Information
Business Continuity and Disaster Recovery

Effective
July 23 2007

Number
ISO 002 v2 0

Applicability
This policy applies to all University workforce faculty and student members including but not limited to faculty staff students temps trainees volunteers and other persons as deemed appropriate while conducting performing work teaching research or study activity using University resources and includes all facilities property data and equipment owned leased and or maintained by the University or affiliates

Administrative Authority
Vice President for Risk Audit and Compliance

Responsible Unit
Information Security Compliance Office
502-852-6692
isopol@louisville.edu

History
This policy is subject to change or termination by the University at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.

Approved July 23, 2007 by the Compliance Oversight Council
Shirley C Willihnganz, Executive Vice President and University Provost, Chair of the Compliance Oversight Council

Revision Date(s):

1.0 / July 23, 2007/ Original Publication
1.1 / January 29, 2013 / Content Update
2.0 / March 3, 2016 / Content review/update removing reference to IT Ops as DR assistance and update to new template
2.0 / June 23, 2022 / Minor edit
Reviewed Date(s): September 24, 2014; March 3, 2016; June 12, 2017; May 18, 2018; April 1, 2021; June 23, 2022; October 15, 2025

Categories

Statement:

Effective business continuity and disaster recovery plans are required in all areas of the University. Each school, unit and division must develop plans that will allow it to perform its core-required operations in an alternative fashion as well as an appropriate disaster recovery policy for their working environment.

Reasoning:

The purpose of this policy is to define planning and related activities to ensure that the University's core, critical or regulatory required functions will either continue or be recovered to an operational state within a reasonable amount of time in the event of an incident or disaster that would otherwise impact the University's ability to conduct operations.

Definitions:

Gap Analysis

A process where the current state vs. the desired state for a process, system or organization is prepared. The differences between the current state and the desired state are called gaps. These gaps then become the basis for prioritization, planning and basis for action to move to the desired state.

Risk Assessment

In disaster recovery or business continuity planning, a risk assessment will typically include:

1. Identification and classification of primary risks and exposures including external and environmental risks as well as inherent business risks.
2. Probability (likelihood) of occurrence.
3. Impact of occurrence including cost and reputation.
4. Strength of existing controls.
5. Consideration of senior management risk tolerance and level of acceptance of identified risks vs. cost of various mitigation plans.

Business Impact Analysis

In business continuity planning, a business impact analysis includes:

1. Identification of critical business processes at departmental/unit level.
2. Risk Assessment including quantification of impact of an event.
3. Identification of points of failure and process interdependencies.
4. Development of recovery time objective (RTO) and recovery point objective (RPO). See definitions of these terms in this document.
5. Degree of criticality and supporting prioritization of processes for recovery.
6. Review and update annually.

Continuity/Recovery Strategy

In disaster recovery or business continuity planning, a continuity and recovery strategy includes these steps:

1. Assess alternate continuity/recovery strategies.
2. Select continuity/recovery strategy.
3. Develop and document continuity/recovery strategy plans.
4. Disaster Recovery Plans as part of a broader Business Continuity Plan should include:
   a. Classification of critical systems and records to ensure priority of recovery.
   b. Mitigation strategies and safeguards to avoid disasters.
   c. Support of RPO and RTO objectives.
   d. Necessary electronic files backup and off-site storage strategy (see IS PS015 Backup of Data).
   e. Security controls equal to those of day-to-day operations.
5. Define organizational responsibilities and critical functions for implementing plans, document, communicate to all involved parties and implement.
6. Off-site storage - which meets University security requirements - for at least one copy of the planning documents.

7. Sufficient and secure off-site facilities for continuation of business, if necessary (see IS PS009 Data Facilities).
8. Annual training and testing of plans to include documented procedures, results and correcting of noted deficiencies.
9. Annual review and revision of the plans.
10. Coordination with central ITS disaster recovery strategy, if applicable.

Disaster Recovery Maintenance and Awareness Program
Process includes:

1. Conduct education and awareness training with personnel.
2. Perform periodic BCP plan walkthrough and testing.
3. Review and update plans and documentation annually or per testing deficiencies.

Responsibilities:

Policy Authority/Enforcement: The University's Information Security Officer (ISO) is responsible for the development, publication, modification and oversight of these policies and standards. The ISO works in conjunction with University Leadership, Information Technology, Audit Services and others for development, monitoring and enforcement of these policies and standards.

Policy Compliance: Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the University and/or action in accordance with local ordinances, state or federal laws.