Disaster Recovery Plan

Date:

Revision: 8.0

Federal regulation states, and internal corporate policies require, that Penson Financial Services, Inc. (Penson) develop Business Continuity Planning and Disaster Recovery Programs. These programs must be continually reviewed and updated. While developing and maintaining these plans, the Disaster Recovery Planning Team must consider the organizational, managerial and technical environments in which the disaster recovery plans will be implemented, assess the types and likely parameters of disasters most likely to occur, and their resultant impacts on the Company's ability to perform its critical business processes; compile a list of protective measures to be implemented in anticipation of natural or man-made business interruptions.

In terms of personnel and financial resources, the tasks and procedures detailed in this Plan represent Penson management's commitment to response, resumption, recovery and restoration planning. Therefore, it is essential that this Plan remain both viable and current in order to ensure the accuracy of its contents.

Executive management has recognized the potential financial and operational losses associated with service interruptions and the importance of maintaining viable emergency response, resumption, recovery and restoration strategies.

The Disaster Recovery Plan is intended to provide a framework for reconstructing vital operations to ensure the safety of employees and the resumption of *time-sensitive operations and services* in the event of an emergency. At the same time, it is intended to be a guide and not a series of defined instructions void of flexibility. The nature of the interruption should determine how a business continuation plan is used.

Although the Penson Disaster Recovery Plan provides guidance and documentation upon which to base emergency response, resumption and recovery planning efforts, it is not intended to be a substitute for informed decision-making. Directors, managers and executives must identify services for which disruption will result in significant financial and/or operational losses.

Constructing a plan and presenting it to executive management may satisfy the immediate need for having a documented plan; however, this is not sufficient if the goal is to have viable response, resumption, recovery, and restoration capabilities. In order to establish that capability, plans and the activities associated with their maintenance, including training revisions and exercises, must become an integral part of the planning process.

Developing a Disaster Recovery Plan that encompasses activities required to maintain a viable continuity capability ensures that a consistent planning methodology is applied including:

- Implementing accurate and continuous vital records, data backup, and off-site storage
- Implementing capabilities for rapid transferral of voice and data communication circuits to alternative sites
- Providing necessary communications systems to Penson's critical recovery teams
- Developing strategies for providing alternative sites for business operations.
- Constructing a contingency organization.

It is the responsibility of the Disaster Recovery Department and its committees to develop and maintain individual business continuity plans in concert with that of the individual department Directors and Managers. To insure the plan is accessible after hours to the individual department managers and directors, it is strongly recommended that a copy of each disaster recovery plan be maintained offsite and available in the event of a business disruption or a planned exercise. Copies of individual department plans are available through Penson's secure extranet server as well.

Penson maintains its vital records in both hard copy and electronic format. In the event of an internal business disruption requiring use of Penson's alternative recovery facility, the electronic records as well as those paper documents stored off-site will support recovery.

Penson maintain its primary business records at its home facility, 1700 Pacific Avenue, Dallas, Texas, 75201. It is Penson's corporate mandate to have systems in place by which all vital records and transactions will be totally replicated at the time the transactions are initially captured. Because of that corporate mandate, copies of the transactions are available at both its home facility and its disaster recovery data center.

Purpose Scope and Fundamentals of Plan Process

Purpose

The purpose of this Disaster Recovery Plan is to enable the sustained execution of mission critical application processes for Penson in the event of an extraordinary event that causes these systems to fail minimum production standards. The Penson Disaster Recovery Plan assesses those needs and requirements so that the department may be prepared to respond to an event and efficiently regain operation of the mission critical business processes that are made inoperable from the event.

Scope

The Penson Disaster Recovery Plan addresses the recovery requirements for the all departments. The Plan does not provide for recovery strategies outside of this department and business unit.

Fundamentals of a Disaster Recovery Planning Process

The fundamental basis of Disaster Recovery Planning is to develop a methodology beginning with project planning and loss avoidance and following through to ongoing testing and maintenance. Below are graphics that describe some rudimentary steps to develop Penson's fundamental Disaster Recovery Plans:

Fundamental 1 - Preparing for the Planning Process

A. Executive Management Meets to define Objectives and Goals of a Disaster Recovery Plan
B. Senior Management appoints Disaster Recovery Specialist
C. Prepare Business/Process Effort Chart & Project Plan
D. Executive Management communicates to all Directors and Managers of upcoming Disaster Recovery Planning Program
E. Receive Department Head Commitment to Goals of Disaster Recovery Planning

Fundamental 2 - Preparing Departments for Planning

A. Department Directors and Managers appointment Subject Matter Experts
B. Disaster Recovery Specialist meets with Department Directors and Managers to Discuss Objectives

Fundamental 3 - Risk Assessment

A. Disaster Mitigation (Risk Avoidance)
B. Insurance Evaluation (Risk Transfer)
C. Security Assessment (Risk Reduction)

Fundamental 4 - Business Impact Analysis

A. Subject Matter Experts, the Disaster Recovery Specialist and Department Directors and Managers Identify Critical Business Processes with the use of Business Impact Analysis tools
B. Subject Matter Experts, the Disaster Recovery Specialist and Department Directors and Managers define Interdependencies (Inputs and Outputs)
C. Executives Prioritize Recovery Objectives – Recovery Time Objectives

Fundamental 5 - Prioritize Critical Business Process

A. Create "Score Card" of Critical Business Processes
B. Department Manager prioritizes all Critical Business Processes in their view of what is necessary to recover basic services or processes
C. The Disaster Recovery Technical Committee evaluates the strategy applied by the Department Directors and Managers
D. Department Manager makes presentation on Critical Business Processes and their priority to Executive Management along with resource requirements and interdependences with other departments
E. The Disaster Recovery Technical Committee identifies minimum workstation requirements

Fundamental 6 - Develop Recovery Strategy

A. Critical Business Processes are submitted for review to their Executives and their priority are reviewed Each Critical Business Process is either approved, rejected, modified or reprioritized
B. Executives meet and prioritize company wide Critical Business Processes
C. Upon approval of company wide recovery strategy, Department Directors and Managers are informed of the priorities
D. Disaster Recovery Specialist identifies Critical Business Partners, Vendors, and develops a budget.
E. The Disaster Recovery Specialist and the Department Directors and Managers review Critical Business Partners, Vendors, and the budget.
F. Executives, Department Directors and Managers reviews the information supplied, including the budget.
G. Executives meet to determine minimal recovery requirements that can be met or priorities change. Can the company afford to recover each Critical Business Process identified? Does the sequence of recovery change the cost of recovery? The Disaster Recovery Specialist and the Department Directors and Managers should be available for their input.
H. The Disaster Recovery Specialist and the Department Directors and Managers may need to refine their Disaster Recovery Plan Strategy.

Fundamental 7 - Plan Development

A. Develop Disaster Recovery Plan Format
B. Identify Teams and Team Members
C. Identify vendors and other contacts
D. Collect data for Disaster Recovery Plan
E. Prepare draft of Disaster Recovery Plan
F. Submit draft for approval to Department Directors and Managers
G. Prepare final copy of Disaster Recovery Plans & obtain Sign-Off from Senior and Executive Management
H. Obtain Involvement and assistance for implementation from Vendors and Suppliers as needed

Fundamental 8 - Test and Maintain Plan

A. The Disaster Recovery Specialist develops and communicates Disaster Recovery Plan maintenance schedule for business units testing
B. The Disaster Recovery Specialist develops and communicates Testing Formats
C. Test and maintenance schedules are posted and followed
D. The Disaster Recovery Specialist executes and update testing formats
E. The Disaster Recovery Specialist, Subject Matter Experts and Department Heads update Disaster Recovery Plans as required.

Summary of Disaster Recovery Plan

This document contains the summary of the Disaster Recovery Plan for Penson Financial Services, Inc. It is intended to serve as the centralized repository for the tasks that would be necessary to facilitate the Penson decision-making process and its timely response to any disruptive or extended interruption of the department's normal business operations. This is especially important if the cause of the interruption is such that a prompt resumption of operations cannot be accomplished by employing normal daily operating procedures.

Immediate Reaction:

Evacuation of the Facility during Business Hours:
- Pack critical data at the sound of the alarm
- Gather all work in process and all unprocessed work and place it in the Evacuation Bag
- Penson Fire Marshals will assist in evacuation using the stairwells
- The department should have a list of those employees who are disabled, experience medical problems or who are pregnant.
- Gather at a Pre-Determined location
- Department head counts *must* be taken to ensure all employees have been accounted for
- If there is staff missing, notify the Penson Fire Marshals and they will notify emergency services
- Everyone must remain in this location until called upon for disaster relief or released to return home. The Business Unit Managers must insist that everyone released return directly to their home in the event their services will be needed later.

Crisis Management Team Mobilized:

The Crisis Management Team has total control over all business recovery efforts during a disruption. They will approve all expenditures related to the recovery of the damaged facility as well as authorizing expenses related to recovery. They will also approve changes in day-to-day activities, priority scheduling of resources and acquisition of services and hardware. They will be the only part of the organization that will have the authority to execute a Declaration of Disaster. All departmental/business unit requests must be channeled through the Crisis Management Team.

Crisis Management Team will work from a temporary local facility, such as an office building conference room or hotel meeting room, close to the damaged facility as an Emergency Command Center to manage recovery efforts. The Disaster Recovery Specialist will remain at the damaged facility. (Examples where office space may be available includes the Republic Tower or the Sheraton Hotel)

Advise the Recovery Center to 'Stand By' for Possible Declaration of Disaster:

- Puts them on notice that a potential, formal declaration may be made
- This is the responsibility of the Disaster Recovery Specialist

Logistical Support Team Mobilized:

When contacted by the Crisis Management Team, the Logistical Support Team will also provide acquisition and administrative support to all teams; they will arrange for supplies and other non-technical resources necessary for recovery. This would include, but not be limited to, arrangements for temporary staffing, training, mass transportation and vehicles, food, day/night care, and flight and hotel accommodations

Damage Assessment Team Mobilized:

The Damage Assessment Team will consist of members of the Enterprise Support Group of MIS; they evaluate the conditions of the interior facility, servers, workstations, files and peripherals. Use the cameras in the Evacuation Bag to gather most of your data if possible. Make notations on the Damage Assessment Form.
- The Disaster Recovery Specialist will contact the leaders of the Damage Assessment Team.
- The Damage Assessment Team will support evaluation of the damaged facility.
    - *If after hours, they may need to have volunteers to contact if sufficient number of the recovery team is not available.*
- Advise them to report to the damaged facility.

This is the initial evaluation stage. As the equipment is evaluated and no damage is immediately found, place a white sticker on it; if minor damage such as dents or scratches, but appears to be functional, place a green sticker; and if heavily damaged, place a red sticker. Have the Disaster Recovery Specialist advise all team members regarding the placement of the stickers to accelerate salvage operations.

Technical Recovery Team Mobilized:

The Technical Recovery Team will be responsible for data, voice and network connectivity for the Emergency Command Center and the business recovery facilities. The team will consist of representatives from Sec Conn in addition to Enterprise Support. The Technical Recovery Team will be activated by the Disaster Recovery Specialist. This team will assist in establishing connectivity of the business recovery site with the data center and service bureaus. The team will assist in supporting Damage Assessment and establishing Business Recovery the Site

Begin Damage Assessment:

If the police, the local fire department or a public utility releases the building for temporary re-entry, Damage Assessment Team may be authorized to re-enter the facility. Emergency services will not release the facility for re-entry unless it is safe to do so.
- The Damage Assessment Team Leader will see that power is turned off to the facility.
    - Receive formal notification from the local fire marshal of power shut off. **Do not,** under any circumstances, enter the facility until this is verified.
- The team will reenter the facility and document with photos and on paper the extent of damage to computer hardware, vital records and facility
- Assess for any potential of further damage and deteriorations
    - Do not attempt to identify source of disaster or financial loss. That is the job of the Insurance Adjusters. They will use the documentation that is collected from damage assessment.
- Damage Assessment Forms, clipboard, markers, labels, disposable cameras and flashlights will be in the Evacuation Bag
- Essential documentation is important to determine hardware that may be reclaimed for purposes of recovery capability and reporting insurance claims
- Undamaged equipment will be salvaged and available for use at the recovery center, if needed
- There is generally a limitation to the amount of time to enter the facility initially. You may need an escort by emergency services personnel.
- Assess the Level(s) of physical disruption. Keep in mind, different floors and different parts of the building may have different levels of disruption
- Assess health and safety related risks within the damaged facility
- A combined inventory of usable equipment will be compiled following the assessment

Assess the Condition of Vital Records:

Vital Records files should have large fluorescent tags on the cabinets so they can be easily identified.
- It is the responsibility of the Business Unit Managers and their immediate subordinates to ensure vital records are protected.

Establish the Emergency Command Center:

The Logistical Support Team and the Technical Recovery Team will prepare the site. The Logistical Support Team will publish a list of those authorized accesses to the Emergency Command Center and update as required. No one not included on the list and without a picture I.D. will be authorized to enter the facility. Security will post a guard outside the facility 24 hours a day, 7 days a week.

The Crisis Management Team and the Logistical Support Team will occupy the Emergency Command Center.

Business Unit Team Leaders and Alternates will be instructed to Standby:

The Crisis Management Team advises the Business Unit Team Managers and/or Directors of the disruption. Instruct them to stand by for additional details following the damage assessment and for a decision to either move to the business recovery site or recover in the damaged facility.
- Business units will initiate recovery following their own plans and their recovery strategy

Update Telephone Message Listed on Penson Website:

- This is the responsibility of the Marketing Manager or other designate on the Crisis Management Team at www.penson.com.
- Do not provide confidential information or the status of the damaged facility; keep in mind this is a public telephone number
- Update the information every 2 hours; reference date and time in the message

Decision to Declare or Stand Down:

The Crisis Management Team will obtain reports from the Damage Assessment Team, the local fire and police department, public utilities and evaluate the information to determine if primary data processing operations will be supported from the data center or the business recovery site.

Decision to Stand Down:

If the decision is not to declare, members of the Crisis Management Team will notify team leaders of the various teams of their decision.
- Teams will stand down and await for a Recovery Time Objective
- Business Recovery Site will be advised by the Disaster Recovery Specialist the 'Standby' is rescinded
  - This will occur immediately or within 4 hours, depending on damage to the   facility

Decision to Declare:

The ranking member of the Crisis Management Team will notify the business recovery site it is exercising its right of Disaster Declaration.
  - Internal legal council should be part of the Crisis Management Team. If the business declines the Declaration for whatever reason, legal council must become involved immediately and begin discussing an alternative recovery strategy and location.
- Advise the Business Unit Managers of the decision to relocate to the business recovery site. For security purposes, do not publish the location of the business recovery site.
- Advise the Business Unit Managers they will be contacted when at the appropriate time for their recovery.
- There will be high priority work that must be completed in order to satisfy the recovery objectives; lower priority tasks can be done during the evening or brought on-line later based on the equipment available and the R.T.O.

Forward Recovery Team Mobilized:

The team is responsible for seeing that the business unit applications are effectively supported with both data and communications
- Consist of members of Enterprise Team and Database Team
- Will be notified by the Crisis Management Team
- Team members will be assigned to work with business units

Coordinate Orientation Meeting with Team Leaders/Alternates:

This is the meeting the Crisis Management Team will have with the Recovery Team Leaders and Alternates
- Define Strategy for Recovery based on the current information available
  - Modify with follow-up meetings as situation changes or more is learned
- Determine time for teams to report to the business recovery site based on their RTO and workstion assignments
- Advise teams to have only skeleton team to report pending Stage 3 recovery

Evaluate the Adequacy of Inventory of Hardware in the D/R Data Recovery Site:

Determine if resources current resources will support Recovery Time Objective. If necessary, obtain approval to order additional hardware to support recovery

Evaluate the Need for additional Hardware for the Business Recovery Site:

- Determine if there is a sufficient number of PCs and peripherals
- If necessary, obtain approval to order additional hardware to support recovery from the Crisis Management Team

Initiate Telephone Calling Tree:

Team Leaders and Alternates will begin calling members. The list of those members are available in their plans or electronically on the Penson extranet web site.
- The Team Leaders and Alternates should advise team members of declaration of disaster.
- Advise members to report to the business recovery site
- If they need transportation, advise them to report to the front door of the damaged facility. Logistical Support team will make arrangement to provide bus transportation
- Team members should mobilize their teams consistent with their Recovery Time Objective
- Advise Alternates members to stand by for instructions regarding a time to report to the Business Recovery Centers

Establish Functional Business Recovery Site:

- Responsible for establishing the Business Recovery Site:
  - Technical Support Team
  - Forward Recovery Team
  - Logistical Support Team
- The Technical Support Team is responsible for insuring the business units have voice and data connectivity to the disaster recovery data center.
- The Forward Recovery Team is responsible for systems integrety
- Logistical Support Team is responsible for obtaining all supplies needed by the recovery sites

Notify Restoration Companies:

- Disaster Recovery Specialist to coordinate this operation
- Coordinate restoration with corporate building security and property management.
- Advise the restoration companies of the nature of the disruption, the number of floors involved
  - This will assist them in determining the amount and type of equipment to required as well as the size of the staff necessary for restoration

Contact Moving and Storage Companies:

- To assist in Salvage and Restoration Operations
- Advise them to stand by until approval is given to enter the facility by emergency services, corporate building security and property management.

Begin Coordinating of Restoration Operations:

Immediately following the decision to execute the plan to move to business and data recovery sites, a plan for the restoration of the home site or an interim site should begin
- Form a committee headed by a senior or executive officer to evaluate the condition of the damaged facility
- Determine if the facility can be restored within two to four weeks
- Establish a list of alternate facilities that could be converted to a full temporary facility

Notify Regulators of Business Disruption:

The Crisis Management Team will assign a member of senior management to notify regulators of the disruption in business process.

Forward Telephone Calls to the appropriate Disaster Recovery Site:

- Only those advertised to customers or Penson frequently call numbers will be forwarded

Coordinate Communication with the Media:

The Marketing Manager, or a designate selected by the Crisis Management Team will coordinate all communications with the media.
- The Marketing Manager should remind all Recovery Team Leaders and Alternates not to discuss any business activities with the media or other third party organization.

Business Unit Teams Members Receive Details and Move to their Business Recovery Site:

Business Unit team leaders/alternates will advise team members of the current situation.
- Instruct them to notify their teams
- Identify location of Business Recovery Site.
- Logistical Support Team will provide maps to the business recovery site, however, they must come to the location where bus service is provided to obtain those instructions
- Advise them to refer to the established Penson Telephone Hotline, (214) 953-3500. The Crisis Management Team will arrange to update the Hotline information every two hours even if nothing has changed.

Do Not, under any circumstances, attempt to use the media to communicate recovery strategy or status.
- Not only is it a serious security breach, it also undermines the confidence of your customers, vendors, or stockholder. A company media representative should be responsible for the release of information related to disruption and recovery, whether oral or in writing.

Keep in mind, not all business units will be recovered immediately. Only those needed to implement the recovery operations within 4 to 8 hours should immediately report to their business recovery site following notification.

Initiate Recovery Strategy Plan:

The recovery strategy involves attaining the Recovery Time Objectives previously established, defining those applications that support the Critical Business Processes, and validating the sequence in which they will be recovered.
- The Recovery Teams will review the List of Critical Business Processes as defined in current version of the Applications Priority List
- The Business Recovery Teams will work with the Forward Recovery Team to prepare applications for recovery
- Assign Individual Critical Business Processes to recovery team members members as required
- Contact Business Unit Team Leaders as required

Define Applications needed to recover Each Critical Business Process:

- Compare List to those Critical Business Processes
- Coordinate the need for Business Applications with the Forward Recovery Team, and the Technical Recovery Team

Communicate Requirements to Vendors and Service Bureaus:

- Teams determine what vendor assistance is required to support recovery response
- What support or service is required? (This will depend on the extent of the interruption)
- What expectations are there with regard to the timing for support or service and training requirements?
- How is the vendor to contact you?
- What impact in a disruption and processing procedures going to have on records backup procedures?
- Advise the vendor or service bureau that these are shared workstations; verify with them the hours of operation you will be working.

Vendors and service bureaus should not be given any more information than is necessary.

Communicate with Customers and/or Other Key Contacts:

- Notifiy them of business interruption
- Team Leaders and Alternates should determine what information is required to communicate for purposes of recovery
- What support or service is required? (This will depend on the extent of the interruption)
- What expectations are there with regard to the timing for support or service and training requirements?
- How are these organizations to contact you?
- What impact in a disruption on processing procedures going to have on records backup procedures?
- Advise the contact that these are shared workstations; verify with them the hours of operation you are working.

Other contacts, like vendors and service bureaus should not be given any more information than is necessary.

Restore Business Recovery Infrastructure at Recovery Site:

- Forward & Technical Recovery Teams will establish priority of business applications
- Restore the business recovery site infrastructure.
- Contact outside service suppliers needed to support recovery of infrastructure.
- Business unit team leaders and alternates should determine if staff is sufficient for recovery; if not go to the staff contact list in off-site storage box

Restore Workstation Applications and Data Files at Business Recovery Site:

- Restore OS and application systems software to workstations
- Restore "off-the-shelf" software on local workstations
- Restore access rights
- Employees will not have "assigned seats." They will work from available pooled workstations daily.
- Employees involved in recovery will have access to recovery site 24/7.
- Work with the Technical Recovery Team members in establishing connectivity to servers (network connectivity)
- Insure all team leaders/alternates invoved with recovery are aware of the Recovery Time Objectives as well as the Recovery Point Objective
- Problems associated with workstation recovery should be directed through a member of the Crisis Management Team

Determine Training and Staffing Needs:

The business unit teams will work through the Logistical Support Team to obtain training and temporary staff requirements.

Determine Operating Fund Requirements:

All requests for financial assistance should be expedited through the Crisis Management Team. The appropriate documentations and receipts are required to support the expenditure.

Report Recovery Status to the Crisis Management Team:

At least twice daily, the team leaders and alternates from every team should meet with the Crisis Management Team to discuss outstanding problems, resource requirements, and issues that prevent a full and timely recovery. The Disaster Recovery Specialist should document all issues and provide an update at the following meeting.

Verify Status of Processing Systems:

- The Technical Support Team and Forward Recovery Team will work with the Business Unit Recovery Teams to:
- Verify the availability and accuracy of the restored applications
- Determine the extent of the operational impacts on all "Critical" processing systems
- Determine processing system interruption and communicate to business unit team leaders
- Determine when "Critical" processing system(s) will be restored (RTO)
- Be mindful of the fact that there is a priority sequence of critical processes
- Support user testing of restored applications
- Insure Business Unit Recovery Teams are prepared to render assistance to support restoration of processing systems
- Escalate the problem solving efforts to the Crisis Management Team when priorities are in conflict or if the disruption cannot be resolved within the RTO

Verify Status of Network Capabilities:

- The Technical Support Team and Forward Recovery Team will communicate the status of the LANS and WANS to the Business Unit Recovery Team leaders/Alternates.
- Verify access to Internet and email services
- Support testing of restored applications
- Escalate the problem-solving efforts to the Crisis Management Team when priorities are in conflict or if the disruption cannot be resolved within the RTO

Verify Status of Telecommunications:

- The Technical Recovery Team will work with the Business Unit Recovery Teams to:
- Restore connectivity of voice communications
- Communicate realistic times for connectivity to the Crisis Management Team
- Call local and long distance carriers for support, if necessary
- Escalate the problem solving efforts to the Crisis Management Team when priorities are in conflict or if the disruption cannot be resolved within the RTO

Prepare to Begin Data Synchronization:

- Technical and Forward Recovery Team should meet with business unit team leaders to prepare for the next stage of recovery

Validate Connectivity & Accessibility for those using VPN & Citrix:

- Resolve if there is a problem
- Report Status to Crisis Management Team

Support Data Synchronization:

- Assist in synchronization of data necessary before beginning forward recovery process
- Do Not begin Forward Recovery if the first three stages of Functional Restoration Processes have not been completed and the impacts of that will negatively impede ongoing processing

Support Forward Recovery:

- Initiate procedures to ensure systems are ready and business units can begin to process incoming transactions
- Hardware and software should be in place to allow for generation of data, documents, printed media, and all other forms of output
- All teams should be available to participate in Forward Recovery

Evaluate Operational Status:

- Crisis Management Team must assess current operational capabilities and determine if additional resources are required. Include hardware, software and personnel.
- Business units should be advised to communicate requirements to the Crisis Management Team.

Support Facility Restoration:

- The Crisis Management Team should enlist members of the staff not participating in mission critical recovery efforts to assist in the following:
- Prepare full inventory of damaged facility
- Representatives from each business unit may be called upon to support some level of restoration of the damaged facility
- Evaluate equipment for damage (i.e., workstations, phones, printers and related hardware and software).
- Assign a member from the Crisis Management Team to work with claims adjusters and investigators to coordinate insurance claims
    - Use photos, original damage assessment forms and expenditures forms and invoices for documentation
- A member of the Crisis Management Team should begin this project on the day the unplanned event occurs
- Details will be provided by the Crisis Management Team and recovery of the facility will be coordinated by the Crisis Management Team

Support Salvage Operations of Damaged Facility:

- Coordinate salvage operations through building security and property management.
- The Crisis Management Team will assign a team member to oversee salvage and restoration procedures

Coordinate the Development of Crisis-to-Normal Transition Plan:

- Organize a Post-Interruption Review meeting with the department heads and directors
- Document lessons learned
- Prepare for senior management a Post-Interruption Review Report
- Update Disaster Recovery Plans