**IT Disaster Recovery Plan.**

1. A plan revision and approval page as a cover sheet, containing date of most recent plan review and revision, name(s) of reviewer(s), date of most recent plan test, and approval of plan as indicated by signature of department head.

2. Identify vital servers or services (e.g., file , Web, application, e-mail, etc.) Provide the relevant information for each instance.

• Name and description
• Campus inventory number

• If a service, the number of physical servers supporting the service
• Server type (virtual or physical)

• Operating System and patch level
• List of essential application software and patch level

• # of Cores
• Disk storage and amount (internal and attached)

• RAM
• Backup type (full, incremental, etc)

• Backup generation frequency
• Number of backup generations available onsite

• Number of backup generations available off-site
• Location of backups

• Media type
• Retention period

• Rotation cycle
• List of personnel authorized to retrieve the backups

**For each server, service, or application, address the following subjects if relevant to the specific instance.**

3. Identify if a severe, long term disruption occurred what would be the minimum requirements/replacement needs to perform the critical function during the disruption if it is less than the capabilities of the current server.

• Type (e.g. server hardware, software, research materials, etc.)
• Item name and description

• Quantity required
• Vendor/supplier

4. Identify if alternate methods of providing the affected services or processes either exist or could be developed, quantifying where possible, impact on processing. (Include alternative manual processes if they exist.)

**5. Identify person(s) who supports the server, service, or application**

6. Identify primary person to contact if server, service, or application cannot function as normal

**7. Identify secondary person to contact if server, service, or application cannot function as normal**

8. Identify all vendors associated with the server, service, or application

**9. Document unit strategy during recovery (conceptually how will the unit function?)**

10. Identify how soon after a re-commencement of unit operations the server or service would be required to be back in operation

**11. Identify maximum age limit of backup data that can be used to restore the server or service**

12. Quantify required resources and time frame required for recovery including resources external to your unit (e.g., server hardware, 2 people for 8 hours, etc.)

**13. Develop and document recovery strategies for each server, service, or application including:**

• Assumptions upon which the recovery strategies depend
• Priorities for recovering system/function components

• Recovery schedule
• Location of documented step-by-step recovery procedures, if not attached to the IT Disaster Recovery Plan