Criticality Levels

Criticality levels are determined by the service owner and are used to classify the criticalness of an IT system* to a business process. The level selected defines the necessary business continuity procedures, methods, and testing requirements.

Core Infrastructure: IT systems that must be functioning and are considered core components, which will need to be operational before other dependent systems can perform as they are intended. Examples of core systems include, but are not limited to; electricity, the data network, network services such as DNS and DHCP, and various authentication systems such as Active Directory. Immediate recovery is required to prevent substantial interruption of University operations. Systems should have a maximum downtime of 2 hours or less.

Critical: IT systems which are essential to support University business operations. Loss or failure of these systems will have an extreme impact on business operations. Systems should have a maximum downtime of 4 hours or less.

High: IT systems which are crucial to support primary University business operations. Loss or failure of these systems will have a significant impact on business operations. Systems should have a maximum downtime of 24 hours or less.

Medium: IT systems which are important to University business operations. Loss or failure of these systems will have a modest impact on business operations. Systems should have a maximum downtime of 72 hours or less.

Low: IT systems which improve the effectiveness or efficiency of University operations. An extensive loss or failure of these systems will have a negligible impact on business operations.

**An Ivlch()][4254.33 Tm[]Tm[]4(g)amo p drdwothe*

Business Impact Analysis (BIA)

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system was unavailable.

System Recovery Procedures (SRP)

System recovery procedures (SRP) provide general procedures for the recovery of a system from backup media or other sources.

Business Continuity Methods

Business Continuity Methods define the system availability and data recovery strategies.

System Availability:

Continuous Availability: A system that is created with a goal of no scheduled or unscheduled downtime. Continuous availability systems can only be reliant upon other systems that are unremitting. Alternate facilities, not physically located within the same building, will be used to ensure that no local disruptions interfere with the system's continuous availability. Real time synchronization between the sites is used to route data to both the primary site and the alternate facility(ies). Continuously available systems consist of hardware and software designed to protect against component and system-level failures at any point in time, with an understanding that the system will always be active.

High Availability: A system that can quickly recover from a failure by way of automation built into the system. There may be a small amount of downtime while one system switches over to another, but processing will continue. There should be a goal of no unscheduled outages or downtimes. High availability systems can only be reliant on unremitting systems or other systems that have no lower availability than high. Alternate facilities, not physically located within the same building, will be used to ensure that no local disruptions interfere with the system's high availability. Near real time synchronization between the two sites is used to mirror the data environment of the original site. The alternate site will have hardware and system resource components; networking equipment with an active connection; and the resources needed to recover the business processes impacted by the system disruption.

Recoverable: Redundant infrastructure components, such as web and file servers, which have data replication. The facility will have backups on hand, but they may not be current or could be incomplete. A full backup should be done

first with either an incremental or differential backup completed on a set schedule. The system will recover by manual intervention which will cause some downtime as tolerable. An alternate facility (possibly smaller in scale) with the equipment and resources to recover the business functions affected by the occurrence of a disaster may be used.

Reliable: Non-redundant components that have no protection or hot-

Walkthrough: Staff walkthrough the recovery plan as a group, discussing each step along the way.

Simulation: Staff members perform a walkthrough in the context of a simulated disaster that includes periodic announcements of events as they occur. Staff do not actually perform any recovery steps.

Parallel: Staff members perform actual recovery steps to move business processes to alternate locations. Staff build or activate recovery servers while primary servers are also still working. Primary everyday business processes should continue uninterrupted.

Component: Individual components (such as a webserver or database) are rendered offline to test failover and backup solutions.

Interruption (complete rehearsal): The business stops performing critical business processes, as though an actual disaster has occurred. Staff members carry