

POLICY

Business Continuity Management Policy

ISSUED ON 11/16/2022

Resiliency and effective response to events that may impact the University's ability to achieve our business objectives is critical to the organization. These objectives include safeguarding human and capital assets, cash flow, brand reputation, and the best interests of the community and our stakeholders. The preparedness for, response to, and recovery from such events significantly influences the confidence and trust of board members, patients, students, and the community.

The objective of a business continuity management program is to develop and implement plans that ensure expeditious response, continuity, and recovery of critical business functions or services during and after an incident. An incident is defined as an occurrence or event, natural or human-caused that requires the activation of business continuity plans to protect life or property, continue critical services, or resume normal activities.

Business continuity is a critical component of the University's risk management portfolio. It includes four disciplines. Each has a specific area of focus, but many times overlap and have interrelated activities and dependencies.

- **Emergency preparedness planning:** the planning for, and response to localized emergencies.

- **Crisis management:** the coordination of resources to mitigate the impact of significant emergencies or crises.
- **IT disaster recovery:** the recovery of electronic systems or data.
- **Business resumption:** the processes implemented to maintain or restore the organization to its pre-incident state.

Business continuity plans shall be developed and documented for the critical business functions identified in the business impact analysis conducted throughout the University.

Business Continuity Requirements

1. The Business Continuity Management Program (BCMP) is responsible for the systematic and consistent assessment of the state of business resiliency planning across the University, and for regularly reporting the status of same to senior management.
2. Departments will identify and analyze the risks to their critical processes and locations. Documented response and recovery plans are required for all critical functions, IT systems, and locations delivering processes where an interruption to the normal delivery would have a **significant** impact on the university.
3. Departments are responsible for developing, testing, and approving their continuity plans.
4. Emergency preparedness plans must provide for timely and coordinated management of an incident to expedite resumption of normal services and minimize

impact.

5. Business resumption plans must have content explaining how to deliver critical processes or outputs in the event of significant interruptions including staff absences, IT System interruptions, inability to access normal facilities or an interruption to services and resources provided by internal and external suppliers and/or partners. These plans must be actionable, should be tested annually, and must be approved by appropriate management. Plans must be updated to comprehend organizational and process changes as they occur.
6. Disaster recovery plans must provide for information technology resources to be available within the defined timeframes determined by the business.
7. Division functional groups (Environmental, Health, and Safety; Human Resources; Information Technology; Facilities, etc.) will be engaged by the business units to effect appropriate coordination related to emergency preparedness planning, crisis management, IT disaster recovery, and business resumption plans.

Business Continuity Responsibilities

BUSINESS CONTINUITY PROGRAM

- Maintain business resumption planning tools, reporting systems, and processes necessary to comply with the Business Continuity Management policy.
- Engage and train business continuity focal points in the disciplines of business continuity.

- Assist with post Incident assessments, when necessary, in conjunction with the business units and information security management.
- Promote the integration of business continuity efforts across the University.
- Facilitate communication among members of the business continuity community through the governance and steering committees.
- Reporting on the overall status of business resumption planning to senior management as required.

GOVERNANCE COMMITTEE

- Facilitate identification of department's critical processes and/or locations.
- Support and/or participate in management reviews to communicate business continuity status and action plans.
- Serve as a liaison between the BCMP and departments.
- Assist BCMP with ensuring response/recovery/resumption plans are developed.
- Provide advice regarding significant changes to policies and disseminate those changes.

DEPARTMENT MANAGEMENT

- Assign business continuity planning responsibilities to employee(s) within their

departments who will be identified as the business continuity management liaisons.

- Champion the identification of critical business processes and locations within their departments.
- Accountable for the department's compliance with this policy.

BUSINESS CONTINUITY MANAGEMENT LIAISONS

- Participate in a business impact analysis to identify critical business functions and associated risks if the functions are compromised. Business functions within business units shall be classified based on the following impact factors:
 - Life safety/patient health
 - Financial (loss of revenue)
 - Brand/organizational reputation
 - Compliance/regulatory
 - Loss of productivity
 - Employee morale and retention
- Document and update departmental continuity plans.
- Ensure plans
 - Address the risks and potential impacts of a disruption.

- Include response and/or recovery strategies.
 - Define roles and responsibilities of key personnel that need to be involved in the response to a disruption.
 - Include strategies to effectively communicate steps to notify, respond, and recover.
 - Provide that they are to be tested on an annual basis with realistic scenarios to test the plan and team's response to identify gaps and take corrective actions to improve the plan.
- Manage all business continuity plans in the approved content management system.

EMPLOYEES

- Follow directives provided in applicable continuity plans. This may include responsibilities such as keeping their contact information up-to-date with department supervisors and, if provided in the departmental plan, taking home a University-assigned laptop at the end of each working day to enable remote work in the event the employee's University office becomes inaccessible due to an emergency.

Appendix 1: Definitions

Business Continuity: An ongoing process to ensure that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.

Business Continuity Planning: Processes and procedures that enable the University to respond to an event so that critical business functions continue with acceptable levels of performance.

Business Continuity Management Program (BCMP): A program that manages the Business Continuity governance process by providing a policy, consultation, training, tools, and status reporting to the BCM governance committee.

Business Impact Analysis: Process that identifies, quantifies, and qualifies the impacts resulting from interruptions or disruptions of an entity's resources.

Emergency Preparedness Planning (EPP): The discipline that ensures the University's readiness to respond to an unexpected or unwanted event of a safety, health, or environmental nature that calls for immediate action at a specific location. These plans also include the coordination of resources to mitigate the impact of significant emergencies or crises. Each location is required to have access to the Emergency Preparedness Plan.

Business Resumption Plan (BRP): Documented processes and procedures, and recovery strategies developed to protect and restore critical business operations in the event of an interruption. The primary objective is to minimize the negative effects of a disruption, and restore the business processes and related sub-processes to normal operations.

IT Disaster Recovery (DR): The activities and plans are designed to both restore the University’s information and communication systems to an acceptable condition; and, to minimize loss of data in the event of a major interruption in services.

Appendix 2: Contact Information

Please address any questions or concerns with any policies set forth within this document to the University of Rochester Business Continuity Program Office (avincent@safety.rochester.edu (<mailto:avincent@safety.rochester.edu>))

Appendix 3: Revision History

Modification(s) Made	Modified By:	Date of Modifi cation	Approver	Approv al Date	

Document Created	Business Continuity Program Director	08/21/2017			
Content updated for program startup	Business Continuity Program Director	6/15/2021			
Content updated for program development	Business Continuity Program Manager	7/14/2022			

ABOUT THIS POLICY

Policy Applies To

Staff

Policy Number

0BCM02

Issuing Authority

Administration & Finance

Responsible Officer

Mike Liberty

Contact Information

mliberty@safety.rochester.edu ([mailto: mliberty@safety.rochester.edu](mailto:mliberty@safety.rochester.edu))

RELATED POLICIES

[Business Continuity Management Governance Policy \(https://www.rochester.edu/policies/policy/business-continuity-management-governance-policy/\)](https://www.rochester.edu/policies/policy/business-continuity-management-governance-policy/)