The University of Iowa

Enterprise Information Technology Disaster Plan

Revised September 2014, V4.0

The University of Iowa
Enterprise Information Technology Disaster Plan V4.0

TABLE OF CONTENTS

PART 1: DISASTER RECOVERY EXPECTATIONS 3

OVERVIEW 3
EXPECTATIONS – PRIOR TO AN INCIDENT OCCURRENCE 3
EXPECTATIONS – PRIOR TO A DISASTER OCCURRENCE 3

PART 2: DISASTER RECOVERY RESPONSIBILITIES 4

DECISION-MAKING PROCESS - DURING AN INCIDENT OR DISASTER 4
WHO DOES WHAT - DURING AN INCIDENT OR DISASTER 5

PART 3: COMMUNICATIONS PROCESSES 5

IT DISASTER COMMUNICATION PLAN 6
IT EMERGENCY COMMUNICATIONS 6
IT EMERGENCY COMMUNICATIONS FLOWCHART 7
UNIVERSITY-WIDE DISASTER EVENT 7
IT INCIDENT ESCALATION AND COMMUNICATIONS 7

PART 4: DISASTER PREVENTION 8

DISASTER PREVENTION MEASURES FOR CRITICAL APPLICATIONS/SYSTEMS 8

PART 5: UNIT DISASTER PLANNING 9

OVERVIEW 9
DISASTER RECOVERY FUNDAMENTALS: UNIT RESPONSIBILITIES 10

STEP 1: COLLECT GENERAL UNIT INFORMATION 10

Use the Action Items Tab to make notes of information that needs to be gathered. 10
Step 2: Identify Critical Functions 10
Step 3: Information Technology 11
Step 4: Key Resources – Personnel 12
Step 5: Key Resources – Non-Personnel 12
Step 6: Regularly review and update your unit plan 12

APPENDIX: REFERENCES 12

The University of Iowa
Enterprise Information Technology Disaster Plan V4.0

Part 1: Disaster Recovery Expectations

Overview

In the event of an IT service outage, it is important that central service units and collegiate/departmental units agree on their respective roles and responsibilities. A common understanding allows IT service owners to plan for a timely and orderly restoration of service.

For IT disaster planning, we distinguish between an *incident* and a *disaster*. Expectations vary between the two.

- An *incident* typically impacts a specific service, location, or server. Examples of incidents include a compromised service resulting from a hacking attack or the loss of a server due to an electrical problem or failure isolated to that server.
- A *disaster* event is a significant or unusual incident that has long-term implications. An example of a disaster event would be the loss of a data center due to a catastrophic fire.

In the context of this document, central facilities staff refers to Facilities Management (FM) and central IT staff refers to Information Technology Services (ITS). Major exceptions include any departments who currently receive such support from other service units (e.g., hospital, outlying buildings).

Each area has an obligation to the University to ensure it can continue to function, or restore function, at a basic level in the event of a disaster. University administration has expectations that each area will assume full responsibility for the following:

Expectations – Prior to an Incident Occurrence

Collegiate/Departmental units are expected to:
1. Have identified an alternate server in the case of the loss of a server.
2. Be able to perform a restoration from the ground up.
3. Restore service to operational status which is fully patched and compliant with IT policy.

Central facilities staff are expected to:
1. Assist with problem identification in the case of an electrical or HVAC failure.
2. Provide advice on environmental-monitoring and building security options.

Central IT staff are expected to:
1. Maintain a central web site for IT policies and best practices.
2. Assist with problem identification and provide general recommendations. Service-specific issues are beyond the scope of central IT support unless previously agreed upon via a Service Level Agreement or Memo of Understanding.
3. Provide central security services and network controls such as Security Software, Monitoring and Intrusion Detection, Vulnerability Assessments, and Incident Response.
4. Notify other work units if the incident could spread elsewhere.

Expectations – Prior to a Disaster Occurrence

Incident expectations are applicable to a disaster event, too. Given the scope of a disaster, there are additional expectations.

Collegiate/Departmental units are expected to have the following documented:

1. Services prioritized as to importance and order of restoration.
2. Officials who have the authority to declare a disaster in the unit.
3. Estimates for the number of days required for service restoration and documented alternative service plans for that length of time, as well as resources needed (people, equipment and sufficient funding) for timely restoration.
4. Identified multiple staff capable of restoring IT services.
5. Location and process for retrieving backup media from remote site(s).
6. Identification of a source for the quick acquisition of IT servers and workstations, including, if necessary, written or contractual agreements with outside entities.
7. Procedure for the annual review of the unit plan, including education of all staff to ensure they are aware of and understand the plan.

Central facilities staff are expected to:

1. Assist in finding alternate facilities with appropriate space, electrical, access control, and HVAC, for sustaining servers, workstations, and staff.
2. Provide advice on fire suppression, uninterruptible power supply (UPS), alternative power sources (e.g., motor generators, redundant electrical feeds), HVAC, and physical security.

Central IT staff are expected to:

1. Work with central facilities to have processes in place for identifying alternate spaces for servers and workstations that have sufficient network infrastructure and bandwidth.
2. Identify available sources for IT servers and workstations.
3. Identify available sources for IT staff with qualifications unique to Higher Ed.
4. Have central facility (data center, network infrastructure) disaster plans[1] in place.

Part 2: Disaster Recovery Responsibilities

Decision-Making Process - During an Incident or Disaster

Identification of a Threat

The decision-making process begins with identifying an impending, or existing, threat. This can occur in many ways, but basically involves awareness something will happen, or is happening, which could plausibly be defined as a “critical incident” by the University (see The University of Iowa Operations Manual, Part V, Chapter 16, Section 16.3). At this point, the threat is not yet classified as a disaster.

Notification of Authority

Immediately following identification is notification of the appropriate authorities of the threat. At the highest level, the University president or their designee (the VP of Student Services) is the appropriate authority. For campus-wide IT-related disasters, notification must be made to the University Chief Information Officer and/or the Chief Information Security Officer, or their designee. Below the VP level—that is, assuming the scope of an incident is determined to be contained wholly within a single department or unit—the authority is defined as the dean or department head, or their designee. It is assumed that a chain of communication exists within each college/department, from senior IT management up to its head, to facilitate the decision-making process.

Declaration of a Disaster Event
A threat is defined as a disaster only when the designated authority (see above) has declared that a disaster condition exists. This will likely include consultation with staff within the department who are directly involved with the affected areas/services, and includes consultation with the CIO or Chief Information Security Officer.

Determination of Response
Those persons who have predefined roles to carry out in the event of a disaster (see below), will then meet to determine the appropriate course of action, based on the area's predefined disaster plan, and proceed from there.

Who Does What - During an Incident or Disaster

Definition of Roles
Each area will have specific needs. However it is recommended that each campus unit, organization or department, identifies a primary and secondary contact, who will be expected to carry out the following basic roles for their unit after a disaster situation has been declared by the designated authority:

Coordination – coordinates activities and makes command decisions, as related to the disaster, within the scope of the area. This person is essentially in charge of the disaster recovery.

Restoration – works with IT staffs and/or outside vendors to restore computers, or other technical systems, to the functionality needed for the unit to operate its critical services. This person may coordinate efforts of other technical staff.

Communication – handles communication with departmental staff and outside entities.

In larger areas, these roles are typically represented by one or more existing positions on the organizational charts. However, smaller units may not have formally-defined positions. It is imperative that all departments have in place a plan that clearly identifies who will perform what role in the event of a disaster. At the same time, flexibility in this regard is important, as it cannot be predicted who will be present when a disaster does occur.

Part 3: Communications Processes

The University Operations manual, Part V, Chapter 16 describes the Critical Incident Management Plan[2] (CIMP) which outlines the communications processes which will be invoked should a university wide critical incident situation occur. It is important that each unit understand how communications at the top level of the university will operate should such an event occur. It is further recommended that units review and understand the CIMP in its entirety. Relevant to issues concerning information technology are the following excerpts:

Part IV: “With any crisis situation it is understood that a state of emergency may need to be declared. The *authority to declare a campus state of emergency rests with the University President* or designee; in most cases the Vice President for Student Services will be the designee if the President is unavailable.”

Part V: “In the event of an emergency or a disaster, the University of Iowa *Department of Public Safety has primary responsibility for immediate response*, and shall cooperate and coordinate with official emergency response authorities and University Administration, in accordance with established policies and procedures.”

Part XIII (Infrastructure Failure): “The first responders, *either FM or ITS, will determine whether a critical incident exists,* and will report that information to the appropriate department heads. In the event that a critical incident exists, the Director of Public Safety and/or the CIO will notify University Administration (President’s Cabinet). The Vice President for Student Services (or another VP) will convene the Critical Incident Management Team (CIMT).

IT Disaster Communication Plan

The IT Disaster Communication Plan is designed to provide an orderly flow of accurate, effective and timely information to the campus through colleges and departments during the onset of a crisis situation, or a situation of potential crisis affecting the University of Iowa campus telephone system, data network, and/or computer and information systems.

In the event of an information technology (IT) emergency, the Information Security and Policy Office has primary responsibility for immediate communication response, and shall cooperate and coordinate with official emergency response authorities and University Administration, in accordance with established policies and procedures (i.e., the CIMP).

IT Emergency Communications

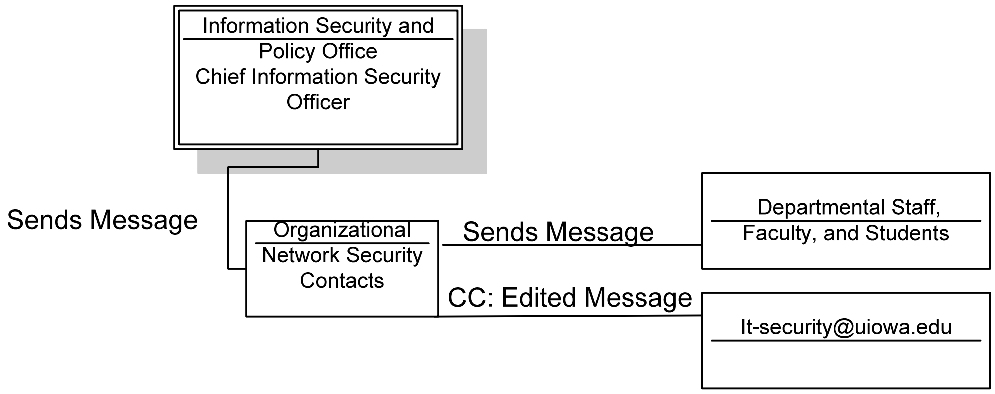
During a campus IT emergency, defined as a serious situation not (or perhaps not yet) having been declared a disaster, the following process will be invoked for communication in conjunction with campus response initiatives outlined in this document.

1. Each college or department has a primary and alternate Network Security Contact (NSC) for receiving messages and taking action.
2. All emergency IT messages will be sent via email, if available, to both the primary and alternate contact by the Chief Information Security Officer or designate.
3. The contacts will either be instructed to forward the message to their organizational users, or if necessary the CIO or CISO will send the message to campus. If contacts are instructed to forward the message, they will be allowed to make revisions, if it is deemed necessary that instructions be customized for their unit. Any customized messages must be carbon copied to the it-security@uiowa.edu mailbox.
4. Each emergency message from the Information Security and Policy Office (ISPO) will identify a “must forward by” time interval for the organizational contacts to send the message out to their users. If the CC: is not received by the ISPO by the time the interval has elapsed, central IT will send the message to that organization’s staff directly (without customization).

5. If central IT sends the message to the unit's staff (the exception, not the rule), the message will be a brief description of the problem, with basic instructions. The message will not include detailed instructions to take specific actions, as they may vary across units.
6. Student messages will be sent by central IT after the pre-identified time interval has elapsed. This will be a generic message that may direct people to a web page with specific instructions. This web page will contain a few sentences of "boiler plate" language that basically instructs students closely aligned with a certain college to work with the IT staff in that college on the issue.

This process is dependent on the campus email system working. In the event that e-mail is not available, the list of organizational representatives will be contacted using alternative methods, such as direct phone calls, SMS messages, or as a last resort, in person.

IT Emergency Communications Flowchart


Information Security and Policy Office
Chief Information Security Officer
Sends Message
Organizational Network Security Contacts
Sends Message
CC: Edited Message
Departmental Staff, Faculty, and Students
It-security@uiowa.edu

University-Wide Disaster Event

Most disaster events will not exclusively affect information technology resources. In the event of a physical disaster event for instance, the University's All Hazards Emergency Management Team will be invoked, and will take responsibility for a coordinated University, City, and County response, including all affected aspects such as power, water, structures, personnel safety, supplies, telecommunications, and information technology.

IT Incident Escalation and Communications

In the event of an attack on University IT resources, the IT Security Incident Escalation Policy[3] provides guidance in determining the proper response. It documents when to involve University administration, judicial representatives, and legal representatives. It also documents the individuals designated for these responsibilities, and procedural details, which depend on the severity and source of the problem.

The entity responsible for support of a system or network which is under attack, or which is experiencing a natural or technological problem, is expected to:

1. Report the problem to the Information Security and Policy Office (ISPO)
2. Under the direction of the ISPO, block or prevent escalation of the attack, if possible
3. Repair the resulting damage
4. Restore service to its former level, if possible
5. Preserve evidence, where appropriate

Part 4: Disaster Prevention

Disaster prevention is in a literal sense avoiding disaster, but in practice it's reducing the impact of problems by minimizing recovery time and effort, to keep an incident from escalating into a disaster event. A clear definition of "disaster" for individual units is important. The basic definition of a disaster focuses on physical events such as flood, fire, tornado, or a bomb. A broader and more appropriate definition of disaster includes some technical (information technology and infrastructure) problems and issues, where preventive controls can and should be considered. **The goal of preventive measures is to decrease recovery time, eventually to zero.** It's not economically feasible, in most instances, to apply enough controls to eliminate all technical disaster events, but it is desirable to reduce their probability and impact.

The purpose of every security control is to protect the availability, integrity, and/or the confidentiality of systems and information. For the purposes of this discussion, we will focus on preventive controls which contribute to the availability of systems and information. Further, if the intent is to prevent incidents from escalating to disaster events, two crucial goals are detecting problems as early as possible, and immediately notifying the persons capable of dealing with them. Automation of monitoring systems and notification processes is one of the best investments towards disaster prevention that can be made.

Disaster Prevention Measures for Critical Applications/Systems

1. Physical Protections
   a. Fire detection and suppression
   b. Backup power supply (uninterruptible power supply, generator)
   c. Heating, Ventilation, and Air Conditioning controls
   d. Secure doors and windows, and facility space
   e. Intruder alarm systems and/or motion sensors
   f. Staff who are trained on emergency procedures
   g. Surveillance cameras at ingress/egress points
2. Technical Redundancies
   a. Mirror data, and store additional backup copies of data off-site in a secure location
   b. Install systems in multiple physical locations, with separate power sources and network connectivity
   c. Purchase key equipment replacement items (spares), and consider reserving space at a secondary location for emergency installation of equipment
   d. Ensure that technical personnel are cross trained, to eliminate key person dependencies (i.e., situation where only one person knows how to recover a particular system)

   e. Identify alternate spaces for personnel to work, including workstation and telephone requirements. Consider emergency work-at-home arrangements, by supplying laptop/desktop, software, and other equipment for use at employee residences.
   f. Ensure key employees have cell phones.
3. Implement a monitoring and intrusion detection system to automate the review and/or testing of normal system functions, and which will generate alerts to technical support personnel in the event of a problem.
4. Perform periodic site and system security reviews to identify weaknesses in security controls as implemented.
5. Document and test both data and system/application backup and recovery procedures.
6. Ensure that at least one complete backup is available at a secure off-site location, and that local backup copies of data are maintained, and kept for a minimum of 30 days. Use incremental, differential, or full backups, depending on the volatility of the information and the recovery time constraints you need to operate within.
7. Set up a contingency communication plan that assumes normal electronic communications, including telephones, will not work. Plan for face to face communication at the local level, and plan for the possibility of inappropriate or inaccurate disaster information. Determine who will be the decision maker(s), and contingent decision maker(s).

Part 5: Unit Disaster Planning

Overview

Each unit must produce and maintain a Disaster Recovery Plan in order to be prepared to continue operating in the event of a severe IT disruption or disaster, and effectively respond to the interruption in services. This is achieved by invoking the plan to restore critical business functions. The focus of the plan is on those **resources and actions that are needed to restore services and necessary operations** in the event that they are unavailable for an extended time or entirely lost. While individual units may not be able to prevent all disaster events from occurring, prior planning will allow them to resume their critical operations in a minimum amount of time.

The Disaster Recovery Planning process consists of three main areas of activity:

1. Identify the elements or characteristics of conceivable IT problems that would cause severe disruption to critical or important unit operations.
2. Project the impact and effects that would likely result from these operational disruptions.
3. Develop and document contingent responses so that recovery from interruptions occurs as quickly as possible.

The result of the planning process will be a Unit Disaster Recovery Plan providing the following benefits:

- Establishes the criteria and severity of a disruption based on the impact it will have on the unit’s critical functions.
- Identifies what the critical functions and systems are, and the associated timeframes for recovery.
- Identifies the resources needed to support critical functions and systems, and defines the requirements for a recovery site.
- Identifies the people, skills, resources, and supplies necessary to assist in the recovery process.

- Identifies the unit's vital records, which must be backed up at an alternate/offsite location to support resumption of unit operation.
- Documents the appropriate procedures and information required for recovery.
- Provides for periodic review and updating of the plan to keep it current.
- Provides for testing of the documented procedures to ensure that they are complete and accurate.

There is no one best way to write a Disaster Recovery Plan. The following information is intended to help units create an IT Disaster Plan as easily and efficiently as possible. *Note: If the Unit currently has a Disaster Recovery Plan in place there is no need to recreate it, but the plan should be reviewed and compared to this guide to ensure the information is complete and current.*

There are two important things to remember:

> ***A crisis is *not* the time to deliberate decisions.***
> ***Communication is a *top* priority.***

Disaster Recovery Fundamentals: Unit Responsibilities

1. Complete a Business Impact Analysis to identify and prioritize critical functions in the unit, and the costs (impact) of failures.
2. Identify Resources, including people (and expertise), systems, supplies, and services needed.
3. Identify Vital Records maintained by your unit, if applicable.
4. Document the recovery procedures for all critical functions performed by your unit.
5. Plan for how communications will occur within your unit if normal channels are inoperable.
6. Establish chain of command for decision making in the event of a disaster.

These instructions assume use of a local tool for collecting information and organizing your DR/BC plan. See http://itsecurity.uiowa.edu/resources/drbcp.shtml

Step 1: Collect General Unit Information

Using the "Dept Info" tab in the spreadsheet, identify the following

- unit personnel (categories, estimated numbers)
- physical locations the unit personnel occupy
- references to other planning documents or resources (UI Pandemic Plan, Faculty Plan, etc)
- provide a link or insert a diagram with an organization chart

Use the Action Items Tab to make notes of information that needs to be gathered.

Step 2: Identify Critical Functions

List of functions *performed by your unit,* and an indication of each function's relative criticality.

- Critical 1: Essential, must continue at normal without interruption (i.e., life safety issues)
- Critical 2: Essential, serious consequences if disrupted, must continue at normal or reduced function
- Critical 3: May pause briefly, must resume within 30 days
- Deferrable: May pause if necessary, resume as soon as conditions permit

Consider important details for each critical function:

1. Peak periods for the function (start or end of semester, fiscal year, etc)
2. References to existing documents
3. Upstream Dependencies (Other units that you depend on for critical functions)
    a. HR, Registrar, ITS, FM , Purchasing, etc
4. Downstream Dependencies (Other units that depend on you for critical functions)
5. Consequences of failure or reduction in the critical function
6. Coping strategies

Use a separate tab for the details of each Critical Function. Use the Action Items tab to make notes of information that needs to be gathered.

Step 3: Information Technology

IT typically **supports** the unit’s critical functions, but is not the critical function itself. For example a web site is a communication vehicle, and a server may provide official document retention, or run an important application. Identify the applications, inventory, and procedures required to accomplish each critical function. Your IT planning goal is to lessen the impact on critical functions in the event of a disaster. Consider redundancy, recovery procedures, and alternatives.

Use the IT tab to document the following. Your priority should be those things necessary to support your unit’s critical functions, however it’s recommended that everything be collected.

- Enterprise applications that your unit utilizes
- Department applications
- Servers owned and managed by your unit
- Workstation inventory
- Backups – looking for adequacy not details

Consider the following questions and record your recovery strategies in the “IT Recovery” tab. Again, collect action items.

1. The remote access options available and how to use them
2. Establishing a new university location and what hardware and software would be needed
3. The minimum necessary support staff resources to restore critical functions to an operational state.

Recovery procedures should be documented, however they are NOT maintained within the DRBC planning tool. Rather references to them should be collected. Maintain and share relevant information such as vendor and supplier contact information, software licenses and where backup software keys are stored, personnel expertise needed, and specialized hardware that is required.

Step 4: Key Resources – Personnel

General things to consider before an emergency

Key Personnel – who has access/authority for critical functions and knows how to complete them
Web site notices, phone recordings, emergency contact list changes
Software, licenses, (vaulted) administrative passwords
Work from home arrangements (device, connectivity, etc)
Critical skills needed

Collect relevant information in the “Key Resources Personnel” tab.

Step 5: Key Resources – Non-Personnel

Where is the unit’s vital information kept, and in what format?
What equipment and supplies are necessary? (workstations, phones, printers, copier, scanner etc)
What facilities, utilities, and transportation are necessary?

Step 6: Regularly review and update your unit plan

- Review and test both on-site and off-site data backup and recovery procedures annually. Make updates as needed to ensure both of the procedures are accurate.
- Review and update manual operating procedures to ensure they are accurate.
- Review and test system level procedures for recovery and/or rebuilding applications. Opportunities arise when equipment is refreshed or updated, and software upgrades are installed.

Appendix: References

(1) IT Disaster Planning Tools
http://itsecurity.uiowa.edu/resources/system-administrators-and-it-managers/drbcp

(2) The University of Iowa Critical Incident Management Plan
http://www.uiowa.edu/cimp/index.html

(3) IT Security Incident Escalation Policy
http://itsecurity.uiowa.edu/it-security-incident-escalation

(4) Unit Planning Resources
http://itsecurity.uiowa.edu/resources/system-administrators-and-it-managers/drbcp