



The institution is located in an area of the United States where a potential disaster would be tornado or severe weather during the winter months including heavy snow and rain. The instructional resources are hosted by a cloud-based service. Any type of geographical disaster at the physical location would not interrupt the day-to-day instructional activities.

**Disaster Response and Recovery Procedures:**

CCR has developed the following disaster response and recovery procedures: The College of Court Reporting (CCR) is located in Northwest Indiana where the potential of a disaster destroying the infrastructure of the college would be a fire; tornado; and severe weather during the winter months including heavy snow, rain, or minor flooding. In addition to natural disasters, other potential hazards that could interrupt online classes are utility outages, cyber attacks, and temporary power failures. This plan safeguards the hardware, software, and networks for an IT recovery plan in case of an unforeseen disaster.

The main goals of this plan are to minimize interruptions to the normal operations in the event of a disaster; to limit the extent of disruption and damage; to minimize the economic impact of the interruption; to establish alternative means of operation in advance; to identify trained personnel knowledgeable of the emergency procedures; and to provide for smooth and rapid restoration of service; and to assure faculty and students that online classes will be conducted as scheduled.

**Authority:** The decision to implement disaster recovery procedures is the responsibility of the President or the Executive Director. The Disaster Recovery Team, which consists of the entire administrative staff, will convene as soon as possible after a disaster has occurred to assess damages and make recommendations to the President to control and coordinate recovery/backup actions and following functions:

- Recovery administration
- insurance notification
- supplies
- organization
- Systems software
- Application software
- Communications
- Operations
- Facilities
- Hardware

The disaster recovery team shall meet periodically on an annual basis to discuss the current document and make recommendations for changes to it. It is the responsibility of the President and Executive Director to make the necessary changes and distribute the new document to the appropriate persons.

In the event of a disaster or major failure, the team should convene with as many team members as possible. All members of the team should assess damages and report to the President and Executive Director at the earliest opportunity.

Disaster Response: This section details the basic actions that need to be taken in the event of a disaster situation.

- The president or executive director must be notified.
- The president and executive director will meet as soon as possible and within reason given the situation.
- They will assess damages.
- An appropriate message will be created for administrators, faculty, and students.
- The team will notify all staff if the building is damaged or not accessible.
- Staff will be required to begin working from home as soon as possible and within reason given the situation.
- The faculty and curriculum development director will contact faculty with the appropriate message and include the message to students.
- Faculty will be required to notify their students with the message.
- A message will be created and uploaded to the [www.ccr.edu](http://www.ccr.edu) Website and LMS.
- An assessment will be made to provide an estimate about service disruption.
- The cloud servers will be checked and monitored.

Recovery Procedures:

- The president will evaluate damages to any servers.
- Back-ups will be employed with 24 hours or within reason given the situation.
- The executive director and designated staff will inventory equipment and files within reason and given the situation and report findings to the president.
- Phone systems will be forwarded to cell phones and Google Voice numbers.
- Paper files are kept in fire- and waterproof cabinets. Files will be re-created from the database contained on the server.
- Administrators will continue to work from home until the building can be occupied.

Offsite Storage of System Backup Data: In the event that disaster befalls the current location of the computers and server having a backup stored off site is critical. Daily backups of the individual computers and server are stored online using the [idrive.com](http://idrive.com) cloud backup storage service. A full server data backup is located onsite in a fireproof cabinet. The most current full server file storage system is also maintained and kept with the president. Cloud storage has been designated for computers and server file storage system is accomplished using [idrive.com](http://idrive.com).

CCR moved into its present location January 2017; therefore, the infrastructure is new and up to date. In the event of a natural disaster, all instruction and administrative responsibilities will be conducted from individual staffs' homes. All staff is equipped with computer systems and Internet access from their remote home location. The college can communicate with staff and students temporarily using personal phone services, Internet services, and cellular phone data and telephony services to communicate with each other and with students.

The instructional learning management system, live class technologies, media servers are all hosted on cloud based services such as 1and1 and Blackboard, Inc., and will not be prevented from running if a natural



disaster occurs with the actual facility of the college. All database information can be operational from any PC once the front and backend data are access. The current records system is a system built using Microsoft Access and all data are secured with the President and cloud based storage.

A recent example of a non-disaster situation was where the college had a severe winter storm and all staff was incapable of travelling to the college. The day's operations were uninterrupted as each staff member were able to continue with their individual job responsibilities, classes continued as scheduled, communications were not interrupted, etc.

Another recent example of a non-disaster recovery situation was the college's cloud media server became corrupted. Within 12 hours, a new cloud server was built, backup media was restored, and content was available and operational before the next morning when students would need to access the content for their skill development practice.

**Describe how identified risks are monitored, managed, and insured.**

Potential risks are monitored on a daily basis by all administrative staff. When risks are identified, the executive director and president, with the assistance of the institution's administrative staff will make needed decisions and changes to ensure risks are eliminated or kept at a minimum as not to disrupt the day-to-day operations administratively and instructionally. The institution maintains adequate insurance to accommodate any disaster risks that may occur that are unforeseen.

As with most organizations, there are inherent risks for a college. CCR, however, has not had a formal risk management plan in place. CCR recognizes this and provides the following as its risk management plan:

Risk Management Team: President and executive director

Risks types: Academics, compliance, financial, operational, technological, and strategic.

Monitoring: The entire administrative staff and faculty are responsible for monitoring academic risks. Student issues must be brought to the attention of the executive director. The president and executive director monitor compliance, operational, and strategic risks. The president monitors financial and technological risks. Monitoring and identifying potential risks are included in the responsibilities of the president and executive director.

Managing: The president and executive director are responsible for managing risks with the assistance of the administrative staff and faculty. Reviewing and analyzing an issue to determine an effective resolution, correction, etc., will depend on collecting information and data from all involved parties. Once information and data are collected, the team will work on minimizing or eliminating the risk.

Insuring: CCR is insured as a stopgap to protect itself from property damage, employee or student injury, and legal liability for the actions of its employees during normal business operations.

