### Executive Summary

### Purpose and Scope for a Unit Business Continuity Plan (BCP)

### Resumption Planning

### Assumptions while BC Planning

### Conducting the Planning Project

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organize the Project</td>
<td>5</td>
</tr>
<tr>
<td>Conduct Business Impact Analysis (BIA)</td>
<td>5</td>
</tr>
<tr>
<td>Conduct Risk Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Develop Strategic Outline for Recovery</td>
<td>5</td>
</tr>
<tr>
<td>Review Onsite and Offsite Backup and Recovery Procedures</td>
<td>6</td>
</tr>
<tr>
<td>Select Alternate Facility</td>
<td>6</td>
</tr>
</tbody>
</table>

### Writing and Testing the Plan

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop Recovery Plan</td>
<td>6</td>
</tr>
<tr>
<td>Test the Plan</td>
<td>6</td>
</tr>
</tbody>
</table>

### Maintaining and Auditing the Plan (Ongoing)

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain the Plan</td>
<td>6</td>
</tr>
<tr>
<td>Perform Periodic Audit</td>
<td>6</td>
</tr>
</tbody>
</table>
**Executive Summary**

Business Continuity (BC) is an all-encompassing term-of-art, and in this context refers to any operation or function performed in support of activities related to loss prevention and incident damage mitigation, response to a crisis, resumption of critical business functions, and technical disaster recovery. It is the ability of an organization to provide service and support for its community and to maintain its viability before, during, and after a disruptive event.

Indiana University recognizes the importance of functional units developing and maintaining business continuity and resumption plans, in order to develop a strategy for anticipating and minimizing the severity and the length of serious disruptions affecting operations. Consider a fire that may render an entire department office area inaccessible. The incident may cause a need to replace office space, supplies, desks, information, paper forms, computers, phones, staff and staff expertise, etc. Organizational units should know in advance what of their functions are critical for the University given the specific date of the incident as compared to the University business calendar; what assets are critical to each of those functions, and from where those resources will be obtained if they must be replaced. Many different support departments will be involved to 1) help a department identify needs, and 2) satisfy some of those needs if a resumption plan should be invoked.

The Business Continuity Planning (BCP) function, under the auspices of the Emergency Management & Continuity division of the [Office of] Public Safety and Institutional Assurance, will be the primary coordinating point for assisting/advising each unit with their continuity/resumption planning efforts. The team will develop a general planning capability by identifying, collecting, and organizing information and tools, assisting units in actual planning, and facilitating storage and periodic review of unit plans.

The Business Continuity Planning process and its associated documents are to be considered as a ‘living process’ that will evolve with the input and guidance of the Indiana University community.

**Purpose and Scope for a Unit Business Continuity Plan (BCP)**

Severe disruptions to operations can result from a variety of situations: natural disasters such as tornados or flood, broad equipment failures, process failures, mistakes or errors, and from malicious acts such as arson, computer attacks, sabotage by a disgruntled employee, etc. While the unit may not be able to prevent these from occurring, planning enables the unit to resume essential operations more rapidly than if no plan existed.

Loss prevention planning has to do with mitigating risk: reducing the probability of an event occurring at all, and with reducing the potential damage if an event does occur. This type of planning includes such activities as providing for data back-ups and remote storage, ensuring passwords are strong and remain confidential, ensuring operating systems remain secure and free of viruses, ensuring that multiple individuals are trained in certain critical functions, installing monitoring for mistakes (human errors or computer bugs), using fire- and waterproof safes, etc.

**Resumption** consists of two phases: a process

1) that focuses on quick temporary resumption of critical time-sensitive services and operations, then over time

2) to provide complete ‘restoration’ – getting back to normal

Critical services and operations, if lost, are defined as ones that have the most impact on financial conditions of the department or university – financial exposure, extraordinary expenses, negative public image, poor customer relations or the inability to provide products or services. A systematic resumption plan does not focus unit efforts and planning on each type of possible disruption. Rather it looks for the common elements in any disaster: i.e., loss of information, loss of personnel, loss of equipment, loss of access to information and facilities, and seeks to design the contingency program around all main activities the unit performs.

The associated plan will specify the set of actions for implementation for each activity in the event of any of these disruptions in order for the unit to resume doing business in the minimum amount of time. As a subset of
resumption planning, *disaster recovery planning* usually refers to guidance developed for restoring and stabilizing the organization’s critical technology support components.

**Resumption Planning**

Resumption Planning consists of three principal sets of activities.

1. **Identifying possible disruptions** that might occur, severely hindering or halting critical unit operations
2. **Identifying common impacts and affects** of those possible disruptions
3. **Developing and documenting responses and contingencies** to those affects, so that recovery from interruptions can occur as quickly as possible

Thus, the product of a **Unit Business Continuity (Resumption) Planning Project** is a plan that:

- Determines and documents **critical functions and processes**, along with tolerable lengths of unavailability
- Determines and documents the **resources** (people, systems, equipment, space, partners, other processes (mail service, transportation, etc.) **required to support those critical functions and systems** under normal circumstances
- Eliminates or reduces the needs to develop, test, or debug new procedures, programs or systems while attempting to replace normal functions with alternate ones
- Identifies and documents **single points of failure in critical functions** (e.g., dependence on the involvement of any specific person or piece of equipment in the critical function)
- Determines and documents **alternate methods** (automated or manual) **to perform critical functions**, along with sources of resources required to support those alternate methods
- **Minimizes the number of ad hoc decisions** that must be made immediately following a severe disruption
- Provides for the **timely notification of appropriate unit and university officials** in a predetermined manner as the severity of the interruption or the duration warrants
- Identifies and documents **the people, skills, resources and suppliers needed to assist in the process of resuming critical operations in an alternate mode**.
- Determines and documents **the people, skills, resources, suppliers required to resume the critical functions and operations in a normal mode**.
- Addresses the **need to maintain the currency of the plan’s** information over time.
- Addresses **testing the documented procedures** to ensure their completeness and accuracy.

**Assumptions while BC Planning**

The following assumptions, coupled with the risk analysis findings, define the boundaries around the BC planning process. These assumptions will be refined, deleted, or new assumptions added as planning progresses.

- Recovery for anything less than complete destruction will be achievable by using the plan.
- Normally available staff members may be rendered unavailable by a disaster or its aftermath, or may be otherwise unable to participate in the recovery.
- Normally available space (and file and information stored in that space) may be unavailable.
- Procedures should be sufficiently detailed so someone other than the person primarily responsible
for the work can follow them.

- Recovery of a critical subset (recovery workload) of the unit’s critical functions during the recovery period will allow the unit to continue critical operations adequately.
- A data center disaster may require departments/units to function with limited automated support and some degradation of service.
- For critical computer systems, the writing of special purpose programs may be required to enable the university department/unit to effectively return to normal conditions. That is to say departments/units may need to first rebuild and/or re-enter data that was lost between the time of the last off-site backup and the time of the disaster/disruption; and secondly, enter transactions that accumulate during the period of ”no automated support”.
- Unit plans typically will not need to deal with the availability of electrical power and other utilities. Physical Plant handles this level of planning for the campus.
- Unit plans typically will not need to deal with campus-level networking issues. University Information Technology Services (UITS) handles this level of planning for the campus.
- Unit plans typically will not need to deal with temporary or permanent space availability. University Real Estate and/or campus Space Management will have to find temporary space. However, unit plans must consider the fact that normal space (and data, files, computers in that space) may be unavailable.
- Unit plans typically will not need to deal with process and procedure planning requirements for global university services including but not limited to [examples] FMS – payroll, accounts receivable/payable; HR – benefits/employment, etc. Financial Management Services and IU Human Resources will handle this level of planning for the campus.

Conducting the Planning Project

Information Gathering

Organize the Initiative
The scope and objectives of the plan and the planning process are determined, 1) a coordinator appointed, 2) the project team is assembled, and 3) a work plan and schedule for completing the initial phases of the project are developed.

Conduct Business Impact Analysis (BIA)
Critical business processes (and supporting equipment, staff, systems and applications) are identified and prioritized. Interruption impacts are evaluated and planning assumptions, including the physical scope and duration of the outage, are made.

Conduct Risk Assessment
The physical risks to the unit are defined and quantified. The risks identify the vulnerability of the critical processes, by identifying physical security, backup procedures (staff and data) and/or systems, data security, and the likelihood of a disaster occurring. By definition Risk Assessment is the process of not only identifying, but also minimizing the exposures to certain threats, which an organization may experience. While gathering information for the Business Continuity Plan, system vulnerability is reviewed and a determination made to either accept the risk or make modifications to reduce it.

Develop Strategic Outline for Recovery
Recovery strategies are developed to minimize the impact of an outage. Recovery strategies address how the critical functions, identified in the Business Impact Analysis (step 2), will be recovered and to what level resources will be required, the period in which they will be recovered, and the role central University resources will play in augmenting or assisting unit resources in affecting timely recovery.
The recovery process normally consists of these stages:

1. Immediate response
2. Environmental restoration
3. Functional restoration
4. Data synchronization/restoration
5. Restoration of business [unit’s daily critical operational] functions
6. Interim site
7. Return home

Review Onsite and Offsite Backup and Recovery Procedures

Vital records required for supporting IU department/unit critical functions/operations, systems, data center operations, and other priority functions as identified in the Business Impact Analysis, are verified, and procedures needed to recover them and/or to reconstruct lost data are developed. In addition, procedures to establish and maintain offsite backups are completed and/or reviewed. Vital records include everything from the libraries, files, and code as well as forms and documentation.

Select Alternate Facility

This item addresses determining recovery center requirements, identifying alternatives and making an alternative facility, site recommendation/selection. Departments/units, working with Space Management and/or University Real Estate, will be expected to identify the types of space and the contents needed if alternative facilities are utilized on a temporary or permanent basis. Consideration should be given to the use of University resources as alternative sites before seeking outside solutions.

Writing and Testing the Plan

Develop Recovery Plan

This phase centers on documenting the actual recovery plan. This includes documenting the current environment as well as the recovery environment and action plans to follow at the time of a disaster or severe disruption, specifically describing how recovery (as defined in the strategies) for each critical service or function is accomplished.

Test the Plan

A test plan/strategy for each critical service or function as well as the operating environment is developed. Testing occurs on the plans and assumptions made for completeness and accuracy. Modifications occur as necessary following the results of the testing. This portion of the project is perpetual for the life of the plan.

Maintaining and Auditing the Plan (Ongoing)

Maintain the Plan

This includes maintaining the plan to keep pace with the changing environment, personnel, procedures, and practices.

Perform Periodic Audit

This addresses periodically reviewing the Unit Business Continuity Plan to ensure that it continues to reflect the organization’s needs.