University of Oklahoma

IT Disaster Recovery Planning Policy

Policy ID:	007
Version:	1.0
Policy Owner:	Chief Information Officer (CIO)
Policy Approver:	President, University of Oklahoma

PURPOSE

Disaster recovery planning is about preparing for and recovering from a disaster. Any event that has a negative impact on OU's business continuity could be termed a disaster. This includes hardware or software failures, a network or power outage, physical damage to a building such as from fire or flooding, human error, or some other significant event.

Disaster recovery planning ensures that system dependencies have been identified and accounted for when developing the order of recovery, establishing recovery time and recovery point objectives, and documenting the roles of supporting Information Technology (IT) personnel.

SCOPE

This Disaster Recovery Policy applies to:

- IT infrastructure and other services which facilitate Information Systems.
- Cloud or Third-Party hosted infrastructure and other services which facilitate Information Systems.
- Information Systems that process or store OU data; this specifically excludes desktop devices and workstations which do not require disaster recovery plans but may require data backup.
- The processes, policies, and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to OU after a disaster or outage.
- College(s), department(s), unit(s), or research projects that maintain or is responsible for a Unit-Critical system or data.

ROLES AND RESPONSIBILITIES

Chief Information Security Officer (CISO)

The CISO is charged with the development and maintenance of university-wide information security policies and standards, the implementation of those standards on university Information Systems, and compliance with those standards. The CISO must:

- Appoint one or more persons to a Disaster Recovery Program owner role.
- At least annually, review and approve the OU IT Disaster Recovery Plan.

Business Continuity Analyst

The Business Continuity Analyst role, or a delegate named by University officials, is charged with coordination, training, guidance, development, maintenance and reviewing, of the business continuity of operations plans (COOPs) or business continuity plans (BCPs) for University Colleges, Department, or Units. The COOP or BCP provides a flexible, scalable strategy to help University Colleges, Department, or Units, efficiently plan, prepare, manage and recover, from situations or events that have a direct adverse impact on operations. The COOP or BCP document is intended as a quick reference guide for specific information, but is not intended for use as Standard Operating Procedures or detailed training manuals. The Business Continuity Analyst responsibilities include:

- Develop and conduct annual business continuity trainings for University Colleges, Departments, or Units in conjunction with IT DR teams, as needed.
- Oversee University business continuity of operations planning efforts for University Colleges, Departments, or Units.
- Update, maintain, and distribute business continuity of operations plan templates annually, or as needed.
- Maintain and distribute key components of the University College, Department, Unit, or Research Project COOP/BCPs to the Disaster Recovery Program Owner.
- Provide guidance to aid in recovery activities, before, during, or after, a disruption, incident or disaster, as requested by University Colleges, Departments, or Units.
- In collaboration with Risk Management, Emergency Preparedness, and the Office of Information Technology, participate in campus specific Emergency Operations table-top or live exercises and trainings.
- In collaboration with Risk Management, Emergency Preparedness, and the Office of Information Technology, review and edit Emergency Operations Plans specific to each campus (Health Sciences Center, Norman, Tulsa).
- Participate in IT Disaster Recovery Plan exercises, as requested by the Office of Information Technology.

Disaster Recovery Program Owner

Disaster Recovery Program Owner functions are essential to maintaining OU's IT DR Program in a consistent state of readiness, will be performed by OU IT Governance, Risk, and Compliance, and include:

- Oversee IT disaster recovery planning efforts for the Office of Information Technology.
- Develop and conduct annual IT disaster recovery training for University College, Department, Unit, or Research Project IT personnel.
- Update, maintain, and distribute IT disaster recovery plan templates annually, or as needed.
- Maintain and distribute key components of IT DRPs to the Business Continuity Analyst.
- Oversee IT Disaster Recovery Plan exercises.
- Work with the Office of Risk Management to review COOPs or BCPs for essential and mission-critical IT systems.
- Develop, document, and disseminate a set of controls that addresses information technology disaster recovery planning. These controls shall include purpose, scope, roles, responsibilities, management commitment, coordination among university entities and compliance.
- Review and update disaster recovery planning controls as necessary.
- Maintain and publish OU IT disaster recovery planning templates and processes.
- Develop, implement, document, and maintain the OU IT Disaster Recovery Program.

University Colleges, Departments, Units or Research Projects

University Colleges, Departments, Units, or Research Projects that maintain information technology systems are responsible for identifying the resources needed to coordinate information security within their area. Colleges, departments, units, or research projects are responsible for maintaining effective security within their organization.

- Oversee IT disaster recovery planning efforts for the College, Department, Unit, or Research Project, with assistance from the Business Continuity Analyst or the Disaster Recovery Program Owner.
- This includes the designation of an IT security contact that shall serve as a conduit for IT Disaster Recovery planning between the organization and the Office of Information Technology.

Information System Owner

Information System Owners are senior university administrators accountable for the creation and

maintenance of information systems relied upon for key university operations. This individual(s) is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

- Approve Business Impact Analysis and IT Disaster Recovery plan, at least annually.
- Distribution and maintenance of College, Unit, or Research Project IT disaster recovery plans.
- Identify unit-critical systems or data.

Information System Administrator
The individual(s) responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System.

- Maintain adequate infrastructure resiliency and data backup and restoration processes for essential and mission-critical data and the IT systems assigned to them.
- Develop, implement, document, maintain, and test disaster recovery procedures.
- Test backup and recovery procedures, at least annually.
- Update the status of their DR planning to OU IT GRC every 2 years.

The **Data Backup Service Owner** is responsible for the selection of, implementation, ongoing maintenance, and availability of enterprise data backup services for regulated and/or confidential data and systems. The Data Backup Service Owner team will provide backup and restoration job assistance for OU IT Enterprise Backup, OU IT Replication services.

The **Research Data Backup Service Owner** is responsible for the selection of, implementation, ongoing maintenance, and availability of data backup services for research data and systems. The Research Data Backup Service Owner team will provide backup and restoration job assistance for OURdisk, OURdrive, and OURRstore services.

The **Mission Support** role is responsible for assisting Students, Staff, and Faculty within colleges they support, in selecting and implementing data backup strategies that meet their needs, using existing services, if possible. If existing services are not appropriate, Mission Support assists Students, Staff, and Faculty in completing a Security Assessment for new backup services. Mission Support may provide backup and restoration job assistance to Students, Staff, or Faculty using Microsoft Backup and Restore or Apple Time Machine tools.

The **IT Services** role is responsible for monitoring the availability of the Essential and Mission Critical services defined in this Plan. IT Services may also support Students in selecting and implementing data backup strategies that meet their needs, using existing services, if possible.

DEFINITIONS

Business Continuity Management Program (BCM), outlines the planning process for developing prior arrangements and procedures to enable the University Colleges, Departments, Units or Research Projects to respond to an event in such a manner that critical business functions can continue within planned levels of disruption. This systematic approach includes policies, procedures, continuity of operations plans COOP), also referred to as business continuity plans (BCP), business impact analysis (BIA), risk assessment (RA), validation and testing, incident identification, and disaster recovery.

Continuity of Operations Plan (COOP), also referred to as a Business Continuity Plan (BCP), a broad plan designed to keep a College, Unit, or Department running, even in the event of a disruption in normal operations, including and up to a disaster. The COOP or BCP is established for the purposes of identifying personnel; resources and location needs before, during and after an event, incident, or disaster. The COOP or BCP document provides core team contact information and responsibilities, essential systems and needs, critical functions, vital records, vendors and dependencies. The COOP or BCP document is intended as a quick reference guide for specific information, but is not intended for

use as standard operating procedures or detailed training materials.

Information System, defined as any and all online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data, including but not limited to, servers, network infrastructure, computers, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment, telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Technology Disaster Recovery Plan (IT DRP), a more focused plan, included in a COOP or BCP, that is narrowed to focus on the data and the information systems of a College, Unit, or Department. The aim of the IT DRP is to save data with the sole purpose of being able to recover quickly in the event of a disaster. IT DRPs are developed to address the specific requirements of IT departments to get back up and running – which ultimately affects the business a whole.

Essential IT Service, defined as a system or service considered critical to the University and included in the OU IT Disaster Recovery Plan. Essential IT Services provide supporting infrastructure to the University and its Mission- or Unit-Critical IT Services. Essential IT Services may include, but are not limited to: OU network infrastructure, data centers, voice and telephony systems, account and identity management services, centralized storage services, virtual hosting platforms, and university messaging and collaboration services.

Mission Critical Service, defined as a system or service considered critical to a university mission and included in the OU IT Disaster Recovery Plan.

Unit Critical Service, defined as a system or service considered to a college, unit, center, institute, or department and included in a department IT Disaster Recovery Plan.

Non-Critical IT Service, defined as a system or service considered to be non-critical and has a Recovery Time Objective of three (3) days or more.

Record, defined by Oklahoma Statutes at 67 O.S. Sec. 203, may take many forms. They include but are not limited to documents, books, papers, photographs, computer disks, electronic mail, video, or audio recordings.

Recovery Time Objective, defined as the maximum time allowed for the recovery of an IT system or service following an interruption.

Recovery Point Objective, defined as the acceptable amount of data loss measure in time.

POLICY

PR.IP-9 INFORMATION TECHNOLOGY DISASTER RECOVERY (IT DR) PLAN

Maintaining an IT DR plan as part of Continuity of Operations Program (COOP) is of key importance to minimize the effects of a manmade or natural disruptive event or disaster. An IT DR plan kept up-to-date and tested on a regular basis allows OU to resume critical functions in a timely and predictable manner.

1. The Office of Information Technology must maintain a written IT DR Plan that address the Office of Information Technology's IT systems so that the effects of a disaster will be minimized, and OU IT will be able either to maintain or quickly resume essential functions.

2. Each College, Department, Unit, or Research Project independently operating or maintaining Information Systems shall maintain a written disaster recovery plan for major or catastrophic events that deny access to department and Cloud or Third-Party hosted Information Systems, for an extended period.
3. Elements of all IT DR Plan(s) will contain:
    a. Elements derived from a COOP, BCP, IT Risk Assessment, or Business Impact Analysis, where available, to systematically assess the potential impact of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from a disruptive event or incident.
    b. Critical internal and external points of contact for personnel who provide or receive data.
    c. Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.
    d. A determination of the Recovery Time Objectives and Recovery Point Objectives.
    e. Dependent information technology systems or services to assess the impact on associated systems or processes.
    f. Existing controls and processes such as backup power, excess capacity, environmental sensors, and alarms.
    g. Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.
    h. Disaster recovery procedures for major or catastrophic events that deny access to Essential and Mission-Critical IT systems or services for an extend period.
    i. Non-critical IT systems must be listed in department/unit-level IT DR Plans and shall have minimal requirements for backup validation testing.
4. IT DR Plans and Procedures must be reviewed and updated at least annually, and more often as necessary, by the Information System Owner.

PR.IP-9 IT DISASTER RECOVERY PLAN TESTING

Periodic testing of the IT DR procedures shall be performed to determine the effectiveness of the procedures and organizational readiness to execute the IT DR Plan. IT DR procedures shall:

1. Be tested following the matrix below:
    a. Essential IT Systems: Every two (2) years
    b. Mission-Critical IT Systems: Every three (3) years
    c. Non-Critical IT Systems: Every five (5) years
2. Tests of the IT DR procedures may include a range of testing methods from virtual (e.g., tabletop) tests to actual events. The tests shall be documented and the results shall be used to update the procedures if necessary. The Information System Owner shall approve the results of the tests and any resulting actions.
3. Provide for testing of backup and/or recovery media to ensure the validity of the recovery media and process.

PR.IP-9 ALTERNATE SITE

An alternate site is an integral part of an IT DR plan. Alternate sites:

1. Should be implemented based on business impact analysis results.
2. Must be geographically separated from the primary storage site to reduce susceptibility to the same disruptive vent.
3. Must be configured to facilitate timely and effective recovery operations.

PR.IP-9 IT DISASTER RECOVERY TRAINING AND AWARENESS

The University must train personnel in their IT DR roles and responsibilities and must provide periodic refresher training.

1. All participants who are required to execute the IT Disaster Recovery Plan must participate in annual IT Disaster Recovery Planning workshops and/or tabletop exercises.

REFERENCES

- National Institute of Standards and Technology Cybersecurity Framework (CSF), PR.IP-9
- National Institute of Standards and Technology Special Publication 800-171, Controlled Unclassified Information, 3.6.1, 3.6.2
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Security Rule, §164.308(a)(6), §164.308(a)(7), §164.308(a)(7)(ii)(D), §164.310(a)(2)(i), §164.312(a)(2)(ii)
- Payment Card Industry (PCI) Data Security Standards
- Gramm-Leach-Bliley Act (GLBA) Safeguards Title 16 I, Subchapter C, Part 314.4(h)
- U.S. Department of Education, Protecting Student Privacy, Data Governance Checklist
- OU HIPAA Policy – Documentation Requirements

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
09/01/2021	0.1	OU IT, April Dickson	Baseline Version
01/20/2022	1.0	OU IT	Revised definitions to include Information System. Added Business Continuity Analyst. Revised Colleges, Units, or Research Projects responsibilities. Added Information System Owner. Added Information System Administrator. Added Cloud/Third-Party hosted infrastructure to Scope. Revised Essential, Mission-Critical, and Non-Critical IT System definitions. Revised Policy Statements – Recovery procedures required for all systems.
02/15/2022	1.0	OU IT HSC Enterprise Risk Business Continuity Analyst	Added COOP and IT DRP definitions. Revised Business Continuity Analyst responsibilities. Revised Disaster Recovery Program Owner responsibilities. Revised University Colleges, Departments, Units, or Research Project responsibilities. Added Business Continuity Management definition.

Table 2 Approval History

Version	Approval Date	Approved by:
1.0	02/08/2022	Information Security Review Board
1.0	02/08/2022	Security Governance Advisory Council
1.0	03/31/2022	University President

Table 3 Review History

Version	Review Date	Reviewed by:
0.1	12/12/2021	Internal Audit
0.1	12/12/2021	Office of Compliance
1.0	02/08/2022	ISRB & SGAC
1.0	02/14/2022	Enterprise Risk and Business Continuity Analyst