The University of Iowa
College of Education
Education Technology Center

Disaster Recovery Plan

Revised Spring 2017

1.0 Accessibility of the plan

This disaster prevention and recovery plan is accessible to all College of Education faculty and staff via a managed file server (L: drive) and is also uploaded to the Education Technology Center web site. Hard copy versions of the plan will be maintained at offsite locations (IT Director Home and Tech Staff homes) in case of a total disaster of all systems. The plan is purposely formatted in all text making it accessible to screen readers and other assistive technologies.

2.0 Purpose

2.1 Information technology policies and tactics

Dependence upon the use of computers and information technologies in the day-to-day business activities has become standard. Vital functions of the College of Education depend on the availability of these computers and networks. The focus of this plan is on resources and actions needed to restore services in the event that they become unexpectedly unavailable. This plan addresses guidelines and procedures guiding the Education Technology Center staff in the recovery of computing equipment, server assets and other critical IT operations in the event of a disaster destroying all or part of the College and its IT functions.

2.2 Broader Collegiate preventative and recovery issues and strategies

There are references to a Recovery Management Team in this plan. The Recovery Management Team includes the Director of Information Technology, Human Resources Director, Director of Finance and Budget, Director of Strategic Communications, and Executive Assistant to the Dean. Each member of the team oversees their respective areas of responsibility.

- Information technology
- Facilities
- Finance
- Human resources
- Communications

The IT Director is a member of the Recovery Management team and sets this plan governing information technologies into motion. The Recovery Management Team oversees processes, establishes timelines, prioritizes efforts, etc. for restoring operations and involvement in the other areas as well. Facilities, finance, human resources and public communications policies and approaches are addressed in a separate more expansive Collegiate-wide plan.

3.0 Maintaining the Plan

This plan has been approved by the College of Education Administrative Council and will be evaluated once a year by the College of Education Director of Information Technology
All aspects including compliance to preventative best practices, data restoration routines and directions leading to normal operations will be reviewed and assessed.

Changes that may affect the plan over time include:

- Hardware
  Additions, deletions, or upgrades to hardware affecting security and access.

Implementation of equipment inventories that can better assess damage and manage (re)allocation of available resources.

- Software
  Additions, deletions, or upgrades to system software affecting security and current assets management systems.
  Changes to application software affected by the plan.
- Facilities
  Changes that affect the availability/usability/location of necessities leading to normal operations.
- Procedural
  Changes to off-site backup procedures, relationships, locations, etc.
  Changes to vendor lists maintained for acquisition and support purposes.
- Personnel
  Changes to personnel identified by name in the plan.
  Changes to organizational structure within the College of Education or ITS.

The College of Education IT Director will determine if changes to the plan are necessary and take corrective action. See section 8.0 *Assessment* for details on testing and assessing recovery plans.

4.0 Disaster Risks and Prevention

Measures to prevent a disaster are addressed; proactive actions to mitigate various threats are addressed below. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created.

- Fire
- Flood
- Tornados and High Winds
- Earthquake
- Computer Crime
- Terrorist Actions and Sabotage

4.1 Fire

The threat of fire in any collegiate building, especially in data center and communication closet locations are very real. All collegiate buildings are filled with electrical devices and connections that could overheat or short out and cause a fire.

The computers within the facility also pose a quick target for arson from anyone wishing to disrupt collegiate operations. Wide area fires affecting one or more building are also a possibility.

<u>Preventive Measures</u>

Fire Alarms

All collegiate facilities are equipped with a fire alarm system, with ceiling-mounted smoke detectors scattered widely throughout the building.

Building Construction

The College of Education locations (Lindquist Center (LC), North Hall (NH), Van Allen (VH), Belin Honors Center (BHC) and Voxman (Vox)) are built primarily of non-combustible materials. The risk to fire can be reduced when new construction is done, or when office furnishings are purchased, to acquire flame resistant products. Personnel need to be instructed on evacuation procedures and area verification to ensure everyone gets out in a timely manner.

Recommendations

Regular review of the procedures should be conducted to insure that they are up to date. Unannounced drills should be conducted by an impartial administrator and a written evaluation should be produced for the department heads housed in the building.

Regular inspections of the fire prevention equipment are currently conducted by the Iowa City Fire Department and the University of Iowa Facilities Management.

4.2 Flood

Iowa City is split in half by the Iowa City River. A natural flood or a flood due to a water main break, sprinkler system malfunction, or roof leak is a strong concern. Flood waters penetrating the machine room can damage to electrical and mechanical systems. Not only could there be potential disruption of power caused by the water, flood waters can bring in mud and silt that can destroy sensitive electrical connections. The presence of water in a room with electrical equipment can pose a threat of electrical shock to personnel.

Preventive Measures

The Executive Assistant to the Dean is in direct contact with Education Technology Center on a continuing basis for any changes in infrastructure that may affect the college and its technological equipment and networks.

Recommendations

We rely on ITS to perform periodic inspections of its server room facilities to detect water seepage, especially any time there is a heavy downpour and other water related events.

4.3 Tornadoes and High Winds

As the University of Iowa is situated in “tornado country,” damage due to high winds or an actual tornado is a very real possibility. A tornado has the potential for causing the most destructive disaster we face.

Safe areas have been determined for evacuation purposes in the case of an event staff have been trained on evacuation procedures. In the event of building being damaged the hope is that people in the safe areas will be able to get out after the emergency event has passed.

Preventive Measures

While a fire can be as destructive as a tornado, there are very few preventative measures that we can take for tornados. Building construction makes a big difference in the ability of a

structure to withstand the forces of high winds. Strong winds are often accompanied by heavy rain, so a double threat of wind and water damage exists if the integrity of the roof is lost.

Recommendations

All occupants of collegiate buildings on campus should know where the strong points of the building are and directed to seek shelter in threatening weather. Most areas within the university are often unaware of outside weather conditions, so the ETC office should be equipped with a radio or other warning device. Staff within the college should also monitor weather warnings over the Internet and keep up-to-date of upcoming weather related issues (Hawk Alerts, Weather.com, KCRG, KGAN etc.).

4.4 Earthquake

The threat of an earthquake in the Iowa City area is low, but should not be ignored. Scientists have predicted that a large earthquake along the New Madrid fault may happen any time in the next 50 years, and that its effects will be felt as far away as our area. Buildings in our area are not built to earthquake resistant standards like they are in quake-prone areas like California. So we could expect light to moderate damage from the predicted quake.

Preventive Measures

The preventive measures for an earthquake can be similar to those of a tornado. Building construction makes all the difference in whether the facility will survive or not. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time. Standby power generators could be purchased or leased to provide power while commercial utilities are restored.

Recommendations

Information Technology Services which oversees College of Education virtual servers should have large tarps or plastic sheeting available in the server room area ready to cover sensitive electronic equipment in case the building is damaged. Protective covering should also be deployed over magnetic tape racks to prevent water and wind damage. Operators should be trained how to properly cover the equipment.

4.5 Computer Crime

Computer crime is becoming more of a threat as computer workstations become more highly distributed. With the new networking technologies, more potential for improper access is present than ever before.

Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within. A disgruntled employee can build viruses or time bombs into applications and systems code. A well-intentioned employee can make coding errors that affect data integrity (not considered a crime, of course, unless the employee deliberately sabotaged programs and data).

Preventive Measures

All systems should have security products installed to protect against unauthorized entry. All systems should be protected by passwords, especially those permitting updates to data. All users should be required to change their passwords on a regular basis. All security systems should log invalid attempts to access data, and security administrators should review these logs on a regular basis.

All users should maintain copies of important data files and research materials on managed network volumes. These protected and backed up shares have been setup for any faculty or staff member who requests one.

Recommendations

Continue to improve security functions on all platforms. Strictly enforce policies and procedures when violations are detected. Regularly let users know the importance of keeping their passwords secret. Let users know how to choose strong passwords that are very difficult to guess.

4.6 Terrorist Action and Sabotage

The University's computer systems are always potential targets for terrorist actions. The threat of kidnapping of key personnel also exists.

Preventive Measures

Good physical security is extremely important. However, terrorist actions can often occur regardless of in-building security, and they can be very destructive. The building should be adequately lit at night on all sides and all doors should be strong and have good locks. Suspicious parties should be reported to the police (they may not be terrorists, but they may have theft of expensive computer equipment in mind).

Recommendations

Maintain good building physical security. During off hours with no staff to monitor activities areas should be locked with systems in place that monitor who goes in and out. The N186 space should be kept secure as well due to the fact that is the primary storage location for all technology deliveries.

5.0 Disaster Notification List

The disaster notification list for the Education Technology Center is listed below. These people are to be notified as soon as possible when disaster threatens or occurs. It is important to contact the Director of Technology as well as Collegiate leadership; Dean, Associate Deans as soon as possible.

5.1 Information Technology Primary Notification List

John Achrazoglou – john-achrazoglou@uiowa.edu Director of Information Technology (College of Education) N158F Lindquist Center Phone 319-335-5620 / Home 319-512-0203 / Cell 319-541-4419 / Cell 319-3384465 (wife)	Wayne Kintz - wayne-kintz@uiowa.edu Desktop support, network file administration. N186 LC Phone 319-384-0502 / Cell 319-321-2391 / Home 319-354-9227 / Cell 319-321-1866 (wife)
David Lippe - david-lippe@uiowa.edu Server operations, network file administration. N186 LC Phone 319-335-6227 / Cell 319 321-2381 / Home 319-354-9756	Daniel Maloy - daniel-maloy@uiowa.edu Desktop support N186 LC Phone 319-384-2607 / Home 319- 227-2017
Brian Douglas - brian-douglas@uiowa.edu Administrator for Finance and Operations Blank Honors Center 609 BHC Phone 319-335-6148	Josh Jacobs - josh-jacobs@uiowa.edu Application Developer Blank Honors Center 517 BHC Phone 319-335-6148

5.2 College of Education Leadership Contacts – Chain of Command

Dean Daniel Clay - dan-clay@uiowa.edu N459 Lindquist Center 319-335-5380	Assoc. Dean Christopher Morphew - christopher-morphew@uiowa.edu N459 Lindquist Center 319-335-5366
Assoc. Dean Nancy Langguth - nancy-langguth@uiowa.edu N310 Lindquist Center 319-335-5363	Assoc. Dean Amanda Thein - amanda-haertling-thein@uiowa.edu N459 Lindquist Center 319-335-5383

5.3 Other Information Technology and Safety Contacts

• Jane Drews, IT Security Officer - 335-6332 • Campus IT Help Desk - 384-4357	• Emergency Fire, Ambulance, Rescue, Police, and HAZMAT - 911 or 9-911 • University Police – 319-335-5022

• HCIS Help Desk - 335-6500	• University Facilities Management Work Control Center – 319-335-5071 • Floyd Johnson, University of Iowa Emergency Management Coordinator - 384-2784

6.0 Preventative measures

6.1 Faculty and staff

The following *top ten* list of best practices in preparing for and preventing IT disasters is uploaded to the College of Education's web site and is shared annually via email to all faculty and staff. These instructions include:

1. Regularly changing HawkID passwords to minimize identity theft and unauthorized access to data.
2. Saving/backing up all files on university network drives (H: and L:) which are located in secure areas and regularly backed up.
3. Using university network drives (H: and L:), OneDrive for Business and other approved storage options to store and share protected or restricted data.
4. Ensure the privacy and integrity of restricted or protected data by avoiding storage on consumer cloud services such as Dropbox, Google Drive, etc..
5. Avoid saving protected or restricted data on desktops, local drives, non-encrypted laptops or devices that can be lost or stolen.
6. Locking computers (Control+Alt+Delete > *Lock this computer*) anytime when leaving the office during the day to avoid data theft or intrusive snooping. Macintosh users press Control+Shift+Power or Control+Shift+Eject. When leaving for the day all programs should be closed and computers are logged off or locked.
7. Restarting computers once in a while so the latest security updates and patches are applied.
8. Being cautious of fraudulent email messages from supposed University of Iowa support entities. ITS will never ask for passwords or personal information in an e-mail message. Never responding to suspicious email messages or clicking on suggested links; just delete the message.
9. Regularly run the *Identity Finder* program on desktops to ensure social security numbers are not stored. Identity Finder is installed on all College of Education Windows and Macintosh computers.
10. Running through the online *UI Security Awareness Training* available through My Training in Employee Self Service.

In the event faculty, staff and graduate assistants are evacuated from offices information is provided to help them continue normal IT operations to the greatest extent possible. This includes facilitating working from home and other remote locations. The below instructions are annually sent out to faculty and staff and are uploaded on the College's web site pertaining to:

- Using Remote Desktop to access their office computer from another computer.

- Connecting to (H:) and shared (L:) drives from off campus with Files@Iowa.
- Initiating UI Anywhere (Virtual Private Network) for secure, off-campus access to resources located on the University of Iowa campus.
- Accessing Microsoft Office on the cloud with other computers.
- The availability of checkout laptops with the full suite of software found on College of Education desktop computers including SMART software, Adobe Acrobat Pro, UI Capture (Panopto) and EndNote.

6.2 Collegiate

The below procedures are intended to protect the availability, integrity, and the confidentiality of IT systems and data. Focus is on preventive controls which lessen vulnerabilities and the chances of misuse.

- All desktop systems and networks are protected-secured by passwords and kept up to date with latest security, operating system and application updates/patches.
- All laptops and mobile devices are encrypted.
- All College of Education servers and vital records are managed and maintained on offsite secured ITS server facilities.
- All users are required to change their passwords on a regular basis.
- Invalid attempts to access server data are logged and reviewed on a regular basis. All suspicious activity is reported to the Information Security and Policy Office.
- All users are directed to maintain copies of important data file, vital records and research materials on managed networks.
- As of July 1, 2017 Belin Honors Center patient records will be stored in the HIPAA compliant cloud service Therapy Notes. In an event of a disaster records can be accessed and patients notified with emergency announcements and/or changes to schedules.
- Loss or theft of any mobile computer is reported to the Information Security and Policy Office.
- Three persons in the ETC have privileged access to systems for recovery or transfer of critical data or applications.
- Routine scanning of networks for social security numbers are performed annually.
- User accounts and access lists are reviewed and kept up to date by deactivating invalid/terminated users and removing unnecessary access rights.
- Devices and media containing confidential data are erased with approved methods prior to disposal.
- Individual account/logins are defined for every user using Hawk ID authentication.

7.0 Declaration of a Disaster Event

A threat is defined as a disaster when the IT Director, Dean or designate has declared that a disaster condition exists which will activate this plan. This includes consulting with staff within the affected departments as well as communicating with Collegiate leadership, the CIO and

Security and Policy Offices. Announcements regarding the emergency situation will be initiated and managed by the Office of Public Safety and the Hawk Alert system.

7.1 Recovery Management Team

The Recovery Management Team sets the plan into motion setting priorities and timelines and processes for restoring normal operations. The Recovery Management Team includes the Director of Information Technology, Human Resources Director, Director of Finance and Budget, Director of Strategic Communications, and Executive Assistant to the Dean. Each member of the team is to review the status of their respective areas of responsibility.

7.2 Recovery of IT assets and operations

A primary goal of the recovery process is to restore all computer operations without the loss of any data. The Director of Information Technology in consultation with other members of the team will:

- Prioritize IT services as to importance and order of restoration.
- Estimate 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. Define a threshold that indicates back to normal operations.
- Identifying and retaining staff capable of restoring IT services (see 3.1 and 5.3).
- All College of Education servers are "virtually" maintained by the ITS Data Center. The Information Technology Director or designee will invoke Data Center technicians in determining what has been destroyed and what will need to be recovered from backup media on ITS remote server sites. Work directly with ITS to have them restore server related assets and grant us access to them once they are restored.
- In the event of a disaster it may be necessary to recover data from systems by users who failed to comply with backing up data to network drives. This recovery would be performed on a case by case basis taking in account the cost of recovery and value of the data. Vendors that provide data recovery services include Data Recovery, ESS Data Recovery, KrollOntrack.
- Work with finance officer, shared services, purchasing agents and collegiate leadership in identifying and securing a source for quick acquisition of workstations and other technologies, including, if necessary, written or contractual agreements with outside entities.
- As soon as practical, all salvageable equipment and supplies are moved to a secure location.
- If the disaster includes the Lindquist Center or other buildings used by COE faculty and staff are damaged and unusable alternate locations with suitable technologies will be located as a temporary work-around until the original facilities are repaired/rebuilt.

7.3 List of services to restore in priority order

Departments responsible for services indicated in parenthesis

Tier 1 services – Services that must be operational within 24 hours

1. Active Directory Services (ITS - Phone: 319-384-4357
   Email: its-helpdesk@uiowa.edu)
   Infrastructure for authentication towards accessing desktops, files, folders, applications and devices.

2. Data Network Connectivity (ITS - Phone: 319-384-4357 Email: its-helpdesk@uiowa.edu)
   Data connections providing access to critical services needed for recovery and continuation functions.

3. Therapist Helper, TherapyNotes - Belin Honors Center patient record service (Blank Honors Center; Brian Douglas, Josh Jacobs)
   Clinic operations software; reschedule appointments, communicate emergency information, lookup or supply patient data.

4. Exchange/Outlook 365 Mail and Calendaring Server (ITS - Phone: 319-384-4357
   Email: its-helpdesk@uiowa.edu)
   Delivers direct communications to faculty, staff and students.

5. COE file servers for Shared L: and Home H:drives, VPN (UI Anywhere) or Virtual Desktop. (ITS - Phone: 319-384-4357 Email: its-helpdesk@uiowa.edu)
   Provide access to data, applications and backups needed for restoration of normal operations and services.

Tier 2 services - Services that must be operational within 48 hours

1. Web site services for College, ITP, IRRC, BHC, etc.
   (ITS - Phone: 319-384-4357 Email: its-helpdesk@uiowa.edu
   Education Technology Center
   Blank Honors Center
   Office of Strategic Communications)
   Web sites used to broadcast emergency information, contact information and provisions for normal operations.

2. Facil software (Education Technology Center)
   Used to check out emergency laptops, cameras and devices.

3. ITS centrally supported applications (ITS - Phone: 319-384-4357 Email: its-helpdesk@uiowa.edu)
   - MyUI

- ICON
- OSIRIS
- PeopleSoft HR Queries, Reports
- ePro applications (eVoucher, PReqs, eBuy, ProTrav)
- PeopleSoft Financials (AP-PO, Inventory, GL)
- GL DSS
- Data Warehouse
- PMO
- Workflow
- MARS
- MAUI

Systems facilitating teaching, research, administrative, financial and HR functions.

Tier 3 services – Services that must be operational within one business week

1. UI Database servers (SQL)
   (ITS - Phone: 319-384-4357 Email: its-helpdesk@uiowa.edu
   Education Technology Center
   Blank Honors Center)
   Databases used for APR, commerce and business intelligence.

2. Windows print server
   (ITS - Phone: 319-384-4357 Email: its-helpdesk@uiowa.edu
   Education Technology Center
   Blank Honors Center)
   Windows printer sharing system.

3. Internet Information Service FTP Server
   (ITS - Phone: 319-384-4357 Email: its-helpdesk@uiowa.edu
   Education Technology Center)
   ePortfolio/Professional servers students upload to.

7.31 Estimated times for back to normal operations

1. Locate other spaces (based on flood of 2008 experience)
   - Find appropriate space(s) within building = 24 hours
   - Space Planning finds appropriate space(s) in other building(s) = 1 business week

2. Obtain new computer
   - Local vendor for rapid acquisition (i.e. Best Buy) = 2 hours
   - Dell order for best pricing and compatibility with current build process = 3 days (1 day to place order + 2 days shipping)

3. Time to configure and test new computer

- Standard install; download software from shared drive and ITS download site = 4 hours
- Therapist Helper - Blank Honors Center clinic operations software
  Therapist Helper installation on new computer in 2015 = 4 hours
  If media (DVD) is destroyed; download a new copy (20.8M) = 1 hour
  TOTAL = Standard install + Therapist Helper installation + download = 9 hours
  NOTE: Will be converting to cloud service TherapyNotes July 1, 2017
- Facil – Software used to check out laptops and devices
  Latest installation August 2016; install from shared drive, import data = 8 hours
  TOTAL = Standard install + Facil installation = 12 hours

4. ITS data-server recovery
   - Restoration of an averaged sized VM = 2-4 hours
   - Multi-terabyte (up to around 10tb of data) file server volume = 1 day

8.0 Assessment

The plan will be regularly tested and assessed as indicated below. All needed information-forms needed for IT testing will be provided by the IT Director to staff performing tests. The College of Education IT Director will collect data and determine if changes to the plan are necessary and take corrective action.

Facil – Conducted at least annually

Staff name _____

Date and start time _____

ETC staff installs Facil from shared drive onto another computer.
Access inventory records and simulate a transaction with Facil.

Stop time_____

Was installation successful?
If not describe problem(s)

Upon technical failure check out emergency laptops with manual paper checkout. Note description, inventory number on tag, person's name, person's email address, time out and estimated time in.

Comments:

Therapist Helper – Conducted at least annually

Staff name_____

Date and start time _____

Blank Honor Center staff will install Therapist Helper on other computers
- Install software from DVD on a computer, or
- Download software from internet and install on a computer

Access records and search for a client

Stop time_____

Was installation successful?
- If not describe problem(s)

Comments:

Therapy Notes – Conducted at least annually (applicable after July 2017)

Staff name_____

Date and start time _____

Blank Honor Center staff from a computer located in another department or building login from a browser and access records and search for a patient.

Stop time_____

Was access and search successful?
If not describe problem(s)

Comments:

COE file and web server recovery - Annually

Staff name _____

Date and time call made _____

The College of Education IT Director or ETC staff member will contact the ITS Help Desk and request a test of restoring College of Education data.

Time of return call _____

Was restoration successful and within standards addressed in plan?
If not describe problem(s)

Comments:

Fire alarm systems
Regular inspections of the fire prevention equipment are currently conducted by the Iowa City Fire Department and Facilities Management.

Evacuation and shelter procedures
Every College of Education faculty and staff member will be provided with emergency evacuation and tornado shelter information. The current manual will be updated reflecting recent remodeling of offices and learning spaces. Departments and units within the College of Education will address procedures during faculty and staff meetings.