
The university is increasingly dependent on computer-related *university resources*. The ability to recover quickly from the loss of access to *university resources* is critical. *Units* must develop comprehensive *business continuity* and *disaster recovery* plans that will ensure continued delivery of university services in the event of a disaster or interruption. A disaster can be as minor as the loss or failure of an individual computer or email service, or as catastrophic as a flood or terrorist *attack*.

The following minimum standards were developed to address *business continuity* and *disaster recovery* planning at the *unit* level. *Units* and individuals are encouraged to implement any additional plans they deem necessary. These minimum standards should not be used to reduce the level of preparedness that may already exist.

These standards apply to *units*, *university employees*, *affiliates*, *associates* and *volunteers*, contractors and vendors and represent the minimum planning and cooperative efforts necessary to develop recovery and *business continuity* practices. This and all other *disaster recovery* planning documents should be stored on a variety of media, including hard copy, so that they are readily accessible when needed.

1. Business Impact Analysis (BIA)/Risk Assessment

University *units* must conduct an analysis of the workflow within the *unit*, including interdependencies between individuals and other university *units*.

2. Coordination

University *units* must establish *business continuity* and *disaster recovery* teams. Procedures and responsibilities must be developed for each team identified. Teams may include: communication, *incident* response, damage assessment, IT support and others. Size, make up and number of teams will be determined by *unit* needs.

3. Backup and Recovery

University *units* must establish procedures and policies for backup and recovery of the *units'* data. Backups should be routinely monitored to ensure that recovery procedures are functional. Detailed documentation of equipment and software necessary to restore *university resources* should be created. The equipment necessary to restore systems and data should be documented improving the time and quality of purchasing decisions in the event of recovery needs.

Backup media and documentation should be stored both on and *off site* at a university approved location.

4. Asset Management

A thorough current inventory of equipment including hardware, software and warranty details should be maintained by university *units*. A *Disaster Recovery* and Asset Management system (LDRPS) is available for *units* through the Center for Computing and Information Technology (CCIT) *Business Continuity* and *Disaster Recovery* Office. See related documents section below.

5. Asset and Media Disposal

All university *units* shall follow university guidelines for proper disposal of equipment and media. As equipment is often transferred within the university or sold to outside parties, appropriate steps must be taken to securely erase all data or physically destroy the storage media before transfer or surplus. Paper copies of *confidential university data* should be shredded or destroyed at a bonded facility.

6. Contingency Planning

University *units* must establish procedures and policies for maintaining time-sensitive operations. In the event of system failure, alternative methods for performing critical functions must be in place to ensure continued operations.

7. Related Guidance

Information Security Policy (IS-100)
Information Security Terms Guideline (IS-G100)
Exceptions Procedure (IS-P100)
Guidelines for Generating a Disaster Recovery Plan:
<http://security.arizona.edu/files/ISG901.pdf>

Disaster Preparedness Inventory: <http://security.arizona.edu/files/ISG903.pdf>
Business Impact Analysis Form: <http://security.arizona.edu/files/ISG902.pdf>
Living Disaster Recovery and Planning System (LDRPS)
<http://ccit.web.arizona.edu/index.php?id=1146>

All *italicized* terms used in this standard are defined in the Information Security Terms Guideline.

Revision History

Initial Draft	08/09/07
Effective Date	04/29/08