University of Connecticut

University Information Technology Services

Information System Contingency Plan Instructions

Prepared by
Victor Font
UITS Business Continuity / Disaster Recovery Coordinator
January 2013

Table of Contents

Attribution

This document is adapted in part from the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) Special Publication 800-series. The series reports on research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations. The NIST provides the series for use or adoption by any organization without copyright.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe a procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by UITS, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by UITS in accordance with its assigned responsibilities. The information in this publication, including concepts and methodologies, may be used by campus Information Technology organizations even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, IT organizations may wish to closely follow the development of these new publications by UITS.

Business Continuity & Disaster Recovery Policy

This policy is available in the Information Security Policy Manual.

Each University department will maintain a current, written and tested Business Continuity Plan (BCP) that addresses the department's response to unexpected events that disrupt normal business (for example, fire, vandalism, system failure, and natural disaster).

The BCP will be an action-based plan that addresses critical systems and data. Analysis of the criticality of systems, applications, and data will be documented in support of the BCP.

Emergency access procedures will be included in the BCP to address the retrieval of critical data during an emergency.

The BCP will include a Disaster Recovery (DR) Plan that addresses maintaining business processes and services in the event of a disaster and the eventual restoration of normal operations. The BCP and DR Plan will contain a documented process for annual review, testing, and revision. Annual testing of the BCP will include desk audits, and should also include tabletop testing, walkthroughs, live simulations, and data restoration procedures, where appropriate. The BCP will include measures necessary to protect Confidential Data during emergency operations.

Data Administrators are responsible for implementing procedures for critical data backup and recovery in support of the BCP. The data procedures will address the recovery point objective and recovery time objectives determined by the Data Steward and other stakeholders.

Information System Contingency Plan Development

This document discusses the key elements that compose the Information System Contingency Plan (ISCP). As described in the IT Contingency Plan and Planning Guide, ISCP development is a critical step in the process of implementing a comprehensive contingency planning program. An ISCP provides established procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including detailed roles, responsibilities, teams, and procedures associated with restoring an information system following a disruption. The ISCP documents technical capabilities designed to support contingency operations and is tailored to an organization and its requirements.

The ISCP differs from a Disaster Recovery Plan (DRP) primarily in that the information system contingency plan procedures are developed for recovery of the system regardless of site or location. An ISCP can be activated at the system's current location or at an alternate site. In contrast, a DRP is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location. Once the DRP has successfully transferred an information system site to an alternate site, each affected system would then use its respective information system contingency plan to restore, recover, and test systems, and put them into operation.

Plans need to balance detail with flexibility; usually, the more detailed the plan, the less scalable and versatile the approach. The information presented here is meant to be a guide; nevertheless, the plan format in this document may be modified as needed to better meet the user's specific system, operational, and organization requirements. UITS provides templates that organizations may use to develop ISCPs for their information systems at the appropriate Categorization of University Information and Information Systems impact level (low-, moderate-, or high-impact level). The information and templates provided are guides and may be modified, customized, and/or adapted as necessary to best meet the specific system, operational, and organizational requirements for contingency planning. Appendix A discusses planning considerations regarding personnel that should be coordinated with the ISCP development.

As shown in Figure 1, this document identifies five main components of the contingency plan. The supporting information and plan appendices provide essential information to ensure a comprehensive plan. The Activation and Notification, Recovery, and Reconstitution Phases address specific actions that an organization takes following a system disruption or emergency. Each plan component is discussed in detail later.

Plans are formatted to provide quick and clear directions in the event that personnel unfamiliar with the plan or the systems are called on to perform recovery operations. Plans are clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures are used. A concise and well-formatted plan reduces the likelihood of creating an overly complex or confusing plan.

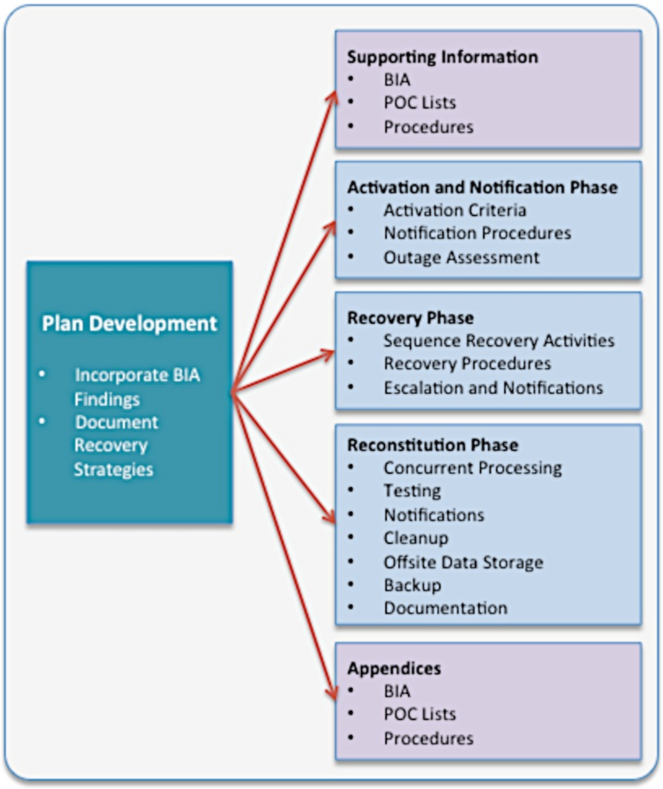

Figure 1: Information System Contingency Plan Structure

ISCPs are integrated into the UITS System Development Life Cycle and are required for all systems before being deployed to production.

Supporting Information

The supporting information includes an introduction and concept of operations section providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.

The introduction section orients the reader to the type and location of information contained in the plan. Generally, the section includes the background, scope, and assumptions.[1] These subsections are described below.

[1] This plan format is meant to guide the contingency plan developer. Individuals may choose to add, delete, or modify this format as required, to best fit the system and organization's contingency planning requirements.

- **System description**. It is necessary to include a general description of the information system addressed by the contingency plan. The description includes the information system architecture, location(s), and any other important technical considerations. An input/output (I/O) diagram and system architecture diagram, including security devices (e.g., firewalls, internal and external connections) are useful. The content for the system description can usually be taken from the System Security Plan (SSP).

- **Overview of three phases**. The ISCP recovery is implemented in three phases: (1) Activation and Notification, (2) Recovery, and (3) Reconstitution.

- **Roles and responsibilities**. The roles and responsibilities section presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.

Activation and Notification Phase

The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.

Activation Criteria and Procedure

The ISCP is activated if one or more of the activation criteria for that system are met. If an activation criterion is met, the designated authority activates the plan.[2] Activation criteria for system outages or disruptions are unique for each organization and should be stated in the contingency planning policy. Criteria may be based on:

- Extent of any damage to the system (e.g., physical, operational, or cost);
- Criticality of the system to the organization's mission (e.g., critical infrastructure protection asset); and
- Expected duration of the outage lasting longer than the Recovery Time Objective (RTO).

[2] The designated authority (typically a senior manager or CIO) has the authority to activate the contingency plan. That authority may vary based on the organization or system, but the individual with this authority should be designated clearly in the plan. Only one individual should have this authority, and a successor should be clearly identified to assume that responsibility if necessary.

The appropriate recovery teams may be notified once the system outage or disruption has been identified and the ISCP Coordinator has determined that activation criteria have been met. Notification procedures follow the procedures outlined in the following section below.

Notification Procedures

An outage or disruption may occur with or without prior notice. For example, advance notice is often given that a hurricane is predicted to affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act. Notification procedures are documented in the plan for both types of situation. The procedures describe the methods used to notify recovery personnel during business and non business hours. Prompt notification is important for reducing the effects of a disruption on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

Following the outage or disruption, notification is sent to the Outage Assessment Team[3] so that it may determine the status of the situation and appropriate next steps. Outage assessment procedures are described in the next section. When outage assessment is complete, the appropriate recovery and system support personnel are notified.

Notifications can be accomplished through a variety of methods, either automated or manual and include telephone, pager, electronic mail (email), cell phone, and messaging. Automated notification systems follow established protocols and criteria and can include rapid authentication and acceptance and secure messaging. Automated notification systems require up-front investment and learning curve, but may be an effective way for some organizations to ensure prompt and accurate delivery.

Notifications sent via email should be done with caution because there is no way to ensure receipt and acknowledgement. Although email has potential as an effective method of disseminating notifications to work or personal accounts, there is no way to guarantee that the message will be read. If using an email notification method, recovery personnel should be informed of the necessity to frequently and regularly check their accounts. Notifications sent during business hours should be sent to the work address, whereas personal email messaging may be useful in the event that the local area network (LAN) is down.

The notification strategy defines procedures to be followed in the event that specific personnel cannot be contacted. Notification procedures are documented clearly in the contingency plan. Copies of the procedures can be made and located securely at alternate locations. A common manual notification method is a call tree. This technique involves assigning notification duties to specific individuals, who in turn are responsible for notifying other recovery personnel. The call tree accounts for primary and alternate

[3] The Outage Assessment Team is a representative title. Depending on how the organization establishes their roles and responsibilities, other names and titles may be used.

contact methods and discusses procedures to be followed if an individual cannot be contacted. Figure 2 presents a sample call tree.

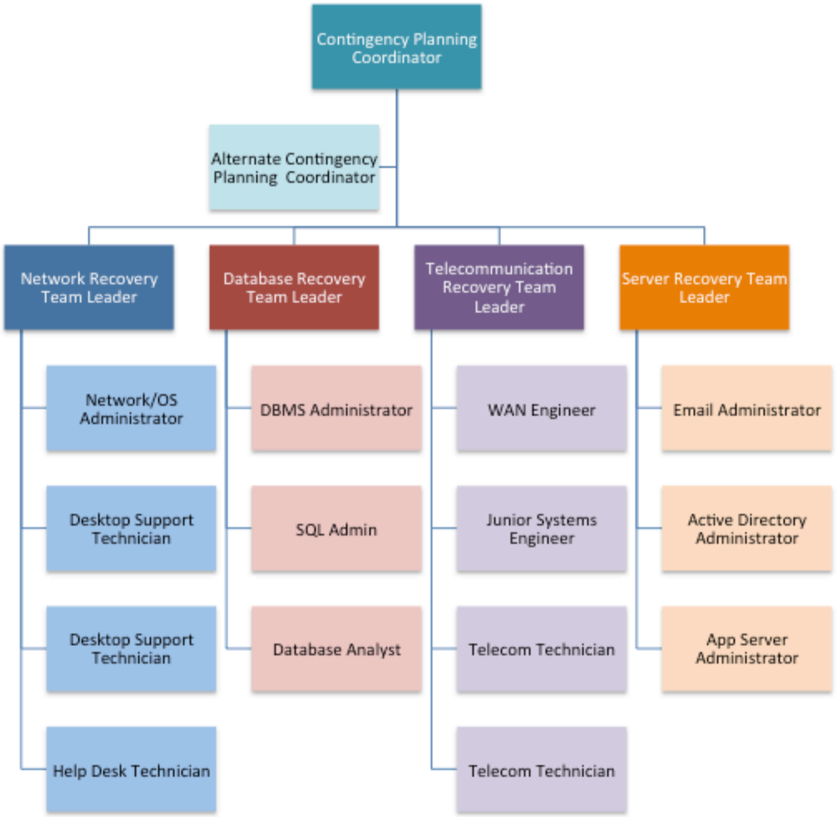
Contingency Planning Coordinator
Alternate Contingency Planning Coordinator
Network Recovery Team Leader
Database Recovery Team Leader
Telecommunication Recovery Team Leader
Server Recovery Team Leader
Network/OS Administrator
Desktop Support Technician
Desktop Support Technician
Help Desk Technician
DBMS Administrator
SQL Admin
Database Analyst
WAN Engineer
Junior Systems Engineer
Telecom Technician
Telecom Technician
Email Administrator
Active Directory Administrator
App Server Administrator

Figure 2: Sample Call Tree

Personnel to be notified are clearly identified in the contact lists appended to the plan. This list identifies personnel by their team position, name, and contact information (e.g., home, work, cell phone, email addresses, and home addresses). An entry may resemble the following format:

Systems Software Team
Team Leader—Primary
Jane Jones
1234 Any Street
Town, State, Zip Code
Home: (123) 456-7890
Work: (123) 567-8901
Cell: (123) 678-9012
Email: jones@uconn.edu; jones@home.ext

Notifications are also sent to Point of Contacts (POCs) of external organizations or interconnected system partners that may be adversely affected if they are unaware of the situation. Depending on the type of outage or disruption, the POC may have recovery

responsibilities. For each system interconnection with an external organization, a POC should be identified. These POCs are listed in an appendix to the plan.
The type of information to be relayed to those being notified is documented in the plan. The amount and detail of information relayed may depend on the specific team being notified. As necessary, notification information may include the following:

- Nature of the outage or disruption that has occurred or is impending;
- Any known outage estimates;
- Response and recovery details;
- Where and when to convene for briefing or further response instructions;
- Instructions to prepare for relocation for estimated time period (if applicable); and
- Instructions to complete notifications using the call tree (if applicable).

Outage Assessment

To determine how the ISCP is implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption. The outage assessment is completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. When possible, the Outage Assessment Team is the first team notified of the disruption. Outage assessment procedures may be unique for the particular system, but the following minimum areas should be addressed:

- Cause of the outage or disruption;
- Potential for additional disruptions or damage;
- Status of physical infrastructure (e.g., structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation and air-conditioning [HVAC]);
- Inventory and functional status of system equipment (e.g., fully functional, partially functional, nonfunctional);
- Type of damage to system equipment or data (e.g., water, fire and heat, physical impact, electrical surge);
- Items to be replaced (e.g., hardware, software, firmware, supporting materials); and
- Estimated time to restore normal services.

Personnel with outage assessment responsibilities should understand and be able to perform these procedures in the event the plan is inaccessible during the situation. Once impact to the system is determined, the appropriate teams are notified of updated information and the planned response to the situation. Based upon the results of the outage assessment, ISCP notifications may be revisited and expanded using the procedures described in the previous section.

Recovery Phase

Sequence of Recovery Activities

When recovering a complex system, such as a wide area network (WAN) or virtual local area network (VLAN) involving multiple independent components, recovery procedures reflect system priorities identified in the Business Impact Analysis (BIA). The sequence of activities reflects the system's Maximum Tolerable Downtime (MTD) to avoid significant impacts to related systems and applications. Procedures are written in a stepwise, sequential format so system components may be restored in a logical manner. For example, if a LAN is being recovered after a disruption, then the most critical servers are recovered before other, less critical devices, such as printers. Similarly, to recover an application server, procedures first address operating system restoration and verification before the application and its data are recovered. The procedures also include escalation steps and instructions to coordinate with other teams where relevant when certain situations occur, such as:

- An action is not completed within the expected time frame;
- A key step has been completed;
- Item(s) must be procured; and
- Other system-specific concerns exist.

If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred or procured. These items may include shipment of data backup media from offsite storage, hardware, copies of the recovery plan, and software programs. Procedures designate the appropriate team or team members to coordinate shipment of equipment, data, and vital records. References to applicable appendices, such as equipment lists or vendor contact information, are made in the plan where necessary. Procedures clearly describe requirements to package, transport, and purchase materials required to recover the system.

Recovery Procedures

To facilitate Recovery Phase operations, the ISCP provides detailed procedures to restore the information system or components to a known state. Given the extensive variety of system types, configurations, and applications, this planning guide does not provide specific recovery procedures.

Procedures are assigned to the appropriate recovery team and typically address the following actions:

- Obtaining authorization to access damaged facilities and/or geographic area;
- Notifying internal and external business partners associated with the system;
- Obtaining necessary office supplies and work space;

- Obtaining and installing necessary hardware components;
- Obtaining and loading backup media;
- Restoring critical operating system and application software;
- Restoring system data to a known state;
- Testing system functionality including security controls;
- Connecting system to network or other external systems; and
- Operating alternate equipment successfully.

Recovery procedures are written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps are assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures and for troubleshooting problems if the system cannot be recovered properly. Figure 3 provides a partial example of a procedural checklist for a LAN Recovery Team.

SAMPLE Recovery Process for the LAN Recovery Team:
These procedures are used for recovering a file from backup tapes. The LAN Recovery Team is responsible for reloading all critical files necessary to continue production.

Step	Description	Check when Complete
1	Identify file and date from which file is to be recovered.	✓
2	Identify tape number using tape logbook.	
3	If tape is not in tape library, request tape from recovery facility; fill out with appropriate authorizing signature.	
4	When tape is received, log date and time.	
5	Place tape into drive and begin recovery process.	
6	When file is recovered, notify LAN Recovery Team Leader.	

Figure 3: Sample Recovery Process

Recovery Escalation and Notification

As identified as part of the BIA, system components, infrastructure, and associated facilities are critical components supporting daily mission/business functions. The systems, applications, and infrastructure that connect users to these are subject to events causing service interruptions and outages. Including an escalation and notification component within the Recovery Phase helps to ensure that overall, a repeatable, structured, consistent, and measurable recovery process is followed.

Effective escalation and notification procedures define and describe the events, thresholds, or other types of triggers that are necessary for additional action. Actions include additional notifications for more recovery staff, messages and status updates to leadership, and notices for additional resources. Procedures are included to establish a clear set of events, actions and results, and are documented for teams or individuals as appropriate.

Reconstitution Phase

The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities:

- Validating successful recovery and;
- Deactivation of the plan.

Validation of recovery typically includes these steps:

- **Concurrent Processing**.[4] Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

- **Validation Data Testing**. Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.

- **Validation Functionality Testing**. Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

At the successful completion of the validation testing, ISCP personnel are prepared to declare that reconstitution efforts are complete and that the system is operating normally. This declaration is made in a recovery/reconstitution log or other documentation of reconstitution activities. The ISCP Coordinator, in coordination with the Information System Owner, Information System Security Officer(s) (ISSO), Chief Information Security Officer (CISO) and with the concurrence of the Authorizing Official, determines if the system has undergone significant change and will require reassessment and reauthorization[5] by the Change Advisory Board (CAB). The utilization of a continuous monitoring strategy/program can guide the scope of the reauthorization to focus on those environment/facility controls and any other security controls that are impacted by the reconstitution efforts.

Deactivation of the plan is the process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption. These activities include:

[4] Information systems are not required to have concurrent processing capabilities.

[5] Examples of significant changes that would possibly apply in a contingency situation are: 1) new or upgraded hardware platform, and 2) moving to a new facility.

- **Notifications**. Upon return to normal operations, users are notified by the ISCP Coordinator (or designee) using predefined notification procedures.

- **Cleanup**. Cleanup is the process of cleaning up workspace or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.

- **Offsite Data Storage**.[6] If offsite data storage is used, procedures are documented for returning retrieved backup or installation media to its offsite data storage location.

- **Data Backup**. As soon as reasonable following reconstitution, the system is fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.

- **Event Documentation**. All recovery and reconstitution events are well documented, including actions taken and problems encountered during the recovery and reconstitution efforts. An after-action report with lessons learned is documented and included for updating the ISCP.

Once all activities and steps are completed and documentation is updated, the ISCP can be formally deactivated. An announcement with the declaration is sent to all business and technical contacts.

Plan Appendices

Contingency plan appendices provide key details not contained in the main body of the plan. Common contingency plan appendices include the following:

- Contact information for contingency planning team personnel;
- Vendor contact information, including offsite storage and alternate site POCs;
- BIA;
- Detailed recovery procedures and checklists;
- Detailed validation testing procedures and checklists;
- Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details should be provided for each entry, including model or version number, specifications, and quantity;

[6] According to UITS Contingency Plan security controls, a low-impact system is not required to have offsite data storage capabilities.

- Alternate mission/business processing procedures that may occur while recovery efforts are being done to the system;
- ISCP testing and maintenance procedures;
- System interconnections (systems that directly interconnect or exchange information); and
- Vendor Service Level Agreements (SLAs), reciprocal agreements with other organizations, and other vital records.

Appendix A—Personnel Considerations in Contingency Planning

Information system contingency plans are rarely developed or executed on their own. When an incident occurs that impacts information system operations, it often impacts an organization's personnel. Proper considerations for the safety, security, and well being of personnel are planned for in anticipation of a disruptive event. Evacuation procedures and regaining access to the facility is coordinated and jointly exercised with UConn's Department of Public Safety and local response organizations.

Planning for these factors typically falls within the scope of an occupant emergency plan (OEP), business continuity plan (BCP), or crisis communications plan (CCP), which are all plans coordinated with the ISCP. In light of heightened awareness of these issues due to the terrorist attacks in 2001, the aftermath of Hurricane Katrina in 2005, the threat of pandemic influenza, and general increased security throughout our society, "personnel considerations" warrant further discussion in all related planning areas.

Personnel Safety and Evacuation

Personnel safety and evacuation during and after a disruption are typically addressed in an Occupant Emergency Plan (OEP). Personnel should be aware of their physical security and exit procedures and should practice these procedures during regular fire drill exercises. OEPs and information system contingency plans may include instructions for securing office spaces, personal workstations, and laptop computers to prevent access to information and to reduce the likelihood of vandalism or theft. Plans may also include reminders to collect identification, car keys, and other important belongings if the nature of the incident and time allows. In addition, procedures may need to address how to regain access. Instructions for the most appropriate ways to exit the facility are based on specific site requirements and local fire code regulations.

The OEP includes procedures and multiple contact methods for collecting a personnel head count after a disaster. It is important for senior management to know who was in the building prior to the event and who has been accounted for (both onsite and offsite personnel) so that the Department of Public Safety, civil authorities (fire, police, and rescue), and families can be properly informed of the situation. Procedures should be developed to instruct personnel to meet and be accounted for at a specific preplanned site, away from the building. Personnel should be provided alternate procedures to contact the organization and provide information on their whereabouts in the event the preplanned location is not safe. A centralized reporting methodology to one person or to a team will reduce possible confusion and conflicting information.

While the OEP provides guidance on facility evacuation, it may be safer to remain within the facility in response to certain emergency situations. Shelter-in-place plans provide instruction to personnel on how to take refuge indoors in response to unsafe environment outside of the facility or contaminations inside the facility that could be carried outside and spread.

Personnel Welfare

During a serious situation, addressing personnel and family matters often takes priority over resuming business. Planning for such matters may involve pre-identification of temporary housing, workspace, and staffing. In some situations, the organization may need to use personnel from associated organizations or contract with vendors or consultants if both primary and alternate team members are unavailable or unable to fulfill responsibilities. Preparations should be made during contingency planning development for this possibility to ensure that the vendors or consultants can achieve the same access as the team members could in the event of a disaster.

Once personnel are ready to return to work, arrangements should be made for them to work at an alternate site or at home if the facility is unsafe or unavailable for use. This is an alternate space *in addition to* the alternate site for information system recovery. Personnel with home computers or laptops should be given instruction, if appropriate, on how to access the organization's network from home. It may also be necessary to assist personnel with procuring temporary housing. Planning for long-term relocations, such as those that took place in response to Hurricane Katrina, should consider locating the alternate site near areas with available housing in safe neighborhoods with schools and other family necessities.

Disasters may take a heavy psychological toll on personnel, especially if there has been loss of life or extensive physical destruction. Organizations should be prepared to provide grief counseling and other mental health support. Nonprofit organizations, such as the American Red Cross, also provide referrals for counseling services as well as food, clothing, and other assistance programs. Personnel will be most interested in the status of the health benefits and resumption of payroll. It is very important that the organization communicate this status. *Every effort should be made to continue to pay personnel as per normal operations*. Due to grief and stress, productivity may also be low during the adjustment period.

Communication Planning

The crisis communication plan (CCP) typically addresses internal communication flows to personnel and management and external communication with the University. The most effective way to provide helpful information and to reduce rumors is to communicate clearly and often. The plan prepares the organization for the possibility that during a significant disaster, the organization may be a communication-forwarding point between personnel, civil and federal authorities, and affected families and friends.
One of the most important activities is internal communication within the organization. Staff and management need to know what has occurred, the status of the situation, what actions they should take, and who is in charge of the situation. One person or team should

be responsible for internal communication. This person should have access to the organization's senior leadership. In addition, the organization should be prepared to use multiple communication methods such as voicemail, email, flyers, Web site announcements, or social networking. Clear and frequent communications from senior executives to all faculty and staff, interconnected POCs, students and their families is necessary after a disruption to assist calming internal anxiousness, worry, and answering general questions.

Declaring Personnel as Essential

In the event of a disaster, it may be necessary to declare certain personnel as essential for the duration of the event. During an emergency, Essential Personnel provide services that relate directly to the health, safety, and welfare of the University, ensure continuity of key operations, and maintain and protect University properties.

Essential Personnel are generally defined as the IT staff who are required to report to their designated work location, to ensure the operation of essential IT functions or departments during an emergency or when the University has suspended operations. There are some individuals who may be required to perform essential services remotely and those individuals are identified in advance and notified by their supervisors, but in most cases Essential Personnel are expected to be on-site. Ultimately, the nature of the emergency determines what services should continue and who is essential to the continued operation of the IT organization.

When declaring personnel as essential, it is important to consider the staff's personal safety and welfare.