# Ferris State University

# Continuity Planning Guide

**Introduction:**

Welcome to Ferris State University's "Guide to Continuity Planning." We are pleased that you are taking time to ensure that your department is prepared to respond to various types of operational interruptions. This guide will help you plan not only for major disasters (e.g., total loss of building) but also lesser interruptions to service (e.g., the computers are down).  It puts planning into perspective and makes it more likely that an efficient and graceful crisis response and recovery will occur.

## What is Continuity Planning?

Continuity planning is an ongoing program of activities conducted in advance of disruption to ensure we are prepared to continue our overall university missions. A continuity plan is a

written plan on how to stay in business in the event of a disruption of service. This plan is developed <u>before</u> a disruption of service, emergency, or disaster.

A continuity plan is a collection of resources, actions, procedures, and information that is developed, tested, and held in readiness for use in the event of a major disruption of operations. Continuity planning helps prepare Ferris State University units to maintain mission-critical operations after any emergency or disaster.

The overall goals of continuity planning are:

- ✓ Ensure maximum possible service levels are maintained during a crisis, and
- ✓ Ensure that departments recover from interruptions as quickly as possible.

Ferris State University is vulnerable to numerous threats (large and small) that could interrupt normal operations. Preparation dramatically increases your department's ability to recover quickly. Not to mention, continuity planning is a good business practice, especially if you are an auxiliary unit. Continuity planning's purpose is to ensure the continued performance of mission critical functions during a wide range of potential emergencies.

> *Possible Reasons for Continuity Planning activation:*
> *Building Fire*
> *Flood*
> *IT Malfunction*
> *Disgruntled Employee*
> *Severe Weather*
> *Severe Pandemic*

You could let your imagination run wild with potential risks. Some of them are more probable than others—perhaps they have happened before or perhaps you are already aware of imminent hazards. Keep those in mind as you continue through this guide. We are not planning for EVERY possibility that could cause an interruption; instead we are planning for the effects of ANY interruption. However, if you know your department is subject to certain risks, it is good to plan for those risks. For example, is your building prone to flooding or are there chemicals or other substances in your building that might make it more likely to experience a fire?

Building a continuity plan is not a one-time project with an established start and end date. Rather, it is a living document. It is essential that information and action items in the plan remain viable and current. The plan should be tested and updated, at a minimum, once a year.

The continuity plan describes the organization's planning assumptions, objectives, and protective measures and thus may contain protected information. The success of the plan, however, necessitates that key personnel have immediate access. All individuals with

defined roles in the plan should be familiar with the continuity plan. Those who play an active role should continually ensure that adequate resources and capabilities exist for carrying out their roles. Most importantly, they must be prepared at home in the event a disaster affects the region. We will discuss these topics throughout this planning guide.

## I. **Developing a Continuity Plan: University Department Responsibilities**

The process of developing your departmental continuity plan may take approximately 2-4 months. The timeframe depends on the complexities of the department and the degree to which it already has emergency and/or safety policies in place. Continuity planning involves a series of actions, each of which contributes to a unit's ability to respond promptly and properly when an emergency occurs. Many of the actions that need to be taken must conform to the specific needs of the unit.

### Getting Started

Appoint a Planning Coordinator.
- The Planning Coordinator should be a full-time member of the administrative team, and preferably an experienced employee who is thoroughly familiar with the unit and university procedures. Knowledge of the unit's programs and physical facilities is also imperative.
- The Planning Coordinator should be a person with the management experience and authority to:
    - Collaborate within the department to develop and maintain the information in the continuity plan.
    - Recruit a core "Department Emergency Preparedness/ Continuity Planning Committee" that represents staff, faculty, and principal investigators from the unit's major subdivisions and locations.
    - Coordinate related staff safety education and training.
    - Coordinate resources for emergency preparedness and recovery.
    - Purchase supplies and equipment.
    - Be ready to support managers during an incident.
    - Be ready to help prepare post-emergency impact summaries and insurance claims.
- Some units already have individuals assigned to coordinate safety functions and may already have broad-based Safety Committees. These units can readily incorporate emergency preparedness planning into their existing programs.

Build a Continuity Planning Team.
- The number of people on the team will depend on the size of the department/unit, its complexities, etc.
- The team will support and help the department resume operations when and if an emergency occurs.
- The team has an intimate understanding of the department and will help identify critical functions, as well as prioritize tasks and activities in the planning process.

- The team will support and help conduct tests, training, and exercises of the continuity plan.
- Consider usage of faculty and student leaders on the team.
- IT representation is also highly suggested.

Create a tentative timeline.
- Separate the project into smaller steps and set deadlines for completion

## Continuity Planning Tool

https://ferris.kuali.co/ready
The continuity planning tool is designed to allow each departmental or unit Planning Coordinator or team to enter department-specific information. Each page has planning tips, information, and links to help the team build a comprehensive and thoughtful continuity plan. Instructions, examples, and guidelines are on the right-hand side of each page.

Supporting documents are also available. They include:
- Introduction to Continuity Planning
- FSU Continuity Planning Training videos
- Continuity Planning Guide (this document)
- Things to Know as You Plan
- Critical Functions: A Fast Track Approach
- How to Create and Manage Action Items
- Annual Review Checklist
- Update Calendar
- Tabletop Exercise

All of the documents that are part of your plan that are attached and uploaded will be saved on a secure server. These documents will be available to those in your unit who have access to the system. The Department of Public Safety-Emergency Management, Safety Director, and other members of the university emergency planning team will also have access to view your continuity plan.

Access to the software is given by request. Please complete the initial setup form and turn in to Mike McKay (mikemckay@ferris.edu) to gain access into the software. Please allow up to one week to be granted access. Once access is given, you will be able to create a new plan or update your plan. You will not have access to other department's plans, unless they grant access to their plan.

**Overview**

The online program will take you through 5 planning steps. Completing each step will bring you closer to completing your unit's continuity plan. You do not have to complete each step in order; the planning team may approach this process as they see fit. The steps, further descriptions, and guidance are outlined below.

Step 1- Department Identification
Step 2- Critical Functions
Step 3- Information Technology
Step 4- Faculty Preparedness
Step 5- Key Resources
The Action Items Summary will automatically be filled out as other sections are completed.


Your unit's focus should be:
- identifying the functions and resources that are critical to the departments overall mission
- safeguarding critical functions and resources against loss (*backup of systems and data, safe storage of research items*)
- actions that will lessen the impact of losses (*prearrangements with other departments, schools, or sister campuses for mutual aid*)
- replacing resources quickly (*contracts with vendors*)
- performing critical functions without some of those resources (*teaching via distance-learning technology*)
- providing your people with the information they will need, post-disaster, to get the campus back in action

## III. Department Identification

Keeping updated information on faculty, staff members, volunteers, and student-staff members will help guide you in the remainder of the planning process. To know where you are going, you must know where you are.

The team will develop and upload an employee emergency call-down list and procedures. The Human Resources Safety Coordinator is able to provide evacuation plans and has the ability to upload the building evacuation plans for your unit directly to the Continuity Planning Tool.

## IV. Critical Functions

The Ferris mission:
Ferris State University prepares students for successful careers, responsible citizenship, and lifelong learning.  Through its many partnerships and its career-oriented, broad-based education, Ferris serves our rapidly changing global economy and society.

Each college, division, and major administrative unit on campus exists in support of the Ferris mission. Each area performs functions that are critical to the ongoing success of the mission. During an emergency or disaster, a department should strive to maintain as high a level of operations as possible.

Continuity planning focuses mainly on these critical functions: tasks that must be restarted in order to enable teaching, research and support services.

What are critical functions?
- functions that need to be resumed within 30 days or less in order to minimize significant disruption of the mission of the University
- functions that impact external or internal customers
- functions that would cause delays or impact the services/operations of other units or Ferris as a whole.  Examples include functions that enable hiring of employees, that are required by regulation/statutes, and that relate to payroll, security, grant management, etc.


How do you integrate critical functions into continuity planning?
- Compile all unit functions.
- Identify mission-critical functions.
- Examine function as it is done daily.
- Determine required resources and equipment.
- Identify dependencies both up- and downstream.


It may seem like an overwhelming task to look at all of the functions of your unit. As you are covering this very important topic, remember to focus on **ONE** function at a time. It is important that the team determines whether each function is a critical or noncritical function.

Ask yourself: (1) Does this function support the mission of the university? (2) Would we focus limited available resources on this function, or would we focus elsewhere? (3) What dependencies are associated with this function? (4) If it is not tagged as a critical function, what would the consequences be?

---

*Hint: It may be useful to ask your people to list what they do during the day to ensure identification of all tasks*

---

Remember to include those tasks or events that take place on a seasonal or quarterly basis.

Once the team has identified all critical functions within your unit, determine the peak period or when this function is the most critical. What do you need in order to be able to complete this function (staff, space, equipment, etc.) and within what time period? (Example: the safety and maintenance of the Science Building requires that hood fans in laboratories be operating.  If the hood fans do not work, the hazardous materials within the labs may pose a threat to individuals in the building.  This would cause a disruption of teaching and pose a safety hazard. Staff and equipment would be needed immediately to repair non-operating systems.  This would be essential when classes in this building are in session.)

What vital records are needed and what are their locations? What are the consequences to the mission of the University if the function is not performed, and within what timeframe will it start causing harm?

By identifying these critical functions, you will better determine which staff, materials, procedures, and equipment are absolutely necessary to keep your department functioning.

Next you will develop a list of action items. These action items will be the most important part of your continuity plan. Action items are things that COULD be done now (or anytime before an emergency strikes) to make your unit more able to recover quickly. The typical action item begins with a verb and can be stated in one sentence. Some examples:
- Back up important documents onto a data stick weekly.
- Develop plan for secure storage of critical research materials.
- Cross-train two (2) staff members to do departmental purchasing.

Action items are ideas, not commitments to act. So think outside the box and don't feel constrained by resources. Some of your action items may be outside your department's sphere. That's okay—the university welcomes your ideas.


*Dependencies – Internal or external resources or inputs necessary for a departmental function/process to operate. Consider <u>upstream</u> (those that you depend on) as well as <u>downstream</u> dependencies (those that rely on you)*

## V.  Information Technology

It is difficult to imagine how we could possibly work without our computers and Internet access. Computer, server, and system crashes can seriously jeopardize our productivity.

Information Technology is critical on our campus and to each department. Work with your IT representative to complete the IT portion of the plan.

Identify critical applications. Determine "functional" and "technical "owners.
➢ The functional owner is the unit that authorized any modifications.

> ➢ The technical owner is the unit that has system administrator or programming access and implements any modifications.

- How quickly do you need this application?
- How many servers does your unit have?
- What are your workstation backup procedures?
- Who provides workstation support?
- How long will it take to recreate your office's current resources and restore normal operations?
- What do you need to restart and recover your IT and where will you get it?

In the meantime, do you have any considerations for workarounds?

Action Items: What can you do NOW to get ready to reestablish your IT services rapidly? Would there be a cost?

If working from home is feasible for department members, is VPN accessible? Do the right people, based on their responsibility, have the appropriate access to the appropriate files? Are there any legal issues to be concerned about if information is duplicated or worked on from home? Work with IT on back-up solutions.

If your department already has a thorough disaster recovery plan, there is no need to recreate the wheel here. Upload the document to the software or simply attach it to the continuity plan when it is complete.

## VI. Faculty Preparedness (Academic and Research Continuity)

Academic continuity is vitally important because it focuses on the core practice of higher education, which is providing students with the opportunity to learn.

Individual faculty members drive teaching and research. It is vital that faculty make preparations to quickly and safely shut down and resume their teaching and research under what may be very adverse conditions.

This is the stage of your planning process where faculty input is most important. Faculty should be encouraged to have at least one alternate method to teach their students when the campus is affected by a disaster.

The checklists below provide faculty with ideas to improve their own preparedness for online, hybrid, or face-to-face course formats.

Before classes begin:
   o Record and backup student names, email addresses, and phone contact information

- Record email and phone number of your director or other appropriate point of contact for your primary program.
- Prepare a backup working copy of your grade book to ensure continuity of grading and reporting to students and administrators if your primary and online grade book is not available for extended period of time.
- Back up critical teaching materials, including lectures, assignments, instructions, quizzes, discussion topics, the syllabus, schedule and other documents. You may be able to provide these to your students via the Internet in the event of a significant classroom disruption even if online training is not your primary method of educating.
- If at all possible, use an online teaching support tool to provide materials to students throughout the semester.

Once class has begun:
- Send a test email message to the students. This test message will help you identify any possible problems with spam filters or firewalls that may block your emails. Create a group distribution list based on students' email contact information. This practice will ensure that both you and your students have each other's current email address. If you prefer students NOT use your email as a primary form of contact, make that clear.
- Remind students regularly about the importance of keeping back up electronic copies of their assignments.
- Download students' assignments when they are submitted so that you will always have ready access to them in the event of a system failure.
- Let students know of your plans for continuing instruction and communication in the event of an emergency or disaster.

Research Continuity:

If research is part of your department's critical functions, you must take measures to protect your research as well as the dollars invested into the research.

- Having updated contact lists for all persons involved or associated with your research is critical. Also, consider having reciprocal agreements with those that could help in the event of a disaster or emergency that would prohibit you from completing or continuing research.
- Have a list of all special equipment safety precautions in case personnel who are not familiar with the equipment must access the area.
- Ensure that there is detailed information regarding feeding/care of laboratory animals in case usual caregivers are unavailable and persons unfamiliar with your research must provide care.
- Ensure that research notes, letters, documents, spreadsheets, etc. are backed up to the network drive every day.
- Consider what portion of research efforts could be continued from home or other site e.g., data analysis, summarizing findings, etc.

## VII. Key Resources

The list in step 5 collects information that you may need close at hand in the early days after an emergency, when (1) crucial staff may not be reachable, (2) offices may not be accessible, (3) computer networks may be down, and (4) leaders/managers may have to handle issues outside their normal spheres.

Staff Basics: These are the people you are relying on to respond to the emergency and resume operations.
Avoid the temptation to list all your staff. The people to list here are those who can help "sort things out" and plan the next steps. Make sure you add after-hours contact information, including non-university email address and phone numbers.

Designate individuals as successors as well as those with formal delegation of power to ensure that decisions will still be made in the absence of key leadership.

Other Key Resources:
- Staff from other units: Who are the most important people from elsewhere on campus that your staff will need to contact within the first few days after a disruption, as you plan how to resume your critical functions?
- Stakeholders:
  - Key Partners: Are there any external partners that your staff will need to contact within the first few weeks after a disruption, as you plan how to resume your critical functions?
  - Key Vendors: Are there any external vendors that your staff will need to contact within the first few weeks after a disruption, as you plan how to resume your critical functions? In a severe or catastrophic emergency, deliveries may slow or cease at every level of the supply chain. Might your unit face a supply crisis? Do you need to adjust your inventory practices or stockpile specific items?
  - Key Clients: Are there any clients (Ferris or external) that your staff will want to contact after a disruption, to enlist their cooperation or to keep them informed? Also include any key donors or other key stakeholders.
- Equipment and Facilities: Please indicate on this screen the MINIMUM equipment and supplies you will need to resume ALL critical functions that you listed in Step 2. Estimate, don't agonize. Guess if you need to.
- Other Equipment: List major items only. DO NOT list consumables, classroom equipment, or lab equipment. (For teaching labs or research labs, this information should be under "critical function" portion of the software.)
- Explain if necessary.
- Facilities: Do you require emergency power in order to continue these functions?
- Supplies: What supplies (consumables) must your unit have in order to function?

**VIII. Reasonable Assumptions for Continuity Planning**

- **Access to buildings.** If university officials have reason to suspect that a building is hazardous to enter, they will immediately close the building and call in trained personnel. In the worst case (a major incident with damage to many buildings), the response and inspection process alone could take weeks, with hazmat cleanup and repairs taking much longer. *You may be unable to enter your building for an extended period of time.*

- **Locating temporary space.** This will be a major challenge for the university, *so any arrangements you have made ahead of time will serve you well*. For example, make an agreement with another department in a separate building or with colleagues in another school or department. Anything you can do within your own unit will be to your benefit, such as sharing labs and offices that remain accessible. In an emergency that affects a number of buildings, Emergency Operations Center (EOC) will also assist in the temporary relocation of departments. Priority will be given to essential university functions as well as those departments that have completed continuity plans.

- **Computing infrastructure.** Restoration of the university's many centrally supported IT applications and administrative systems will be of highest priority after any disruption. Examples include e-mail, Internet connectivity, HR/Payroll, as well as the physical campus data network. Many resources continue to be directed toward hardening Ferris' IT systems to minimize damage and aid quick recovery. Definite predictions, of course, are not possible. *Within your unit, you should work with your IT provider/liaison—who in turn should work with ITS—to take steps to back-up data and make plans for restarting your own servers and applications.*

- **Communications protocol.** General mass communications with students, faculty, staff, and the public will be handled by University Advancement & Marketing, the Office of the President, and the FSU Department of Public Safety with assistance from Information Technology and Services and will be tightly managed so that messages are consistent. *As your unit resumes functioning, communications of an operational nature to your constituents (staff, faculty, students) will be your responsibility*.

- **Contacting your staff, faculty, and students.** This will be a departmental responsibility. Departments should maintain staff, faculty, and student emergency contact lists and institute a call-down tree as a best practice.

- **Care of staff and faculty.** Many staff and faculty issues arise during disaster recovery: pay, temporary leave, and temporary alterations of assignment, safety, benefits, work-at-home, stress, and family issues. *You should assume that Human Resources and Payroll/Benefits will be available with guidance and mechanisms to assist departments in these complex areas.* Conversely, departments should seek guidance from these

departments when there is uncertainty in these matters—both before and after an emergency.


## IX. Bringing It All Together

After an emergency, the focus should be on the recovery of the people associated with the department and the recovery of the department's operational process.

Once the safety and security of people in the department has been assured and emergency conditions have been abated, assemble your recovery team to begin the process of restoring the department's programs.

Employees will need prompt and accurate answers to their questions about the department's operational status, safety of the premises, and access. Your best efforts to provide this information in as many ways as possible will better facilitate the recovery efforts.

Specific Recovery Procedures
1. Activate your unit Continuity plan
2. Assess the emergency's impact on physical operations. Gather the following information:
- Determine the extent of physical damage to buildings and equipment; photographs or videotapes should be taken of all damage to the facility and equipment before any repairs are made or areas are cleaned.  If your facility is inaccessible, do not attempt to gain access to complete this task.
- Review personnel issues (what staff were affected? who is able to support recovery?)
- Determine your needs for facilities, equipment, personnel, or other resources that will speed the unit's recovery.

3. Provide ongoing reports on the department's recovery status to appropriate dean or director and the Ferris Emergency Operations Center or Emergency Management staff to be reported up channels as appropriate.

4. Document the extent of damage. Most FEMA insurance claims require extensive documentation of damaged facilities, lost equipment and resources, and special expenses. Documentation of all time spent repairing or recovering is critical.


## X. Disaster Safety Begins at Home: Family Disaster Planning

There is no more important resource on campus than that of human resources. After a disaster, computer backups and new facilities are useless without people to manage them. Encourage each employee to develop a family disaster plan. This is the MOST crucial part of

the success of your plan. Those that are not prepared at home will not be able to contribute to the recovery efforts.

Get Informed
- Learn about community hazards.
- Learn about your community's disaster plans.
- Learn about your community's warning systems.

For more information about personal preparedness, visit

https://www.ferris.edu/HTMLS/othersrv/campussafety/Education_Prevention_Section/index.html

## XI.    Testing, Training, and Exercises

Conduct orientation and training for identified personnel with continuity planning responsibilities. A PowerPoint presentation has been created to complement this planning guide. Additional training may be identified as you progress in this planning effort. For example, you may cross-train some of your staff so that you have some redundancies within your system.

ALL plans should be tested and updated annually. This includes the emergency alert and notification procedures within your department. Repetition, practice, and training are the best preparation for a disaster response.

## Completion of Continuity Planning Draft

The first step is to review the entire draft for accuracy. Then provide copies to all employees with roles in the response and follow with an orientation, training, or Q&A session to answer any questions that your key staff may have regarding their plan and responsibilities. Establish a training and exercise schedule. For assistance on your exercise/table-top, contact Public Safety, Emergency Management.

Finally, submit the plan to the FSU continuity tool. The document will be reviewed for completion. The project manager will receive an e-mail when the document has been approved.

Questions? Contact:

Mike McKay
Safety Director
Safety, Health, Environmental, Risk Management
(231) 591-2147
mikemckay@ferris.edu