at: [Insert Instruction Link Here].
* Consulting with system owners, system administrators, and other key stakeholders to determine the type of data stored on or accessible from the affected systems, if unknown.
* Reviewing the [Insert the Organization’s Data Classification Standards] to identify the classification level of potentially affected data.

|  |  |
| --- | --- |
| **No Sensitive Data - No Cyber Security Incident** | **Sensitive Data - Cyber Security Incident** |
| If the classification exercise reveals that the data impacted by the event is not sensitive, or there is confirmation that the event was not a cybersecurity incident, then system administrators should proceed to performing normal eradication and recovery activities, any applicable improvements to their systems, or normal troubleshooting and resolution processes.   | If the determination has been made that a cybersecurity incident did in fact occur that might have affected sensitive data, then TSIRT is responsible for coordinating the remainder of incident response procedure. |

***Investigative Analysis:*** [Insert Technology Services Security Department] performs initial analysis including memory dump analysis and review of other clues to develop a better understanding of the type of cyber security incident that has occurred.  TSIRT works with [Insert Technology Services Security Department], system owners or system administrators to conduct further investigation and resolve issues. TSIRT membership will depend on the risk-level of the incident and the skills needed to investigate and appropriately respond. Typical composition of the team involves the [Insert Technology Services Security Department], system owners, and subject matter experts associated with the impacted systems. The TSIRT may call upon other offices and resources required to carry out the investigation and remediation of the incident.

***Evidence Retention:*** TSIRT, in consultation with law enforcement [or University Police] the [Insert Office of Legal Counsel] should assess the requirements for retention of evidence gathered during the investigation. Cost should also be included as a key consideration.

***Cyber Security Consultant:*** If necessary retain the services of a cyber security consultant to assist in the forensic investigation and containment strategies.The following companies/consultants are available through existing Technology Services contracts or university insurance policies.

|  |  |
| --- | --- |
| Company/Consultant | Contact Information |
| *Ex. Bills Computer Store* | *Ex. Bill Gates, (123)-456-7890, bgates@ms.com* |
| [Insert Company Name] | [Insert Name and Contact Information] |
| [Insert Company Name] | [Insert Name and Contact Information] |

***Incident Prioritization:*** TSIRT will prioritizes the incident by estimating the criticality, impact and scope of the incident, confirming the classification of data potentially impacted, and assessing the level of importance of the affected systems. In addition, if appropriate, the TSIRT develops indication of compromise (IOC) packages to facilitate assessment against other systems connected to the compromised system to estimate the scope of the incident. Finally, TSIRT activates the predefined departmental or unit-level data breach response plan or establishes an impromptu action plan.

***Mandatory Reporting & Notifications:*** If the incident involves a breach of sensitive university data, for example, social security numbers, credit card numbers, sensitive research data, protected health information, or personally identifiable information, the TSIRT will notify appropriate internal university stakeholders so that all who need to be involved will play their roles. The following stakeholders are typically involved in reporting and notifications:

* University CIO/Vice President of Technology Services
* Director, Security & Compliance
* Incident Response Coordinator
* Primary Forensics Examiner
* Local Information Security Officer
* System owner/administrator
* Human Resources (for cases involving employee misconduct)
* Appropriate Data Steward
* Office of the General Counsel
* Internal Audit
* University Communications (for incidents that may generate publicity, or require external notifications)
* Data Owner…..
* [Insert Positions]

***Containment:*** Actions taken to contain the incident and prevent further damage should be based on pre-planned actions outlined in the unit’s breach response plan. Otherwise, in accordance with [applicable university policies], the TSIRT should take appropriate actions to contain the incident and minimize the risk to university computing resources. Containment actions will vary based on the type of system and the type of incident. The following are common containment options:

* Temporarily disconnecting the system from the network, or other methods to remove access to/from the affected system
* Blocking all communication with the system at the network level
* Temporary removal of access to affected systems or resources
* Shutting down the system
* Disabling compromised accounts
* Disabling selected system functions
* [Insert Additional Processes]

***Containment Note 1:*** Containment actions should be done in a methodical and delicate manner in order to prevent the tampering of evidence, tipping off attackers that we are on to them, and preventing other implosive actions by malicious scripts (e.g., malware could be configured to destroy data or otherwise render it useless if connection to the attacker is interrupted).

***Containment Note 2:*** If further evidence needs to be collected and preserved, the goal is to perform containment activities, to the degree possible, in parallel with additional forensics work in a manner that avoids contamination of evidence. For example, a copy of the affected system may be taken for forensic work so that containment activities can begin on the original system while forensic activities are performed on the copy.

### 5.9.3 Eradication & Recovery

After the incident has been contained it may be necessary to implement eradication and recovery activities. It is not unusual for eradication and recovery actions to take weeks or months depending on the scale of the incident. Eradication and recovery steps should be appropriately prioritized and completed in a phased approach. System administrators should take the following general actions based on the incident to eradicate infection and recover from a breach:

**Eradication**

* **Identify and Remediate.**  During eradication it is important to identify all affected hosts within the organization so that they can also be remediated.  IOC packages should be developed as needed and affected network(s) scanned so that all affected hosts within the organization can be addressed.
* **Account Change**. It may be necessary to disable breached accounts, or change passwords of affected accounts
* **Initial vulnerability scans**. Vulnerability scans should be performed against affected systems and identified weaknesses that were exploited mitigated.
* **Anti-malware.** Malware scans should be performed so that malware can be identified and deleted.

**Recovery**

* **Rebuild or re-image**. Affected computers should be rebuilt or re-imaged to eradicate viruses and/or other malware infection to minimize the chance of further hidden infection.
* **Restore**. Systems may also be restored from clean backups; compromised files may also be restored with clean backups.
* **Patching**. It is essential that systems be updated with applicable security patches, especially during eradication of infection to prevent immediate reinfection
* **Firewall**. Host-based firewalls may be enabled, and network firewalls may be added, or the rules tightened to prevent unauthorized connections.
* **Logging & monitoring**. Logging and monitoring should be improved to minimize incident detection time (e.g., university file integrity monitoring, university log monitoring and security information and event management service)
* **Overall Security Assessment.** [Technology Services Security Department] may perform and overall assessment of security of the affected area including root cause analysis, security architecture review, tools and procedures and make recommendations to management for improvements.
* **Extensive Vulnerability scans**. Extensive vulnerability scans should be performed and all security weaknesses mitigated. Depending on the incident [central security unit] may perform vulnerability scans against impacted system and other systems directly connected to them to identify critical weaknesses in the environment. System administrators are responsible for addressing identified weaknesses including correcting weak configuration settings, applying security patches as) to prevent further breaches.

**5.10 Damage to Technology Services Space and Equipment**

In the event that Technology Services office spaces, supplies, hardware, or equipment are damaged due to severe weather, fire, or other event, a report of damages should be filed with the institution’s Office of Risk Management to initiate an insurance claim. In some instances repairs and replacement of items may be covered by the institution’s insurance policy. [Insert name of institutional form] should be completed and submitted to the Office of Risk Management as soon as possible after the damage is identified and no later than three days after damages are observed.

# 6.0 Disaster Recovery and Business Continuity

*[If you have an existing disaster recovery or business continuity plan, refer to that plan here.* *If there is no existing DRBC plan the following example can be used as an initial guide]*

In the event of an emergency that requires the activation of the disaster recovery site or Technology Services business continuity/continuity of operations strategies the following procedures should be observed:

1. Convene the TSIRT to coordinate preparedness, response, and recovery operations.
2. Identify systems that are impacted or may be impacted and determine if they can be relocated, backed up, shutdown, or modified to maintain operations.
3. Notify all affected parties and provide assistance with business continuity strategies to include:
	1. Providing guidance or support to relocate or roll over phone numbers.
	2. Relocate applications to different servers or to the disaster recovery site if necessary.
	3. Provide temporary storage for databases or other applications on desktop or distributed servers that may become damaged.
	4. Assist departments and units with identifying which applications are remote hosted, locally hosted, and centrally hosted so that departments and units can make appropriate business continuity decisions.
4. Conduct DRBC site activation procedures.
	1. Activate disaster recovery site
	2. Communicate internally and externally as necessary
5. Maintain contact with senior leadership and the institution’s EOG (if activated) through the TSLO.
6. Participate in business continuity and recovery operations as necessary.

## 6.1 Disaster Recovery Site Activation

Upon notification that the data center is compromised or must be relocated due to an impeding threat (e.g., fire, storm, flooding, etc.), Technology Services will immediately take steps to activate disaster recovery or alternate site services. Below is the responsibility matrix for this action step:

|  |  |
| --- | --- |
| DR Site Activation Personnel | Responsibility |
| *Ex. Steve Jobs* | *Ex. Begin Application Recovery Sequence* |
| [Insert Name or Position] | [Insert Responsibility]  |
| [Insert Name or Position] | [Insert Responsibility]  |
| [Insert Name or Position] | [Insert Responsibility]  |
| [Insert Name or Position] | [Insert Responsibility]  |
| [Insert Name or Position] | [Insert Responsibility]  |
| [Insert Name or Position] | [Insert Responsibility]  |

A detailed [Insert Name of DRBC Site Activation Plan] documents the procedures for activating, staffing, operating, and managing the disaster recovery site. This plan is available [Insert Location].

## 6.2 Communications

Upon activation of the disaster recovery site, Technology Services is responsible for notifying the following (see section 6.0 for communications procedures):

* 1. All parties affected by the transfer of operations from the data center(s) to the DRBC site; initiate business continuity procedures for critical Technology Service functions.
	2. Advise the university’s senior leadership and EOG of the status, availability, impairment, or modification of technology services that will or do result from a DRBC site activation.
	3. All Technology Services personnel are expected to support the disaster recovery site.
	4. External Vendors that rely on data center operations/databases.
	5. Instruct Technology Services personnel of alternate work schedules, telework procedures, or changes in technology services operations as necessary.
	6. Update all affected parties on a regular basis.

## 6.3 Staffing

The following personnel are expected to make arrangements to travel to alternate site or DRBC site services location as soon as possible:

|  |  |  |
| --- | --- | --- |
| Name or Position | Primary Responsibility | Backup Responsibility |
| *Ex. Director of Network Serv.* | *Ex. DNS Switching* | *Ex. Run Initial Diagnostics* |
|  [Insert Name or Position | [Responsibility #1] | [Responsibility #2] |
|  [Insert Name or Position | [Responsibility #1] | [Responsibility #2] |
|  [Insert Name or Position | [Responsibility #1] | [Responsibility #2] |
|  [Insert Name or Position | [Responsibility #1] | [Responsibility #2] |
|  [Insert Name or Position | [Responsibility #1] | [Responsibility #2] |
|  [Insert Name or Position | [Responsibility #1] | [Responsibility #2] |

If the emergency is a regional emergency, accommodations should be made as soon as and to the extent possible to facilitate telework, virtual private networks, and remote access for all employees.

## 6.4 Critical Technology Services Shut Down Procedures

Use the [Insert Name of DRBC Site Activation Plan] to transfer critical technology services. The following services should be maintained for as long as possible or with the least amount of disruption to facilitate university operations:

|  |  |
| --- | --- |
| Critical Technology Service | Dependency |
| *Ex. Telecommunications* | *Ex. Internal and external communications* |
| *Ex. Data network* | *Ex. Email, phone, and application services* |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |
| [Insert Services] | [Insert Dependency] |

**6.5 Non-Essential Service Shutdown Procedures**

The following individuals are responsible for shutting down non-essential systems and services:

|  |  |
| --- | --- |
| Service Areas | Responsibilities |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |

## 6.6 Backup & Replication Action Steps

The following service areas are responsible for backup of critical systems and documenting backup procedures.

|  |  |
| --- | --- |
| Service Areas | Systems/Databases that Require Backup |
| *Ex. Learning Mngt. System* | *Ex. Image system, core database, system analytics* |
| [Insert Service Area Name] | [List of Systems, Applications, or Databases] |
| [Insert Service Area Name] | [List of Systems, Applications, or Databases] |
| [Insert Service Area Name] | [List of Systems, Applications, or Databases] |
| [Insert Service Area Name] | [List of Systems, Applications, or Databases] |
| [Insert Service Area Name] | [List of Systems, Applications, or Databases] |
| [Insert Service Area Name] | [List of Systems, Applications, or Databases] |
| [Insert Service Area Name] | [List of Systems, Applications, or Databases] |

## 6.7 Disaster Recovery Business Continuity Site Operations

DRBC operations will be conducted in accordance with the [Insert DRBC Plan]. The concept of operations is as follows:

* 1. *Ex. Technology Services will initiate a university wide notification to all system/end users.*
	2. [Insert Process]
	3. [Insert Process]
	4. [Insert Process]
	5. Etc…

# 7.0 Continuity and Recovery

## 7.1 Critical Applications

The following is a list of applications deemed critical to continuity of operations. In an emergency the following applications will be given priority in order to resume business operations as quickly as possible. Each application is provided with a target recovery time objective (RTO); actual recovery time may vary depending on each scenario.

|  |  |  |  |
| --- | --- | --- | --- |
| Application | Owner | Location |  RTO |
|  *Ex. Banner Elucian* | *Ex. Tech Services* | *Ex. Data Center* | *Ex. <12 Hours* |
|  [Insert Application} |  [Insert Owner] | [Insert Location] | [Insert RTO] |
| Etc… |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |

## 7.2 Technology Services Alternate Work Locations

|  |  |  |
| --- | --- | --- |
| Technology Services Function | Primary Location | Alternate Location |
|  *Ex: Telecom Admin* |  *Ex. Taj Mahal rm. 209* | *Ex. Trump Tower rm. 000* |
|  *Ex. Tech Services Executive Offices* | *Ex. Taj Mahal Third Fl.* | *Ex. Trump Tower rm. 001-010* |
|  [Insert Function] | [Insert Primary Location] | [Insert Alternate Location] |
|  Etc…  |   |   |
|   |   |   |
|   |   |   |

## 7.3 Resume Operations at Primary Data Center

In the event that the DRBC site is activated, the following steps will be taken to resume operations at the institutions primary data center. Resumption of operations will be guided by the Recovery Team [or TSIRT]. The Recovery Team is responsible for the following:

* [Insert Roles and Responsibilities]
* [Insert Roles and Responsibilities]
* [Insert Roles and Responsibilities]
* [Insert Roles and Responsibilities]
* Etc…

### 7.3.1 Recovery Team

The Recovery Team is comprised of the following positions:

* [Insert Position]
* [Insert Position]
* [Insert Position]
* [Insert Position]
* [Insert Position]

### 7.3.2 Recovery Steps

The timeline for recovery will vary depending upon the severity of any damage sustained to technology service systems. The intent is to restore operable systems to service within 48 hours after landfall service interruption or as soon as practical and safe. Below is the responsibility matrix:

|  |  |
| --- | --- |
| Service Areas | Responsibilities |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |
| [Insert Service Area Name] | [Insert Responsibilities] |

* Staff will return to campus as soon as travel and campus conditions are safe and the senior administrator in the chain of command of the EOG announces that the campus is open. Staff should monitor the University emergency notification system, the University web site, and local media for important campus information and instructions.
* Assess any damage to equipment (technology-related and environmental systems-related) and contact support providers to obtain replacements.
* Determine the status of all personnel. Assess the ability of personnel to return to work.
* As personnel return to work, begin preliminary damage assessment of office areas and workstations.
* Complete Property Loss Forms [Insert Where Form Can be Located]. Fax or deliver completed forms to the [Insert Department Name e.g., Office of Risk Management].
* Once damage assessment is complete, determine what essential supplies, equipment, space, personnel etc. are needed in order to restart the department's business or academic activity.

# 8.0 Post-Incident Activities

## 8.1 After Action Reporting

**Lessons learned**. The incident response process should evolve to reflect new threats, and technological advances. As such ongoing incident lessons learned sessions will be coordinated by [central security unit] to achieve closure with respect to incidents by reviewing what occurred, what was done to intervene, and how well intervention worked. Meetings will address questions such as:

* Exactly what happened, and at what times?
* How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
* What information was needed sooner?
* Were any steps or actions taken that might have inhibited the recovery?
* What would the staff and management do differently the next time a similar incident occurs?
* How could information sharing with other organizations have been improved?
* What corrective actions can prevent similar incidents in the future?
* What precursors or indicators should be watched for in the future to detect similar incidents?
* Where might additional user awareness and training be needed?
* How can this document be updated to improve response to the next incident?

**Incidents Response Metrics**. Another key post-incident activity is to document key metrics related to the handling of the incident, to facilitate appropriate budget and staffing plans, identify systematic security weaknesses, as well as changes in incident trends. The following metrics are required:

* Number of incidents
* Man-hours per incident
* Incident detection time (how long after the incident occurred before detected - only relevant for incidents investigated)
* Likelihood of sensitive data exfiltration
* Type of incident
* Root cause
* Estimated cost to respond and recover
* Containment action categorization
* Eradication and recovery categorization

# Appendix A: Technology Services Contact List

|  |
| --- |
|  Unit Name: Vice President/Dean for Technology Services |
| **Contact** | **Name** | **Title** | **Work** | **Cell** | **Home** | **Email** | **Alternate Email** |
| VP/CIO |   |   |   |   |   |   |   |
| Successor  |   |   |   |   |   |   |   |
| Successor |   |   |   |   |   |   |   |
| Unit Name: Technology Services Incident Response Team (TSIRT) |
| **Contact** | **Name** | **Title** | **Work** | **Cell** | **Home** | **Email** | **Alternate Email** |
| #1 |   |   |   |   |   |   |   |
| #2 |   |   |   |   |   |   |   |
| #4 |  |  |  |  |  |  |  |
| #5 |  |  |  |  |  |  |  |
| #6 |  |  |  |  |  |  |  |
| #7 |  |  |  |  |  |  |  |
| #8 |  |  |  |  |  |  |  |
| Unit Name: Network Operations Center |
| **Contact** | **Name** | **Title** | **Work** | **Cell** | **Home** | **Email** | **Alternate Email** |
| #1 |   |   |   |   |   |   |   |
| #2 |   |   |   |   |   |   |   |
| #3 |   |   |   |   |   |   |   |
| Unit Name: Data Center Operations |
| **Contact** | **Name** | **Title** | **Work** | **Cell** | **Home** | **Email** | **Alternate Email** |
| #1 |   |   |   |   |   |   |   |
| #2 |   |   |   |   |   |   |   |
| #3 |   |   |   |   |   |   |   |
| Unit Name: [Insert] |
| **Contact** | **Name** | **Title** | **Work** | **Cell** | **Home** | **Email** | **Alternate Email** |
| #1 |   |   |   |   |   |   |   |
| #2 |   |   |   |   |   |   |   |
| #3 |   |   |   |   |   |   |   |
| Unit Name: [Insert] |
| **Contact** | **Name** | **Title** | **Work** | **Cell** | **Home** | **Email** | **Alternate Email** |
| #1 |   |   |   |   |   |   |   |
| #2 |  |  |  |  |  |  |  |
| #3 |  |  |  |  |  |  |  |
| Unit Name: [Insert] |
| **Contact** | **Name** | **Title** | **Work** | **Cell** | **Home** | **Email** | **Alternate Email** |
| #1 |  |  |  |  |  |  |  |
| #2 |  |  |  |  |  |  |  |
| #3 |  |  |  |  |  |  |  |
| Unit Name: [Insert] |
| **Contact** | **Name** | **Title** | **Work** | **Cell** | **Home** | **Email** | **Alternate Email** |
| #1 |  |  |  |  |  |  |  |
| #2 |  |  |  |  |  |  |  |
| #3 |  |  |  |  |  |  |  |

# Appendix B: University and External Contact List

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  Contact | Website | Office | After Hours | Alternate | Emergency | Email |
| University Police |   |   |   |   |   |   |
| Emergency Management |   |   |   |   |   |   |
| FBI Field Office |   |   |   |   |   |   |
| Facilities Management |   |   |   |   |   |   |
| University Information |   |   |   |   |   |   |
| Public Relations |   |   |   |   |   |   |
| Human Resources |   |   |   |   |   |   |
| Risk Management |   |   |   |   |   |   |
| Legal Counsel |   |   |   |   |   |   |
| Consultant #1 |   |   |   |   |   |   |
| Consultant #2 |   |   |   |   |   |   |
| Consultant #3 |   |   |   |   |   |   |
| Consultant #4 |   |   |   |   |   |   |

#

# Appendix C: Critical Resources Directory

**I. Software Applications Systems**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Company | Application/ System | Primary Contact/ Contact Information | Alternate Contact/ Contact Information | Account/License Information If Applicable |
|   |   |   |   |  |
|   |   |   |   |  |
|   |   |   |   |  |
|  |  |  |  |  |
|  |  |  |  |  |

**II. Infrastructure**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Company | Application/ System | Primary Contact/ Contact Information | Alternate Contact/ Contact Information | Account/License Information If Applicable |
|   |   |   |   |  |
|   |   |   |   |  |
|   |   |   |   |  |
|  |  |  |  |  |
|  |  |  |  |  |

**III. Unix-based Systems**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Company | Application/ System | Primary Contact/ Contact Information | Alternate Contact/ Contact Information | Account/License Information If Applicable |
|   |   |   |   |  |
|   |   |   |   |  |
|   |   |   |   |  |
|  |  |  |  |  |
|  |  |  |  |  |

**IV. Networks, Telecom & Academic Technology Support Services**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Company | Application/ System | Primary Contact/ Contact Information | Alternate Contact/ Contact Information | Account/License Information If Applicable |
|   |   |   |   |  |
|   |   |   |   |  |
|   |   |   |   |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Content Area | Data Set | Comments |
| **Status** | Open/Closed |  |
| **Category** |   Network  Server  Applications  Firewall  Telephone  Power Outage | *Define the incident type. If none fit, provide a description of the incident.*  |
| **Reference Number** | Incident Number | *If available*  |
| **Associated Incidents** | Associated Incident Numbers | *If Available* |
| **RFC Number** |  | *Most will have none* |
| **Title Of Incident** | Outage Name | *Title as listed in the Resolved Alert.  If the Technical Service Support team did not initiate an alert, contact the Support center to enter a Resolved Alert to associate with the After Action Report.*  |
| **Location** |   Campus  Building  Floor  Room  Specific campuses Online, and Other | *Provide additional information if needed for clarity* |
| **Affected Services** | Names of specific services | *If known (i.e. Banner, etc.)* |
| **Timeline** | **Start Time:** *Date, Day, and Hour***End Time:** *Date, Day and Hour* |  |
| **Description** |  Initial Symptoms Duration Impact to university | *If you use an acronym, please include the actual term the first time you use the acronym, using a Key Performance Indicator (KPI) for example.* |
| **Root Cause Analysis** |  Cause Resolution Prevention |  |
| **Statistics** |  ITU Service Team\* ITU Technical Service Team+ | *\*These are stats like the number of circuits/servers/accounts/files restored, etc.**+ These would be stats provided by the Support Center* |
| **TSIRT Members** | *Insert names/positions of TSIRT members responding to this incident* |

# Appendix D: Incident Response Form