**Borrowed and adapted from a model created by University of Virginia**

### IT Security Risk Management Process Flow

w_bnidno[1]w_bnidno[1]w_bnidno[1]

1. **Disaster recovery plan example**
2. **Interim manual procedures example**
3. **Criteria**
4. **Template**
5. **Assessment questions**
6. **Threat scenarios**
7. **Response strategies**
8. **Security plan template & example**

*Security*

*Plan*

*Interim*

*Manual*

*Procedures*

*Disaster*

*Recovery*

*Plan*

Step 4 – Evaluation and Reassessment

Required at least once every two or three years

Step 3 – Mission

Continuity Planning

Create a response plan to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed

Step 2 – Assess Risks

For each critical asset:

1. Assign weight to likelihood & impact of threats to each asset
2. Prioritize threats
3. Select response strategies
4. Develop security plan

*Critical*

*Assets*

*List*

Step 1 - Identify

Critical IT Assets

## Step 3: IT Mission Continuity Planning

In Step 1, your department determined what IT assets are critical to the functioning of your department. In Step 2, you analyzed risks to those assets, and determined how to mitigate those risks or accept them where mitigation was infeasible or unaffordable. Now in Step 3, you will identify short- and long-term plans for continuing to provide your mission-critical functions in the event that the mitigation responses from Step 2 prove insufficient or if an unmitigated risk becomes a reality.

What is the impact of your department being down for hours or days? Do you have a way to restore your systems if they are destroyed? Do you have a manual way of performing critical functions in the meantime?

Should a critical asset be rendered unavailable, continuity planning prepares for the continuation of critical functions, minimizes the negative effects of the problem and protects data from compromise. Concrete deliverables of such planning include backup, off-site storage, recovery plans and interim manual procedures.

In the event of a true disaster, entailing widespread damage to buildings and people, the University would activate its Critical Incident Management Plan (CIMP). However, departments are expected to plan for and coordinate recovery when problems are localized. CIMP requires critical incident planning at the departmental level, the IT component of which is included in this process.

The point of disaster recovery is to have your critical functions up and running as quickly as possible. Interim manual procedures need to be prepared for highly critical processes that need to be performed before full recovery may be possible. Create (or update) a response plan for your department to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed. Below are a series of questions to help you prepare and test this plan.

*Note:* The costs associated with mission continuity preparedness can be significant, and they increase dramatically the more rapid the recovery that is required. Such efforts do benefit from economies of scale, however, allowing larger organizations to put measures in place that would be cost-prohibitive for smaller ones. Having other departments and units host services or servers for your department can pay for itself when continuity preparedness costs are factored in, even in cases where the financial case is marginal based simply on day-to-day operational costs.

|  |  |
| --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Mission Continuity Questions  The development of a plan for restoration of resources identified in the mission impact analysis and for interim manual processes for continuing critical mission functions during the restoration process. | |
|  | Documentation Location and/or Decision |
| **A. Interim Manual Process Components (aka Downtime Procedures)** | |
| 1. Does the department know how long it could function without department computers, servers, or network access? |  |
| 2. For each mission-critical departmental function, what is the maximum time the department can wait on recovery efforts before proceeding with manual alternatives?  *Note: Some functions may vary in criticality depending on the time of the year. Example: Class registration procedures may have a long recovery window some weeks, but a very short window in other weeks.* |  |
| 3. How does the department proceed manually with mission-critical functions if critical IT assets are lost, unavailable, corrupted, etc.? How long can this be maintained?  Repeat for each identified function. |  |
| 4. In the event of partial damage or disruption, are the department computers standardized so that users could work from another department or University computer without difficulty? Are data necessary to such work stored on a central server or backed up so it can be restored? (See Question B.11. below.) |  |

|  | Documentation Location and/or Decision |
| --- | --- |
| **B. Disaster Recovery Components** |  |
| 1. List the team leader and members of your designated recovery team.  Include name, title, responsibility, e-mail address and telephone number(s) of each member. |  |
| 2. Do you have the necessary University and departmental personnel contact lists?   * Who will decide “this is a mission continuity problem” * Who should be notified in case of a mission continuity problem? * Who will be responsible for responding to a mission continuity problem? * How will you contact them in an emergency situation (pager, cell phone, call lists)? |  |
| 3. Do you have hardware diagrams and system configurations, including physical and data security issues? |  |
| 4. Do you have infrastructure information about your facilities (requirements for power, cooling, network cabling, etc.)? |  |
| 5. Are installations and changes to those critical physical configurations governed by a formal change management process? (This will vary from simple chronological logging of changes to assist in troubleshooting or back out, to a multilevel review involving significant testing for more complex and highly critical systems.) |  |
| 6. Do you have the necessary hardware and software vendor contact lists? |  |
| 7. Do you have a current inventory of your hardware, software and critical data files? Is it updated in real time? |  |
| 8. Does the department securely escrow passwords for accounts that may need to be accessed in the absence of their normal administrator or in an emergency situation? |  |
| 9. Do you have a plan for emergency procurement? (For example, contracts for emergency replacement and a procurement contact list.) |  |
| 10. Do you have recovery plans for each service to be restored (specific, complete, up-to-date)? Do they include a list identifying all system, application and data file systems that must be recovered for each system? |  |
| 11. Are all important data backed up, with secured off-site rotation? (Off-site rotation involves periodically and systematically moving backup media to a physically and environmentally secure facility at a significant distance from the asset being backed up.) |  |
| 12. Is system and recovery information stored off-site in a readily accessible secured location?   * Any documentation referenced above * Data backups * Software media * Software license packs * Any other key information needed for recovery or continuation of essential services |  |
| 13. Do you test your plan annually by at least doing a paper walkthrough? When was the last test? |  |
| 14. Do you update your plan after each test, or when there is a significant technology change? |  |
| 15. What training do you have for staff involved with the plan, including communicating and testing the plan? |  |
| 16. Have departmental personnel received training on what to do and whom to contact within the department and /or University if a computer security or a disaster incident should occur? |  |
| 17. Are recovery and continuing operations instructions written in simple, clear, complete sets of steps that upset, fatigued people could follow correctly? |  |
| Prepared by: Administrative contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Prepared by: Technical contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

Below are simple checklists outlining the key steps in disaster recovery and interim manual procedures. Any plan you develop will need to address at least these issues.

Disaster Recovery Plan Checklist

* Assess damage
* Notify all appropriate University personnel
* Assemble recovery teams
* Provide infrastructure (space, power, cooling, network, etc.)
* Secure needed hardware and supplies
* Return backup information from off-site storage (backup tapes, documentation)
* Install operating systems on restored servers
* Restore applications and institutional data
* Thoroughly test before going on-line

Interim Manual Procedures Checklist

* Identify the procedure
* Identify those with the knowledge, skill and ability to complete the procedure manually
* Determine how long the process can be interrupted before proceeding manually
* Develop detailed documentation on how the procedure will be performed
* Determine how data is reintegrated once the IT-based system is restored

Based on your answers to the Mission Continuity Questions and the steps outlined in the checklists, create (or update) your IT Mission Continuity Plan using the template below.

Your department may also take advantage of any general disaster recovery or mission continuity plans you have in place, inserting or integrating IT assets and strategies as appropriate.

|  |  |
| --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| IT Mission Continuity Plan Template  Based on your answers to the Mission Continuity Questions, replace *the italicized text* below with the appropriate information. | |
| * 1. Mission Continuity Requirements      1. Mission Continuity Plan Overview   *INSERT here your overview of the departmental plan, identifying the systems it includes and the mission impact of their unavailability.*   * + 1. Scope of the Mission Continuity Plan   *INSERT here what your plan covers and does NOT cover.*   * + 1. Mission Continuity Plan Assumptions   *INSERT here any assumptions implicit in the plan—e.g., nature of the service interruption; availability of staff; what backups are available…. This section should identify existing downtime procedures and include the time tolerance during which the procedures may be used by departmental personnel.*   * + 1. Interfaces   *INSERT here a list of any inbound or outbound interfaces to other systems required for the departmental application’s operation.*   * + 1. Escalation Plan   *INSERT here steps taken to evaluate an outage, declare a disaster, and notify departmental and senior management of the event and the decision to invoke this plan.*   * + 1. Decision Timeframes for Plans   *INSERT here the timeframe in which an event is assessed for mission impact; if a disaster is declared, the timeframe in which staff must respond; the timeframe for notifying senior management.*   * + 1. Interim Manual Procedures (aka Downtime Procedures)   *INSERT here references to existing documented procedures to be used during a system outage.*   * 1. Team Structure, Contacts, and Call Lists      1. Team Structure and Tasks   *INSERT here a description of the major activities that must be completed as part of the plan and the departmental teams that must be assembled for their completion; these teams may include people and vendors outside the department and the University.*   * + 1. Emergency Notification Plan/Call Lists   *INSERT here lists of documentation required by the teams to accomplish the plan, including their physical location as both electronic and paper documents; contact information for all team members, including office, home, and pager telephone numbers.*   * + 1. Vendor Contact List   *INSERT here contact information (names, phone, email, Postal Service, web sites, etc.) for each vendor that may require contact during a mission continuity event. Include in an appendix a description of all software and hardware products with version and, if applicable, server/CPU serial information.*   * + 1. Assembly & Command Centers   *INSERT here designation and description of locations to which staff should report in the event of a disaster or a required evacuation of a building housing departmental equipment subject to recovery; alternate sites should be included; these will be focal points for mission continuity activities when a disaster is declared.*   * + 1. Recovery Site(s)   *INSERT here detailed information describing any alternate sites at which computer equipment will be located for recovery purposes; if these locations are provided by an organization outside the department, notification procedures should be included.*   * 1. Backup Procedures      1. Backup Procedures   *INSERT here detailed description of tools/products used to regularly back up departmental software and data; location of any off-site tape libraries or tape storage; backup schedules; reference to any backup tasks performed by any other entity on behalf of the department.*   * + 1. OS/Application Backup/Recovery Procedures   *INSERT here step-by-step actions to be taken to recover operating system, application software, and departmental system data using the tools/products outlined in the previous section; this should contain enough detail so that a knowledgeable person unfamiliar with the daily backups could complete the recovery.*   * + 1. Hardware/System Software Plan Overview   *INSERT here describes the computer hardware and operating system software necessary to restore a departmental system in the event of a disaster; includes procedures and controls to assure efficient and timely restoration at an alternate site; appendices may be used to list existing hardware and software and to detail what is available or required at an alternate site.*   * + 1. Operating Systems/Other Software   *INSERT here technical references to required OS and application software that will be restored; these should include both electronic and paper copy references as well as material available at vendor web sites.*   * + 1. Data Communications Plan   *INSERT here detailed requirements for alternative network connections that must be established in the event of a disaster; if common carrier connections are required, these should be detailed and contracted for in advance; departments should work with the University network team to detail and diagram any alternative network connections required.*   * 1. Recovery Procedures      1. Hardware/Software Recovery Overview   *INSERT here an overview of the general steps to be taken to restore a departmental application’s operation; in general, this would include hardware configuration, OS reinstallation and initialization, application reinstallation, restoring data, and application operability.*   * + 1. System Recovery Procedures   *INSERT here step-by-step actions to be taken to recover the hardware and operating system; this should contain enough detail so that a person with only general knowledge of the OS could complete the recovery.*   * + 1. System Initialization Procedures   *INSERT here step-by-step actions to be taken to initialize the operating system; this should contain enough detail so that a person with only general knowledge of the OS could complete the initialization.*   * + 1. Storage Restore List   *INSERT here a list (or references to auxiliary documentation) identifying all system, application and data file systems that must be recovered for each system included in the plan.*   * + 1. Applications Recovery   *INSERT here step-by-step actions to be taken to restore the departmental application; this should contain enough detail so that a person with only general knowledge of the application could restore it.*   * 1. Implementation Plan      1. Types of Recovery Tasks   *INSERT here definitions of task types to be accomplished by the recovery teams; examples are recovery (hardware, OS, application) and support (security, transportation, procurement, etc.).*   * + 1. Recovery Team Tasks   *INSERT here a detailed listing of all recovery tasks needed to fully restore the departmental application of operability on an alternate (or redundant) computer platform. Each task should include:*   1. *an estimated start time after a disaster occurs;* 2. *estimated time to complete the task;* 3. *identification of the team responsible for the task;* 4. *predecessor tasks that must be completed before each task is started;* 5. *a description of the task.*   *Step-by-step instructions for completing each task are contained in previous section of the plan.*   * 1. Mission Continuity Plan Testing      1. Mission Continuity Plan Test Objective   *INSERT here departmental disaster plans should be periodically tested. This section defines testing objectives and frequency.*   * + 1. Plan Test Requirements and Methodology   *INSERT here testing may be accomplished in many ways (paper walk-throughs, scheduled tests, unannounced tests, tactical exercise, etc.). This section defines the plan testing requirements determined to meet the department’s needs to insure plan success.*   * 1. Mission Continuity Plan Maintenance      1. Plan Maintenance Objectives   *INSERT here any disaster plan must be maintained. This section specifies departmental objectives for keeping the plan current and maintaining staff awareness of it.*   * + 1. Mission Continuity Plan Maintenance   *INSERT here maintenance of the plan will be required on a scheduled basis (periodic reviews to detect the need for plan changes) and on an unscheduled basis (due to events—an OS upgrade, an application upgrade, a network change, etc.). Periodic reviews should include verifying that recovery hardware capacity is sufficient to meet increasing application transaction processing volume.*   * + 1. Interdepartmental Relationships   *INSERT here any required relationships with other departments necessary for the successful completion of a mission continuity plan should be included here. Examples include HS/CS or ITC, Procurement (Material Support Services in the Health System), Legal, and University Relations (Media Relations in the Health System).*   * + 1. Mission Impact Analysis (MIA)   *INSERT here departments should periodically perform a Mission Impact Analysis on their operation of the effect of a departmental application failure. This section should contain a summary of the most recent MIA the department has conducted.*   * 1. Relocation Plan      1. Returning to Normal Operations   *INSERT here factors affecting a return to normal operations should be included here if temporary relocation to a Hot/Cold Site is part of the recovery plan.*   * 1. Appendices      1. Appendix A: Call Lists/Contact Information      2. Appendix B: Equipment Inventory      3. Appendix C: Software Inventory      4. Appendix D: Network Diagrams      5. Appendix E: Mission Continuity Contracts | |
| Prepared by:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |