(Please insert services and subservices)

Departmental DR Plan

(Please insert today’s date)

Disaster recovery planning involves the process, policies, and procedures that enable delivery of critical technical services to Indiana University in the event of natural or man-made disaster.

Disaster recovery (DR) is an integral part of the overall business continuity program. While business continuity is concerned with continuation of the business of the university, disaster recovery or information technology business continuity is focused on the continued operation and function of technology to support those business functions.

A disaster recovery program ensures the technology that supports the business of the university will continue to function after an event occurs. The purpose of this document is to help departments form a disaster recovery plan. Many services hosted by university departments are key in conducting daily university business; as such, plans for these services to provide continued functionality in the event of disaster is paramount.

The Indiana University Data Centers provide faculty and staff with the necessary equipment and networking capability to support the most critical university functions. With these data centers, Indiana University is capable of meeting predetermined recovery windows that will allow the university’s most critical functions to continue even in a worst case scenario.

Critical systems / applications are determined by the need of the university. Departmental staff should identify and prioritize systems and applications by their necessity to maintain the ongoing operation of the university.

**General Info**

1. Department
2. Person providing recovery information
3. Provide a list of all services required to keep your department operational (e.g., file servers, web services, physical controls)

Please include any subservices that may be critical to support these services (e.g., network, HVAC, alarm systems)

            1) Service name:

            2) Service name:

            3) Service name:

            4) Service name:

            5) Service name:

1. Locations of services (data center, cloud service, local)

**Service(s) Info**

1. Services

Provide general descriptions of services, including function and university audience.

List service subcomponents in order of importance to university operations, with the most important first.

Example: Student Information Systems contain multiple subcomponents: Financial Aid, Student Loans, Registration, and Grades

a)

b)

c)

d)

e)

1. Dependencies
   1. Personnel resources. What departmental IT units or UITS units would you depend on to provide staff to recover your services?
   2. Provide a detailed list of hardware and software required to support your services. Provide an architecture diagram of components and their interactions as a separate document in your DR folder.
2. Interfaces

What other technical services/applications do your services interact with for reading, sending, or receiving data?

**Recovery Info**

1. Overview of recovery strategy
2. Business impact. What tools and resources are impacted when the service is unavailable?
3. Impact of unavailability of services to customers. How much time can pass before your customers are negatively impacted by not having access to the resources in 8a?
4. Recovery Strategy. What high-level steps will you use to reinstate your services?
5. Details of recovery. For this section please assume one UITS computer facility is available at either Bloomington or Indianapolis.

* Some recovery information may be the responsibility of UITS or an external vendor.

Note: Do not assume individuals using this document understand your service's architecture, hardware, or software; be specific in your recovery information.

* 1. Outline any assumptions regarding the technical environment in which your services will be housed for this recovery effort.

Example: If you are assuming the network or ADS will be available prior to the recovery of your services, state those assumptions in this section.

* 1. Outline any assumptions about the staff’s technical knowledge that will be required in recovering your services.

Example: If you assume involved staff have certain expertise such as detailed understanding of Linux operating systems, state those areas of required expertise in this section.

* 1. Identify what duplicate services are available now in your target recovery facility to support the recovery process.

Example: Your production application host data center is at the Bloomington location. If the Bloomington computer facility is unavailable, equivalent equipment at the Indianapolis location will be used for production recovery.

* 1. Identify the order of recovery for each component inventoried in the technical architecture section of this document under 6b for hardware and software.
* Indicate dependencies between components.
* Indicate what components may be recovered in parallel by using duplicate numbers in the “order installed” column as found in the example below.
* Indicate which UITS or IU service area will be responsible for the specific components. See example below:

Examples:

**Component name Order installed Dependencies Area responsible**

Server hardware installed or re-located 1 SAV team

VMware installed 2 after hardware SAV team

Connectivity confirmed

Restore operating system 3 ESA & SAV teams

* 1. If you are leveraging vendor documentation, please include copies as supporting documents with your DR folder and list document titles where appropriate below.
  2. Identify the detailed steps involved in recovering your services from the ground up back to normal service levels. Include the following:
* Outline what each step entails, in detail.
* If you are attaching additional documents for detailed recovery steps, record those document titles in this section. Additional documents may originate from your area, UITS groups, or external organizations.

Note: Documentation can be attached to this template or filed separately in your DR folder.

Example: If your service calls for recovering a database, provide specific written instructions on how to recover the database.

* 1. Data backup/recovery
  2. Based on your recovery details, outline your current data backup/recovery strategies.
  3. If there are times when your “Point in Time” recovery could result in lost data, explain those situations.
  4. If data is lost, please explain the impact on your users.

1. Time required to recover

Estimate how much time it will take to recover the services.

Information in section 9, “Details of recovery,” should state what tasks are being done during this time, even if the recovery time spans weeks or months.

* 1. Indicate time in hours, days, weeks, and/or months.

**Exercise Plan**

1. Outline what methods are in place to exercise your recovery plans to confirm they will function in an actual recovery situation.

* Be very specific on steps for testing, areas involved, and detail on how testing will be performed.

1. Perform IT risk management to identify, assess, and address risks appropriately for IT systems.

* Assess significant risks that would result in an extended outage to your service.
* Evaluate risks, where appropriate, for each hardware and software component that is part of your service as listed earlier in your DR plan.
* Don’t overstate what you already have set up or understate what you plan to do in the future. Please be truthful with the risk management information you provide. Providing accurate information will enhance your risk management assessment.

Identify potential risks, risk impact, risk controls, risk probability, risk magnitude of impact, risk action, and risk control enhancements.

* IT risks are composed of natural, environmental, or man-made (intentional and unintentional) threats that exploit vulnerabilities in a system.
* Risk impact should explain how tools, resources, or data are affected by the risk. It is similar to the business impact when your service is unavailable as listed earlier in your DR plan.
* Risk controls are technical systems, management systems, or other systems that reduce the probability or impact of a risk. Duplicating service hardware and software at both the Bloomington and Indianapolis data centers is an example of a control enhancement that would significantly reduce the impact of a risk.
* Use the table below to determine risk probability. When determining each threat’s probability, consider its reason for happening.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk probability table** | | **Probability of natural threat,**  **environmental threat, or**  **human threat** | | |
| **Low** | **Moderate** | **High** |
| **Effectiveness of controls** | **High** | Low | Low | Moderate |
| **Moderate** | Low | Moderate | High |
| **Low** | Moderate | High | High |

* Use the following to determine the magnitude of impact.
* High: Risk may result in highly costly loss of high profile tangible assets or resources plus significantly violate, harm, or impede an organization’s mission, reputation, or interest.
* Medium: Risk may result in costly loss of tangible assets or resources plus violate, harm, or impede an organization’s mission, reputation, or interest.
* Low: Risk may result in some loss of tangible assets or resources plus noticeably affect an organization’s mission, reputation, or interest.
* Now that you have determined your magnitude of impact and risk probability, the next step is to use the magnitude of impact and probability to determine your risk action. Use the following to determine risk action.
* Low impact with low risk probability – Accept risk, no action required.
* Low impact with moderate/high probability – Avoid risk, add controls or restructure your service so the risk is avoided.
* Moderate/high impact with low risk probability – Share risk, share the responsibility of reducing the probability and impact of the risk with other related services.
* Moderate/high impact with moderate/high probability – Reduce risk, add controls to reduce the probability and impact of the risk.

The above method to determine your actions is similar to a ‘heat map’. A heat map is used to decide what type of risk action would be the best way to respond to the risk.

(IU’s risk management strategies are based upon the Committee of Sponsoring Organizations enterprise risk management framework. Information contained in the risk management instructions references the following:

Indiana University Office of the Executive Vice President for University Regional Affairs, Planning, and Policy. *Enterprise Risk Management (ERM) Strategy*. )

Examples:

1. Risk description: Hacker bypasses server’s security and has unauthorized access to server.

Risk impact: Confidential or sensitive data could be compromised.

Risk controls:

1. Card-key access is required to have physical access to server.
2. CAS authentication is required for users to connect to server.
3. OTP authentication is required for users to connect to server.

Risk probability: Moderate

Risk magnitude of impact: High

Risk action: Reduce risk.

Planned control enhancements: All confidential and sensitive server data will be encrypted in the coming months.

1. Risk description: Broken cooling pipe floods housing data center and damages server.

Risk impact: Server’s services are unavailable.

Risk controls: There are no controls to prevent this risk.

Risk probability: Moderate

Risk magnitude of impact: High

Risk action: Reduce risk.

Planned control enhancements: Add an enhanced drainage system to housing data center during the next year.

For each risk to your services, fill in the following as shown in the examples:

1. Risk description:

Risk impact:

Risk controls:

Risk probability:

Risk magnitude of impact:

Risk action:

Planned control enhancements:

.