SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued:	Revision Date: 12/23	Page: 1 of 8 Classification Code: 10-12
		Section: INFORMATION TECHNOLOGY		
		DISASTER RECOVERY PLAN		

Objectives

The University disaster and emergency response process must reduce the disruption to university information systems to an acceptable level through a combination of preventative and recovery controls and processes. Such controls and processes must identify and reduce risks to university information systems, limit damage caused by disasters and emergencies and ensure the timely resumption of significant information systems and processes. Such controls and processes must be commensurate with the value of the information systems being protected or recovered.

Scope

Conditions for Plan Activation

For proper planning and management, this plan must specify the difference between a disaster and an emergency as the remediation process is different for each.

1. An emergency has a limited impact and is a short-term issue. Examples include:
    a. An isolated malware attack (single user or server).
    b. A compromised server or service.
    c. Power failure affecting a portion of the University's information technology (IT) assets.

2. A disaster is a significantly more disruptive or unusual event. This event can have long-term ramifications. Examples include:
    a. Loss of an entire data center or regional campus due to an earthquake or flood.
    b. Catastrophic data loss due to device failure, breach, or malware.

Disaster Recovery Plan

The University will maintain a disaster recovery plan to recover its information systems if they are impacted by a disaster. The plan must be reviewed periodically and revised as necessary. At a minimum, the recovery plan must include:

- The conditions for activating the plan.
- Identification and definition of university workforce member responsibilities.

- Resumption procedures which describe the actions to be taken to return University information systems to normal operations within established time frames.
- The order in which information systems will be recovered.
- Notification and reporting procedures.
- A maintenance schedule that specifies how and when the plan will be tested, as well as the process for maintaining the plan.

Workforce Member Responsibilities
Should the Assistant VP of Information Technology designate an emergency, the IT staff initiates Emergency Event Procedures and contacts the following Southeast Missouri State University personnel as part of the Emergency Response Team (ERT). The list below is a minimal core group:

- Assistant Vice President, Information Technology
- Director, Campus Infrastructure
- Manager, Systems and Network Services
- Director, User Services
- Director, Academic Technologies
- Information Security Officer

Emergencies that could damage the University's finances warrant the addition of the Vice President, Finance and Administration, as part of the ERT and emergencies that could damage the University's reputation warrant the addition of General Counsel as part of the ERT.

ERT Designations
ERT Leader: Assistant VP of Information Technology
ERT Incident Leader: This designation will vary based on the type of emergency. For example, infrastructure failures will be led by the Director of Campus Infrastructure, while security issues will be led by the Information Security Officer.

ERT Supporting Members: The remaining experts or responsible parties on the response team.

The members of the Emergency Response Team analyze all data concerning the incident. Depending on the emergency's breadth and severity, this team provides updates to the campus community or even the surrounding community.

Maintenance and Testing Schedule

The Southeast Missouri State University Disaster Recovery Plan, once formally approved, will be annually evaluated by the Assistant VP of Information Technology and the Information Security Officer. Based on changes in the Southeast environment, the plan will be modified for accuracy and to ensure enhanced protection of the Southeast environment.

Changes affecting the disaster recovery plan include, but are not limited to:

- Hardware
    - Upgrades, decommissioning, change of location or means of inventory collection or any additional hardware changes that may affect hardware security and access
- Software
    - Upgrades, removal/uninstallation, software permission changes or any other changes that may affect software security and access
- Facilities
    - Changes in location and access control or any other changes that may affect facility security and access
- Procedures
    - This includes changes to patching schedules, change control, backup methods or procedures, changes in purchasing or other procedures that may affect the access or security of Southeast IT assets.
- Personnel

- Personnel changes including new hires, departures or any change that may affect IT asset security or access.

In order to make any needed changes to the processes for disaster recovery, the Southeast Disaster Recovery plan must be tested twice a year. The plan testing can occur as annual tabletop exercises. Issues or weaknesses in the plan will be addressed and changes tested during the next tabletop exercise.

Disaster/Risk Prevention
Southeast Missouri State University is located in a region that presents a variety of threats both natural and man-made. This section of the disaster recovery plan examines the possible threats of the environment with steps to mitigate risk. Threats include:

- Flood
- Fire
- Earthquake
- Tornado
- Cybercrime or Data Breach
- Terrorist Event

Flood
The main campus of Southeast Missouri State University is located near the Mississippi river, but at a significantly higher elevation. The River Campus, however, is much closer to the river and thus could encounter flooding.

Preventative Measures and Recommendations
All Southeast IT assets from desktops to switches should be kept off the floor. Servers and switches should be rack-mounted and inspected regularly.

Fire
Obviously, every home, business or school suffers from the threat of a devasting fire. However, computer data centers and computer labs present a specific type of risk due to the large number

of electronic devices from servers and desktops to switches and routers. A fire of any size involving Southeast IT assets would cause a significant disruption.

Preventative Measures and Recommendations
Data centers, data closets, computer labs and offices must comply with all fire and safety regulations. Southeast data centers must have fire suppression installed and tested regularly.

Earthquake
All of the Southeast Missouri State University campuses either reside on or near the New Madrid fault line. Because of the campus locations, it is highly likely that the campus community will one day be affected by a significant earthquake.

Preventative Measures and Recommendations
The likelihood of a significant earthquake increases each year. To prevent disruption after a large quake, all racks, whether in data centers or data closets, must be secured to the floor to prevent racks from shifting or falling over.

Tornado
All Southeast campuses are located in areas that have been dramatically impacted by tornadoes and high winds in the past. The likelihood of one of the Southeast campuses being adversely affected by a tornado or high winds is great.

Preventative Measures and Recommendations
To prevent disruption after a large natural disaster, all racks, whether in data centers or data closets, must be secured to the floor to prevent racks from shifting or falling over. Additionally, data centers should be located as centrally as possible within a building. No data centers walls should be external.

Cybercrime or Data Breach

The threat of cyber incidents is increasingly exponentially each year. Unfortunately, regardless of the defenses in place to protect IT assets on campus, the likelihood of a significant cyber incident is more a matter of when than if as bad actors are always on the watch for weaknesses.

Preventative Measures and Recommendations
In spite of firewalls, user access management and server or desktop patching, the most important and effective preventative measure is user training. Ensuring students, faculty and staff can recognize phishing emails, suspicious websites and the tell-tale sign of social engineering is vital for enhanced security.

Terrorist Event
There are a variety of actions or events that are encompassed by this threat, any of which could severely disrupt services.

Preventative Measures and Recommendations
First and foremost, significant physical security is critically important to mitigate this threat. Sufficient lighting, strong locks and cameras all assist in providing enhanced physical security.

ERT Recovery Operations
The objective of any disaster recovery initiative is the restoration of computer assets and data to allow resumption of normal operations. To this end, when convened by the ERT Leader/AVP of Information Technology, the ERT (*see Workforce Member Responsibilities*), in concert with all appropriate Southeast staff, performs the following:

1. Determines what IT assets have been affected and prioritizes both assets and IT services from most important to least important to ascertain the order of restoration.
2. ERT Leader, in consultation with Southeast executive staff, may contact law enforcement if needed (based on type of event).

3. ERT leader identifies and contacts all appropriate IT staff with the skills required to restore services.
4. IT staff and other appropriate Southeast personnel determine the estimated amount of time (Hours, Days, Weeks, etc.) required for service restoration and report to the ERT.
5. The ERT leader notifies all appropriate management and staff and provides updates as needed *(see Notification and Reporting Procedures*).
6. In the event of a cybercrime (malware, ransomware, breach), appropriate IT staff isolate affected systems from the network for evidence collection and remediation.
7. In the event of server breach or remote takeover, the ERT initiates the process of server or device teardown and rebuild once all forensic evidence is collected. **NOTE**: Depending on the size and scope of the event, this determination may be made by law enforcement rather than the ERT.
8. Contacts Purchasing for rapid purchase of replacement hardware if Southeast personnel determine affected systems cannot be rebuilt.
9. If needed, begins process of restoring data from designated backups (physical or cloud-based).
10. Initiates testing by IT and campus staff and remediates issues as needed.
11. Once all required services are operational, transitions to standard maintenance mode.
12. Compiles incident report with lessons learned.

Notification and Reporting Procedures

The need and frequency of campus notifications vary based on the type and scope of an emergency. Nevertheless, all communications to executive staff regarding recovery are to come from the ERT leader. Information disseminated to Southeast leadership can be distributed to remainder of the campus at their discretion.

Reporting Methods:

The methods used by the ERT Leader to communicate with executive staff will vary based on the extent and sensitivity of the event. For instance, it may not be prudent to discuss sensitive issues or concerns via email. Therefore, Zoom or Microsoft Teams may be the selected method.

However, standard email communication may suffice for events when the information the ERT Leader is providing is more general or procedural in nature. The method selected for communicating the status of recovery efforts during an emergency or during disaster recovery is selected by the ERT Leader.

Reporting Frequency:
The frequency of communication also varies based on the type of event, the extent of damage and the speed of progress toward recovery. Dynamic events with rapid developments require a higher frequency of communication, although the rate of communication should not act as an impediment to recovery efforts. However, ERT leadership can choose to communicate on a significantly less frequent basis for events or incidents without rapid changes such as a lengthy data restoration from backup.