DEPAUL UNIVERSITY

Business Continuity Management Policy

Category: Operations
Responsible Department: Office of the Executive Vice President
Responsible Officer: Executive Vice President
Effective Date: 10/13/2021

Policy Summary

The purpose of the Policy is to provide reasonable, but not absolute, assurance that DePaul's business will continue as soon as possible after any incident that disrupts some or all of the university's essential business operations. The Policy is aligned with and subservient to DePaul's Emergency Procedures& Communication Policy.

The Policy defines the ongoing management process that each university unit completes to:

- identify potential threats which could cause a break in operations;
- implement cost-appropriate actions to mitigate the likelihood and/or severity of a threat;
- design an effective plan that recovers lost business functions with minimal downtime and safeguards the reputation of the university and its stakeholders; and
- confirm the capability of the unit to implement the plan.

Scope

This policy affects the following groups of the University:

- Hiring/Supervising Managers
- Executive Offices
- Assoc. / Assist Vice Presidents
- Full-Time Staff
- Part-Time Staff
- Full-Time Faculty
- Part-Time Faculty
- Budget Managers
- Student Employees
- Vice Presidents
- Deans
- Directors/Department Chairs
- Full-time Employees covered by a Collective Bargaining Agreement

- Temporary Staff

Academic and Administrative Officers are responsible for ensuring compliance with the Policy throughout their respective units and for completing the actions prescribed by the Policy. Executive Officers are responsible for ensuring compliance with the Policy in their respective offices and for their leadership roles and completing the actions prescribed by the Policy.

All employees of DePaul University are required to be aware of their unit's business continuity plans, their individual responsibilities if a plan were invoked, and how to access the resources - including other employees, information, and/or materials - needed to carry out their responsibilities.

Out of the scope of this policy are:

- Emergency response plans (defined by the Emergency Procedures and Communications Policy),
- Crisis management and crisis communications plans, and
- Disaster recovery plans (developed by Information Systems and Facility Operations).

Policy

Any number of incidents - from minor equipment malfunctions to life-threatening emergencies such as natural disasters or malicious attacks - can disrupt DePaul's normal activities and essential business functions. Effective incident response protocols may permit the organization to minimize an incident's adverse effects on the safety and welfare of individuals and property; restore critical operations; manage communications and protect the university's reputation and assets; and expedite the return to normal activities and operations.

This policy is aligned with and subservient to DePaul's *Emergency Procedures and Communications Policy* and the *DePaul University Emergency Operations Plan: Loop and Lincoln Park Campuses*. As defined by these documents, each unit will develop emergency information appropriate for the characteristics of their unit.

The focus of this policy is business continuity management. This policy defines the ongoing management process and procedures that each unit follows to:

- identify and prioritize essential business functions
- identify potential threats which could cause a break in their operations;
- implement cost-appropriate actions to mitigate the likelihood and/or severity of threats;
- design an effective Business Continuity Plan (BCP) that defines strategies to restore lost business functions with minimal downtime and efficiently return to normal operations; and
- confirm the capability of the unit to implement the plan.

Academic and Administrative Officers are responsible for their unit's compliance with the policy. Executive Officers are likewise responsible for ensuring compliance with the Policy in their respective offices and for their leadership roles in supporting university completion of the actions prescribed by the Policy. Academic and Administrative Officers have the responsibility to address

business continuity management for their unit as a whole. They also are responsible for ensuring that subunits complete the process for their essential business functions.

Execution of the Business Management Process and all outcomes of the process must comply with all DePaul policies. This includes but is not limited to:

- Faculty inclusion in all steps in the process as specified by faculty governance in the *Faculty Handbook*, and
- Amending existing policies that require provisions for specific recovery situations.

The tangible outcome of complying with the policy is the development, approval, storage, and ongoing maintenance of a BCP. The unit's Academic or Administrative Officer documents their approval on the first page of the BCP with the name and title of the Officer and the approval date.

Once the Academic or Administrative Officer approves a unit's BCP, the unit must regularly review and update the plan, train faculty and staff and exercise portions of the plan:

- Annually review each BCP to check that it is up-to-date and complete. The unit's Academic or Administrative Officer must approve each update to the BCP, with the name of approver and date documented on the first page of the BCP.
- Annually update faculty and staff on changes to the BCP and refresh their understanding of the plan. Annually train new faculty and staff on the plan. Training is confirmed by employees during a Quality Assurance Review.
- Every two years a unit must exercise a portion of the plan using a table-top exercise or drill. Document and retain an exercise assessment that summarizes the result of the exercise and informs future BCP updates.

Procedures

REPOSITORY FOR UNIT BUSINESS CONTINUITY MATERIALS

All unit materials supporting Business Continuity Management must be stored in a repository that ensures reliable and timely access in the event of a disruption. Since BCPs may contain information about DePaul's internal business processes that is confidential in nature the repository must also have access control. Information Services supports two repositories with these features. Each repository requires a Campus Connect logon. The decision of which repository to use resided in the unit executing the process. The options are:

- DePaul Knowledgebase wiki: https://knowledge.depaul.edu Business continuity related documents stored in the DePaul Knowledgebase should be in a space named "Business Continuity Plan - <unit name>."
- DePaul OneDrive: https://depauledu-my.sharepoint.com/:f:/g/personal/eshanah2_depaul_edu/Egn9n42g_MhAo9XgIFjh-Z0Bo1xXurzyjVxDZP-R2Jo0kg Business continuity related documents stored in OneDrive should be in a folder named "Business Continuity Plan - <unit name>."

Each repository also contains resources for executing the Business Continuity Management process including templates for accessing, creating, storing and maintaining BCPs; background on business

continuity management; and materials to support employee training and plan testing. The resources are posted in:

- For DePaul Knowledgebase wiki: https://knowledge.depaul.edu/display/BCM/Business+Continuity+Management+Resources+Home
- For OneDrive: https://depauledu-my.sharepoint.com/:f:/g/personal/eshanah2_depaul_edu/Egn9n42g_MhAo9XgIFjh-Z0Bo1xXurzyjVxDZP-R2Jo0kg.

BUSINESS CONTINUITY MANAGEMENT PROCESS

Units must complete a six-step process and annually review each step to ensure currency of plans and the unit's ability to execute the plans. Faculty and/or staff responsible for essential business functions of their unit must be engaged in all steps in the process:

1. *Conduct a Business Impact Assessment (BIA):* Analyze the unit's work flows to:

   - Prioritize the unit's business functions.
   - Identify, document, and communicate interdependencies with other units or among functions within a unit.
   - Document contractual, regulatory and legal requirements for the business functions.
   - Establish maximum allowable downtime and recovery time objectives (RTOs) for each function.
   - Establish acceptable level of losses and recovery point objectives (RPOs), defining the point that a process will be restarted.
   - Identify the critical paths and dependencies for restoring a prioritized business function.

   The outcome of the BIA is a prioritized listing of the key business functions in the unit This listing is retained in the DePaul Knowledgebase with the unit's business continuity materials.

2. *Conduct a Risk Assessment:* Numerous natural disasters, technical disruptions or human-initiated incidents can affect the ability of a unit to deliver normal business functions. Each unit shall determine which risks have the greatest likelihood of occurrence and/or most severity of impact on the unit. These risks are reviewed to identify common effects, such as personnel are unable to perform functions, facilities are not available or information access is disrupted.

   The outcome of the Risk Assessment is a listing of the risks highlighted and the impacts the unit reasonably foresees encountering. This listing is retained in the DePaul Knowledgebase with the unit's business continuity materials.

3. *Develop Risk Reduction Strategies:* Based on the risk assessment, the unit will consider preemptive options for decreasing the likelihood of occurrence and/or decreasing the severity of the impact if an incident occurs.

   The outcome is an action plan for implementing practical strategies.

4. *Develop a Business Continuity Plan:* Based on the risk assessment findings and business impact analysis, develop plans for the unit's response and recovery of essential business functions for the risks that are most likely and/or most severe. A BCP template is provided.

    The BCP includes:

    - o the essential functions performed by a unit and the order for restoring these functions, recognizing the prioritization among functions, time demands for functions, critical paths within functions, and outside dependencies;
    - o succession plans for individuals in leadership role or with specialized expertise;
    - o alternatives for needed facilities, equipment, or supplies; and
    - o a collection of procedures and work instructions.

    All BCPs must be compliant with DePaul's policies. If the planning process identifies response situations that would be non-compliant with an existing policy, amend the affected policy to incorporate provisions for disruptions.

    The outcome is a BCP, approved by the unit's Academic or Administrative Officer and stored in the DePaul Knowledgebase with all accompanying documentation.

5. *Training and Communications:* All employees shall receive communications on the existence of and location of their unit's BCP. All employees who would have new or expanded roles if the BCP were invoked shall receive training appropriate for their additional responsibilities.

    The objective is that

    - o all faculty and staff are aware of the BCP and how to access the plan
    - o all faculty and staff who have a role during a recovery have participated in at least one BCP training session. Employees confirm training during a Quality Assurance Review.

6. *Evaluate the Plan's Effectiveness:* Every two years each unit shall conduct a tabletop exercise simulating a specific disruption. This exercise will serve as a practice for faculty and staff who must implement the plan and confirm that the robustness of the plan for that incident.

    The outcome is a summary statement of the exercise, and if appropriate, an action plan that identifies updates for the BCP or modifications to training. This document is presented during a Quality Assurance Review and retained in the DePaul Knowledgebase with the unit's business continuity materials.

Divisional Collaborations

Collaborations include:

- DePaul Public Safety, particularly the Assistant Director Emergency Management and the Associate Director Emergency Management;
- Information Services, particularly the Director of Infrastructure and the Director of Information Security; and

- Compliance and Risk Management.

Contact Information

Office of the Executive Vice President
evp@depaul.edu
(312)362-6695

Appendices

Background information, including the DePaul Business Continuity Management Overview and the Business Continuity Plan Template is located in the DePaul Knowledgebase.

History/Revisions

Origination Date: 12/06/2017
Last Amended Date: 10/13/2021
Next Review Date: N/A