

University of Virginia
Information Technology Security
Risk Management (ITS-RM)
Program

Version 3.0

Revised 08/03/10

Unit Name: _____

Sub-Unit Name: _____

Submitted: _____

Contact: its-rm@virginia.edu
<http://www.itc.virginia.edu/security/riskmanagement/>

Contents

<i>Reporting Requirements</i>	1
<i>Mission Impact Analysis Questions</i>	2
<i>Risk Assessment Questions: General</i>	5
<i>Risk Assessment Questions: HIPAA Supplement</i>	17
<i>Risk Assessment Questions: GLBA Supplement</i>	21
<i>Risk Assessment Questions: FERPA Supplement</i>	24
<i>Threat, Attack and Vulnerability Scenarios</i>	27
<i>Security Plan Template</i>	35
<i>IT Mission Continuity Plan Template</i>	41
<i>Evaluation and Reassessment Questions</i>	46

This is version 3.0 of the University of Virginia Information Technology Security Risk Management (ITS-RM) Program materials.

All materials ©2010 by the Rector and Visitors of the University of Virginia.

Reporting Requirements

1. A copy of all ITS-RM working papers and final forms should be kept in the department, and a copy should be placed in secured off-site storage (e.g., along with your backups) for retrieval in the event local access is impossible.
2. Upon the completion of the five forms listed below (A-E) and approval of them by the department head (and the appropriate dean or vice president if he/she has decided this additional step is important), a copy (templates are available in a compact reporting format in [Word format](#) and [PDF format](#)) should be sent by e-mail to:

its-rm@virginia.edu

or by messenger mail to:

ITS Risk Management
Information Security, Policy, and Records Office (ISPRO)
P.O. Box 400898

- A. **Mission Impact Analysis Questions**
- B. **Risk Assessment Questions and Threat/Response Scenarios**
- C. **Security Plan**
- D. **IT Mission Continuity Questions and Plan**
- E. **Evaluation and Reassessment Questions** (if appropriate)

ISPRO will file a copy of each department's mission continuity plan with the University Disaster Recovery Coordinator, U.Va. Police Department. Documentation from departments hosting HIPAA/HITECH-protected data will be shared with the HS/CS security office. These documents will be used to identify new services required and areas where central assistance is needed. Moreover, they assist the University in doing its own assessment of its overall IT security risks. They also need to be stored in a protected central location for University access in emergency situations. These documents will be kept in strictest confidence and will be used only in emergencies and to gauge an aggregate view of the University's IT security environment.

This reporting process will be repeated with each subsequent evaluation and reassessment.

Unit Name: _____ Sub-Unit Name: _____

Mission Impact Analysis Questions

The identification of information, computing hardware and software, and associated personnel that require protection against unavailability, unauthorized access, modification, disclosure or other security breaches.

Note: Any use of [highly sensitive data](#) (including Social Security numbers, protected health information, etc.) is inherently a critical component of the unit's mission and a source of significant risk.

1. What's your department's mission?

See related list in [Table 1](#)

2. What are the key functions your department performs to implement your mission?

3. What IT hardware infrastructure and assets are critical to the performance of those key functions? Please list these assets and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, central U.Va. and external (e.g., vendor) assets as appropriate, and list a system administrator, model number and operating system, where applicable, for each asset.

Examples:

- Servers (including those hosted by others)
- Desktops/laptops/PDAs that host critical or [highly sensitive data](#)

<p>4. What software applications are critical to the performance of those key functions? Please list these and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, central U.Va. and external (e.g., vendor, federal and state) assets as appropriate.</p> <p><i>Note:</i> Even common applications, like web browsers and Microsoft Office, may be critical and must be kept updated and secure to protect your systems.</p>	
<p>5. What IT data assets are critical to the performance of those key functions? Please list these assets and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, central U.Va. and external (e.g., vendor, federal and state data swapping) assets as appropriate.</p> <p><i>Examples:</i></p> <ul style="list-style-type: none"> •<i>Academic:</i> instructional resources, databases necessary to maintain a given research program •<i>Administrative:</i> sensitive student or financial data necessary for business operations and student services •<i>Health-related:</i> sensitive patient data, both clinical and research •External data provider 	
<p>6. Provide a complete location inventory of all data of the following types used or stored in the department, whether in paper or electronic form:</p> <ul style="list-style-type: none"> • Social Security Numbers (SSNs) • Health Insurance Portability & Accountability Act (HIPAA) or Health Information Technology for Economic and Clinical Health (HITECH) Act protected health information (PHI) • Family Educational Rights and Privacy Act (FERPA) protected student data • Gramm-Leach-Bliley Act (GLBA) protected financial data • Payment Card Industry (PCI) data, including 	

<p>credit card numbers and transaction information</p> <ul style="list-style-type: none"> • Passport numbers • Any other highly sensitive or legally protected data <p>Other examples of legally protected data may include data related to patents, contracts, and national security.</p>	
<p>7. What IT personnel are critical to the performance of those key functions? Please list the job roles and the incumbents' names and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, central U.Va. and external (e.g. vendor) personnel as appropriate.</p> <p><i>Examples:</i></p> <ul style="list-style-type: none"> •Server administrators •Local Support Partner (LSP) or Associate (LSA) •Database administrators •ITC Engineers who provide contracted support 	
<p>Prepared by: Administrative contact</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Title: _____</p> <p>Date: _____</p>	<p>Prepared by: Technical contact</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Title: _____</p> <p>Date: _____</p>
<p>Approved by: Unit head</p> <p>Name: _____ Signature: _____</p> <p>Title: _____ Date: _____</p>	

<p>Unit Name: _____ Sub-Unit Name: _____</p>

Risk Assessment Questions: General

These questions will help determine and evaluate threats to the resources identified through a mission impact analysis, as well as adherence to general secure computing practices.

	Yes	No	Documentation location or explanation for not following
A. Physical Security			
1. Are all computers located in areas that are not easily accessible to outsiders?			
2. Are mission critical systems located in a locked location to which access is restricted to authorized personnel only?			
3. Are faculty and staff taking responsibility for locking doors and windows where computers are housed?			
4. Has physical security been reviewed with the University Police and Facilities Management?			
5. Are department desktops and notebooks equipped with anti-theft devices?			
6. Are departmental keys logged in and out individually with one staff person responsible for the tracking of the keys? Has this procedure been approved by Facilities Management (FM)? See FM key policy .			
7. Are department servers physically secure in a separate area, i.e., physically restricted, a double-locked door, with card access and access logging.?			
8. Are servers in environmental control areas that include: Smoke detectors? Water detectors? Fire suppression systems? Temperature sensors?			

	Yes	No	Documentation location or explanation for not following
9. Are mission critical servers away from high-traffic areas; e.g., not near an auditorium or along a well-travelled hallway?			
10. Are uninterruptible power supplies (UPS) with surge protection used on servers and other important hardware?			
11. Are surge protectors (at least) used on desktop computers?			
12. Are individual firewalls (software or hardware) installed on any desktops, laptops or servers in the department?			
13. Are security incidents (for example, unauthorized use, loss, theft, or compromise of devices) reported in compliance with the IT Security Incident Reporting policy?			
14. Is there an accurate inventory of all computing equipment and software? If so, is a copy of the inventory stored off-site?			
15. Do you have individual use devices with sensitive data in a publicly accessible area?			
<i>B. Account & Password Management</i>			
1. Do you have defined, documented criteria for granting access based on job responsibilities?			
2. Are all sensitive data used for authenticating a user, such as passwords, stored in protected files?			
3. Are users authorized to access only those resources required to perform their jobs and nothing more?			
4. Does the department deactivate accounts for terminated or transferred employees in a timely manner?			

	Yes	No	Documentation location or explanation for not following
5. Does the department periodically review current employee accounts that have not been used in a long time and consider deactivating them?			
6. Does the department prohibit shared accounts? If shared accounts are not prohibited, please list what systems/applications require shared accounts and justify continued use. <i>Note:</i> No justification is possible for highly sensitive data on shared accounts.			
7. Has the department emphasized to users that their password, along with their computing ID, is the key to their electronic identity?			
8. Does the department have a policy on keeping passwords confidential? (See Responsible Computing Handbook and Electronic Access Agreement .)			
9. Does the department assist users in selecting passwords that will ensure privacy while promoting regular use? (See ITC guidelines and/or HS/CS guidelines .)			
10. Does the department require that passwords not be written down or shared, except for purposes of escrow?			
11. 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? (A short overview of and rationale for password escrow is available here .)			
12. Does the department require that passwords on departmental workstations and servers be changed periodically?			
13. Is there a reasonable “previous used” password history list to deter users from repetitive use of the same password?			
14. Does the department require passwords for access to department workstations and servers?			

	Yes	No	Documentation location or explanation for not following
15. Does the department require the use of password-protected screen savers, automatic application timeouts and automatic network log-offs?			
16. Does the department log and review more than three attempts to enter a password for a given account? (The U.Va. Audit Department suggests locking out a user after three unsuccessful log-in attempts.)			
17. Does the department prohibit modems attached to servers and desktops that can receive calls?			
<i>C. Virus Protection</i>			
1. Is Symantec (Norton) or other anti-virus software installed on all department computers?			
2. Is a procedure for updating the anti-virus software in place? For personal systems, if this is up to the user, are instructions and recommended update intervals provided?			
3. Does the department remind users to scan regularly for viruses in addition to updating?			
4. If a computer becomes infected with a computer virus, do users know to follow the IT Security Incident Reporting policy?			
5. Does the department periodically remind users to open only attachments they are expecting?			
<i>D. Data Backup and Recovery</i>			
1. Have faculty and staff been advised of their personal computer backup options? Do they have instructions for the options and recommended backup cycles?			
2. Does the department regularly back up department servers? Does the server backup procedure include secure off-site storage?			

	Yes	No	Documentation location or explanation for not following
3. Does the department periodically test restoration of personal and server files?			
4. Do users store all local data in a single directory to simplify backup of personal data and ensure all data is captured?			
5. Are backup needs periodically reviewed?			
6. Does the department comply with University's Records Retention and Disposition Policy ?			
7. Does the department consult with the University Records Officer before implementing any electronic document management system, including ImageNow?			
<i>E. Operating Systems</i>			
1. Are only ITC and/or HS/CS-supported operating systems used?			
2. Are appropriate operating system updates and security patches being applied in a timely manner to all department computers and servers?			
3. Are servers and desktops periodically scanned by ITC for security vulnerabilities?			
4. Have unnecessary services and features in desktop and server operating system configurations been disabled?			
5. Is the use of shared drives or folders between desktop computers (peer-to-peer sharing) prohibited or restricted?			
6. Is it verified that file permissions are properly set on servers?			
7. Is Autorun and AutoPlay functionality disabled for removable disks and shares?			

	Yes	No	Documentation location or explanation for not following
<i>F. Application Software</i>			
1. Are appropriate application software updates and security patches being applied in a timely manner to electronic devices <i>on which University-related data reside or business is done</i> (whether University or personally owned devices)?			
2. Have faculty and staff been instructed to place on-line orders only through secure Web sites?			
3. If employees are allowed to install U.Va. and/or HS/CS licensed software at home, is it installed in compliance with the license, and has any necessary user acceptance form been completed and returned to the appropriate person?			
4. Does the staff have the appropriate level of access to applications based on their current responsibilities?			
5. Is application access promptly removed for employees who have left the department?			
<i>G. Confidentiality of Sensitive Data</i>			
1. Are all departmental locations of highly sensitive data , both electronic and paper, inventoried?			
2. Following the Electronic Data Removal policy , a) are all data and software removed from hardware and electronic media prior to transfer within U.Va., and b) are all hardware and media processed through Procurement's designated vendor when leaving U.Va.? Media include hard drives (from computers, printers, copiers, etc.), magnetic tapes, diskettes, CDs, DVDs and USB storage devices.			
3. Is access to sensitive departmental data restricted?			
4. Is ownership of data clearly defined?			
5. Do data owners determine and periodically review appropriate levels of data security required?			

	Yes	No	Documentation location or explanation for not following
6. Is access to information technology resources explicitly granted to personnel by data owners?			
7. Have the faculty who are conducting research determined if the data they are collecting should be classified as sensitive?			
8. Do the faculty and staff who administer sensitive data understand and follow appropriate federal, state, grant agency, or university regulations for protecting and backing up data?			
9. Are student workers given access to confidential teaching, research or administrative data? If so, is their use of such data monitored closely?			
10. Are authentication, authorization, and data security policies established by data owners protected from compromise during data sharing and systems interoperability?			
11. Are user agreements clearly stating required authentication and protection levels established with all external agencies and institutions with which data are shared? List all such data sharing relationships, indicating the data shared and the transmission method used (e.g. VPN, SFTP).			
12. Is the unencrypted transmission of highly sensitive data through e-mail prohibited?			
13. Do web-enabled transactions that require user authentication, transfer highly sensitive data , or transfer funds use encryption?			
14. Are the employees who have VPN access aware they should be disconnecting from the VPN when not in use and when away from their desk?			
15. If the department has a wireless network, is the network encrypted? If so, what type of encryption?			

	Yes	No	Documentation location or explanation for not following
16. Are cryptology technologies for data storage and transmission of data based upon open standards?			
17. Are encryption key management policy and procedures in place to ensure the integrity and recovery of encryption keys?			
18. Are all sensitive data stored and transmitted in compliance with the University's Institutional Data Protection Standards and the Electronic Storage of Highly Sensitive Data policy?			
19. Do all iKey hardware token users disconnect from the VPN when not in use and/or when away from their desk? Are users aware of their responsibilities regarding the protection of the iKey token?			
20. Are all highly sensitive data files routinely and promptly deleted in a secure manner when no longer needed for their approved business purpose or official records retention?			
21. If highly sensitive data are stored on individual use devices or media , has the appropriate vice president or dean completed the approval form ?			
22. If highly sensitive data are stored on individual use devices or media , is it encrypted?			
23. If highly sensitive data are stored on individual use devices or media , are all security requirements strictly followed?			
24. Do you have a regular schedule for scanning departmental devices for highly sensitive data ? If so, what is it?			
25. If the department accepts credit cards (over the web or through a point-of-sale terminal), are all credit card numbers collected, stored, protected and destroyed in accordance with the University's PCI-compliant Credit Card Requirements ?			

	Yes	No	Documentation location or explanation for not following
26. Have you returned your SSN Inventory and Remediation Status Report, indicating that you have completed your remediation plan?			
27. Do you understand and acknowledge the on-going responsibilities you have regarding the use and protection of SSNs as outlined in the Protection & Use of Social Security Numbers policy , Institutional Data Protection Standards , Electronic Storage of Highly Sensitive Data policy , and Guidance on Social Security Number Redaction and Records Management ?			
28. Do you submit a Request for Approval to Use Social Security Numbers and receive approval before using SSNs for any new purpose?			
29. Do you regularly review the necessity of, and seek to reduce, any continued use of SSNs?			
30. Do you periodically scan computing devices with Identity Finder or similar software to ensure that SSNs have not reappeared; delete any newly found instances and determine how to prevent future recurrences?			
31. As required by state law, do you promptly destroy records containing SSNs <i>within six (6) months of their completed retention period</i> by following the procedures established by the University Records Officer ?			
<i>H. Security Awareness and Education</i>			
1. Are faculty and staff aware of their responsibility for computer security according to the Responsible Computing Handbook ?			
2. Have all copies of department software been properly licensed and registered?			
3. Has the University's copyright policy been distributed and discussed within the department?			

	Yes	No	Documentation location or explanation for not following
4. Have University and/or Medical Center and department-specific security policies and procedures been documented and shared with all faculty and staff?			
5. Are faculty and staff keeping current on University and/or HS/CS security issues and alerts ?			
6. Are suspected violations of security appropriately reported to a designated system or departmental administrator?			
7. Do your system administrators and LSPs have training commensurate with the level of expertise required, which may include ability to identify threats, vulnerabilities and risks specific to your information resources?			
8. Are individuals involved in information technology management, administration, design, development, implementation, and/or maintenance aware of their security responsibilities and how to fulfill them?			
9. Does training for these individuals enable them to identify and evaluate threats, vulnerabilities, and risks and understand best practices relevant to the systems components and resources for which they are responsible?			
10. Does the department encourage staff to take available ITC cyber security awareness classes?			
11. Do all departmental staff take the Information Technology Security Awareness Tutorial annually?			
<i>I. Publicly Accessible Computers (Computing lab, public kiosks, etc.)</i>			
1. Are the computers created with a software image configured for the greatest practicable restrictions on disk access, software installation and user rights?			

	Yes	No	Documentation location or explanation for not following
2. Are the computers refreshed frequently (daily, if possible) to force reversion to the designated software image and the removal of personal data?			
3. Are log-in IDs required?			
4. Is information posted (either by sign or log-in screen) warning users to log out of all applications, Web sessions, server connections, etc. to prevent access to their personal data by subsequent users?			
5. Are extensive anti-theft devices utilized, including locking down all peripherals and locking the computer case?			
6. Are users automatically logged-off after a short period of inactivity?			
<i>J. Review and Response</i>			
1. Is there a documented procedure for handling exceptions to security policies and standards? Does this procedure include higher management level review of exception approvals?			
2. Are critical systems and infrastructures, including all those storing or transmitting highly sensitive data , formally identified on a periodic basis?			
3. Do procedures for development, installation, and changes to systems and infrastructures include review and approval steps for security implications and design features?			
4. Do you have a written process for handling suspected breaches to security safeguards (e.g. intrusion detection)?			
5. Is a process in place to identify and evaluate threats and to assign appropriate action based upon risks?			
6. Does your hardware firewall technology have security logging turned on?			

U.Va. IT Security Risk Management Program

Prepared by: Name: _____ Signature: _____ Title: _____ Date: _____	Approved by: Unit head Name: _____ Signature: _____ Title: _____ Date: _____
-------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------

Unit Name: _____ Sub-Unit Name: _____

Risk Assessment Questions: [HIPAA](#) Supplement

These questions will help determine and evaluate threats to the resources identified through a mission impact analysis, as well as adherence to general secure computing practices.

In addition to the issues covered in the general questions, additional HIPAA issues focus on the need for documenting each policy and process, knowledge and training on compliance regulations, facility access controls, workstation use and location and the review of logs and other auditing measures.

Note: The HITECH Act extended the reach of HIPAA. See [Appendix D](#) for additional details.

Note: As HIPAA data is defined as [highly sensitive data](#), in addition to the HIPAA specific requirements below, all HIPAA data must be protected as required by the [Electronic Storage of Highly Sensitive Data](#) policy and the [Institutional Data Protection Standards](#) for highly sensitive data.

	Yes	No	Documentation location or explanation for not following
A. Documentation			
1. Does your organization have complete and current formal documentation instructions for reporting security breaches including both report procedures and response procedures entity-wide? Do they include formal written mechanisms to document security incidents?			
2. Are documented formal procedures that establish and maintain personnel security in place and current?			
3. Does the organization maintain a record of the transport, movement, and location of hardware, software, and electronic media?			
4. Do you retain for at least six years after their last effective date all compliance planning records along with decisions and justifications?			

	Yes	No	Documentation location or explanation for not following
<p>5. Have access control policy and procedures been implemented which formally document authorization, establishment, and modification of system accounts which access protected healthcare information (PHI)? Do they include:</p> <ul style="list-style-type: none"> • Access-establishment information use policies and rules to determine initial right of access to a terminal, transaction, program, process or transfer to some other user? • Access-modification information policies and rules to determine the types of and reasons for modification to established right of access to a terminal, transaction, program, process or transfer to some other user? • Access authorization records? (Access authorization could be recorded as part of a job description or other policy for the end user that details level of access in accordance with job function.) • Assurance that operating and maintenance personnel have appropriate access authorization? 			
<i>B. Compliance Knowledge and Training</i>			
<p>1. Have you reviewed all Administrative Simplification regulations for their applicability to your business? (This refers to standardization of billing and claims transactions; contact the Office of the Director of Patient Financial Services for information about transactions and coding issues.)</p>			
<p>2. Are the mandated, formal policies and procedures about sanctions or disciplinary actions in place and communicated to the entire workforce including notice of civil or criminal penalties for the misuse or abuse of health information?</p>			

	Yes	No	Documentation location or explanation for not following
3. Does your organization have a documented, formal process assuring that security awareness training is provided on a routine basis, including all system users, workforce and maintenance personnel? Does this include periodic awareness reminders?			
<i>C. Facility Access Controls, Workstation Use and Location</i>			
1. Are formal, current physical access control policies and procedures in place which allow only appropriate access to an entity including visitor control, and control of access to software programs for testing and revision? Do they include: <ul style="list-style-type: none"> • Validation of access privileges prior to granting physical access to the facility/facilities? • A plan for security of the facility/facilities to safeguard against unauthorized access? 			
2. Are formal, current documented policies and procedures in place that <ul style="list-style-type: none"> • Decrease or limit the chance that PHI can be viewed inappropriately? (E.g., terminal placement in any area of a doctor's office where the screen contents can be viewed from the reception area.) • Define the functions, manner of performance, and physical attributes of the surroundings of a computer terminal site based on the sensitivity of the data accessed from that site? 			
3. Is each workstation and printer labeled to identify it as a part of a specific system or network and for maintaining inventory?			
<i>D. Review and Audit</i>			
1. Does the department take responsibility for monitoring its own compliance as required by Health System Policy 0217 (<i>Compliance Auditing and Monitoring Program</i>)?			

U.Va. IT Security Risk Management Program

	Yes	No	Documentation location or explanation for not following
2. Does the security awareness training program include mandatory information about monitoring log-in successes and failure and reporting discrepancies or suspicions?			
3. Are audit controls in place and documented to record and examine system activity?			
4. Is there a data authentication mechanism in place to corroborate that data have not been altered or destroyed? (This could include the use of a check sum, double keying, message authentication code, or digital signature.)			
Prepared by: Name: _____ Signature: _____ Title: _____ Date: _____	Approved by: Unit head Name: _____ Signature: _____ Title: _____ Date: _____		

Unit Name: _____ Sub-Unit Name: _____

Risk Assessment Questions: [GLBA](#) Supplement

These questions will help determine and evaluate threats to the resources identified through a mission impact analysis, as well as adherence to general secure computing practices.

In addition to the issues covered in the general questions, additional GLBA issues focus on the need for specific training of employees on GLBA compliance, confidentiality agreements and safeguards and the protection of paper-based data.

Note: Since GLBA data may be some combination of highly and moderately sensitive data, in addition to the GLBA specific requirements below, all GLBA data must be protected as required by the [Electronic Storage of Highly Sensitive Data](#) policy and the [Institutional Data Protection Standards](#) for highly and moderately sensitive data.

	Yes	No	Documentation location or explanation for not following
<i>A. Employee Training and Management</i>			
1. Do you train employees to take at least the basic steps below to maintain the security, confidentiality and integrity of customer financial information (hereafter “protected data”)? <ul style="list-style-type: none"> • Locking rooms, file cabinets where records kept • Locking access to terminals with strong passwords • Changing passwords periodically • Maintaining password confidentially, including not posting them • Encrypting sensitive customer communication when transmitted or stored electronically • Referring requests for information only to other authorized individuals who have been trained 			
2. Do you obtain signed confidentiality agreements from all employees handling protected data?			
3. Do you limit access to protected data to those who have a business reason to see it?			

	Yes	No	Documentation location or explanation for not following
B. Information Systems			
<p>1. Do you store records in a secure area?</p> <ul style="list-style-type: none"> • Paper records in a room, cabinet or container that is locked when unattended • Storage areas are protected from physical hazard like fire or flood • Store electronic data on a securely administered server located in a physically secured area, and limit local workstation storage as much as possible • Maintain and secure backups of protected data 			
<p>2. Do you provide for secure data transmission?</p> <ul style="list-style-type: none"> • Use SSL or other secure connection to encrypt protected data in transit • Caution customers and/or students against transmitting sensitive data by e-mail • If e-mail is used, secure the receiving account and encrypt transmission, if possible 			
<p>3. Do you dispose of protected data in a secure manner?</p> <ul style="list-style-type: none"> • Shred or recycle protected paper-based information securely • Remove all data and software from hardware and electronic media prior to transfer within U.Va. • Process all hardware and electronic media through Procurement's designated vendor when it is leaving U.Va. • Media include hard drives (from computers, printers, copiers, etc.), magnetic tapes, diskettes, CDs, DVDs and USB storage devices 			
<p>4. Do you use audit and oversight procedures to detect improper disclosure or theft of protected data?</p>			

	Yes	No	Documentation location or explanation for not following
<i>C. Detecting, Preventing & Managing Systems Failures</i>			
1. Do you follow the best practices outlined in the main question set? <ul style="list-style-type: none"> • Timely installation of software patches • Automatic anti-virus checking and updating • Backup • Mission continuity planning 			
2. Do you use tools like passwords and other personal identifiers to authenticate the identity of customers and/or students seeking to transact business electronically?			
3. Do you notify customers promptly if their non-public personal information is subject to loss, damage or unauthorized access?			
4. Do you ensure that all financial services contracts contain boilerplate language confirming third-parties will maintain appropriate safeguards?			
Prepared by: Name: _____ Signature: _____ Title: _____ Date: _____	Approved by: Unit head Name: _____ Signature: _____ Title: _____ Date: _____		

Unit Name: _____ Sub-Unit Name: _____

Risk Assessment Questions: [FERPA](#) Supplement

These questions will help determine and evaluate threats to the resources identified through a mission impact analysis, as well as adherence to general secure computing practices.

In addition to the issues covered in the general questions, additional FERPA issues focus on the need for specific training of employees on FERPA compliance, confidentiality agreements and safeguards and the protection of paper-based data.

Note: Since FERPA data is defined as moderately sensitive data, in addition to the FERPA specific requirements below, all FERPA data must be protected as required by the [Institutional Data Protection Standards](#) for moderately sensitive data.

	Yes	No	Documentation location or explanation for not following
<i>A. Employee Training and Management</i>			
1. Do you train employees to take basic steps to maintain the security, confidentiality and integrity of student information (hereafter “protected data”)? <ul style="list-style-type: none"> • Knowing which student data may be released without permission and which may not • Locking rooms, file cabinets where records kept • Locking access to terminals with strong passwords • Changing passwords periodically • Maintaining password confidentially, including not posting them • Encrypting sensitive customer communication when transmitted or stored electronically • Referring requests for information only to other authorized individuals who have been trained 			
2. Do you obtain signed confidentiality agreements from all employees handling protected data?			
3. Do you limit access to protected data to those who have a business reason to see it?			
4. Do you require completion of the FERPA Tutorial for anyone handling FERPA-protected data?			

	Yes	No	Documentation location or explanation for not following
B. Information Systems			
<p>1. Do you store records in a secure area?</p> <ul style="list-style-type: none"> • Paper records in a room, cabinet or container that is locked when unattended • Storage areas are protected from physical hazard like fire or flood • Store electronic data on a securely administered server located in a physically secured area, and limit local workstation storage as much as possible • Maintain and secure backups of protected data 			
<p>2. Do you provide for secure data transmission?</p> <ul style="list-style-type: none"> • Use SSL or other secure connection to encrypt protected data in transit • Caution customers and/or students against transmitting sensitive data by e-mail • If e-mail is used, secure the receiving account and encrypt transmission, if possible 			
<p>3. Do you dispose of protected data in a secure manner?</p> <ul style="list-style-type: none"> • Shred or recycle protected paper-based information securely • Remove all data and software from hardware and electronic media prior to transfer within U.Va. • Process all hardware and electronic media through Procurement's designated vendor when it is leaving U.Va. • Media include hard drives (from computers, printers, copiers, etc.), magnetic tapes, diskettes, CDs, DVDs and USB storage devices 			
<p>4. Do you use audit and oversight procedures to detect improper disclosure or theft of protected data?</p>			

	Yes	No	Documentation location or explanation for not following
<i>C. Detecting, Preventing & Managing Systems Failures</i>			
<p>1. Do you follow the best practices outlined in the main question set?</p> <ul style="list-style-type: none"> • Timely installation of software patches • Automatic anti-virus checking and updating • Backup • Mission continuity planning 			
<p>2. Do you use tools like passwords and other personal identifiers to authenticate the identity of customers and/or students seeking to transact business electronically?</p>			
<p>Prepared by:</p> <p style="padding-left: 40px;">Name: _____</p> <p style="padding-left: 40px;">Signature: _____</p> <p style="padding-left: 40px;">Title: _____</p> <p style="padding-left: 40px;">Date: _____</p>	<p>Approved by: Unit head</p> <p style="padding-left: 40px;">Name: _____</p> <p style="padding-left: 40px;">Signature: _____</p> <p style="padding-left: 40px;">Title: _____</p> <p style="padding-left: 40px;">Date: _____</p>		

Unit Name: _____ Sub-Unit Name: _____		
<h3 style="margin: 0;">Threat, Attack and Vulnerability Scenarios</h3> <p style="margin: 0;">In priority order, categorize each of the assets identified in Step 1 by threat; most assets are vulnerable to multiple threats. Then identify strategies that your department <i>currently</i> follows or <i>plans to</i> follow to address these threats.</p>		
Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
1. System Software		
<p><i>A. Automated or user-initiated network-aware attacks</i> (viruses, worms, trojan horses, peer-to-peer)</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> • Destroyed files • Exposed data • Lost productivity • Lost machine control • Lost IT staff time to rebuild machines 		<ul style="list-style-type: none"> <input type="checkbox"/> Automatic anti-virus software updates and regular scans <input type="checkbox"/> Don't open attachments <input type="checkbox"/> Limit use of attachments <input type="checkbox"/> Back up frequently <input type="checkbox"/> Patch applications, including e-mail clients <input type="checkbox"/> Managed desktop services <input type="checkbox"/> Configure automatic Windows Update or Microsoft Update <input type="checkbox"/> Departmental patching service <input type="checkbox"/> ITC's free Windows Patch Management <input type="checkbox"/> HS/CS free SMS update management service <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
<p>B. Malicious system misuse</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> • Ownership of shared resources (e.g. Web sites, research data) • Any resource with a password • Exposed data 		<ul style="list-style-type: none"> <input type="checkbox"/> Effective password policies (ITC HS/CS) <input type="checkbox"/> Access controls, including access revocation ASAP but no later than one day after transfer or termination <input type="checkbox"/> Don't allow applications to save passwords <input type="checkbox"/> Least privilege principal <input type="checkbox"/> Configure security settings properly, e.g. disable unused services <input type="checkbox"/> Move to ITC's more secure network or HS/CS's secure clinical subnet <input type="checkbox"/> ITC's Internet security scanning service <input type="checkbox"/> ISPRO's web application security scanning service <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
<p>C. Unmanaged (uncontrolled) software installation ("unknown" items installed along with intended items; untested or unstable programs that interfere with supported applications)</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> • System reliability • Lost productivity 		<ul style="list-style-type: none"> <input type="checkbox"/> Policies re testing software before deployment <input type="checkbox"/> Standard desktop configurations with limited administrator privileges <input type="checkbox"/> Managed desktop services <input type="checkbox"/> Unix server administration service <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
2. Data Integrity, Confidentiality and Availability		
<p>A. Compromise, theft and/or disclosure of databases (due to outsider cyberattack or malicious or accidental insider actions)</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> • Research databases • Grants • Reputation • Reproduction time • Effect on publishing (past, present, future) • Graduate student work • Financial, student, health, social security numbers and/or personnel information 		<ul style="list-style-type: none"> <input type="checkbox"/> Prevention: see 1.B. above <input type="checkbox"/> Periodically compare electronic data to paper (or off-line) data (e.g. backup) <input type="checkbox"/> Store data encrypted <input type="checkbox"/> Back up frequently <input type="checkbox"/> Use encrypted network data transport (SecureCRT, SecureFX, ssh; VPN) <input type="checkbox"/> Move to ITC's more secure network or HS/CS's secure clinical subnet <input type="checkbox"/> Regular staff training on legal requirements and Electronic Storage of Highly Sensitive Data Policy <input type="checkbox"/> Follow Electronic Data Removal policy <input type="checkbox"/> De-identify (anonymize) protected data used in research projects <input type="checkbox"/> Regularly scan with Identity Finder to remove non-essential highly sensitive data <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
<p>B. Data loss</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> Any resource with electronic data storage 		<ul style="list-style-type: none"> <input type="checkbox"/> File management practices <input type="checkbox"/> Back up frequently <input type="checkbox"/> Test backups <input type="checkbox"/> Off-site backup, documentation <input type="checkbox"/> Have ITC (HS/CS) manage or host services Win Unix <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
<p>3. Staffing</p>		
<p>A. People critical to support of IT equipment/ services not available (due to illness, weather, etc.)</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> IT staff 		<ul style="list-style-type: none"> <input type="checkbox"/> Cross-training <input type="checkbox"/> Remote access <input type="checkbox"/> Documentation of procedures and practices <input type="checkbox"/> Common procedures across departments with partnerships for mutual backfill <input type="checkbox"/> Contract for backfill <input checked="" type="checkbox"/> Escrowed passwords <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
<p><i>B. Untrained services administrators (system, database, Web, etc.)</i></p> <p>Consider these assets:</p> <ul style="list-style-type: none"> • Servers • IT staff 		<ul style="list-style-type: none"> <input type="checkbox"/> Hire appropriately <input type="checkbox"/> Provide thorough administrator training <input type="checkbox"/> Security training <input type="checkbox"/> Provide time for knowledge and skills maintenance <input type="checkbox"/> Provide time for on-going systems maintenance <input type="checkbox"/> Remote access restrictions <input type="checkbox"/> Strict access controls <input type="checkbox"/> Least privilege principal <input type="checkbox"/> Back up frequently <input type="checkbox"/> Have ITC (HS/CS) manage or host services Win Unix <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
4. Older and Specialized Hardware and Software		
<p><i>A. Non-replaceable equipment (no longer manufactured); operating systems no longer supported by vendor</i></p> <p>Consider these assets:</p> <ul style="list-style-type: none"> • Assets more than 3 years old • Specialty, unique systems 		<ul style="list-style-type: none"> <input type="checkbox"/> Fund technology migration in coordination with vendors' product end of life schedule <input type="checkbox"/> Interim manual procedures <input type="checkbox"/> Contingency plan for parts and emergency migration <input type="checkbox"/> Perform frequent, secure and tested backups <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
<p>B. "Black box" devices (non-upgradeable systems, often with unchangeable passwords)</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> Specialized devices with Web interfaces (e.g. facilities control modules) Non-computer "intelligent" devices on network; web-enabled appliances Engineering devices 		<ul style="list-style-type: none"> <input type="checkbox"/> Procurement contracts allowing for replacement as needed <input type="checkbox"/> Remove device from general network <input type="checkbox"/> Contingency plan for parts and emergency migration <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
<p>5. Equipment and/or Service Unavailability</p>		
<p>A. Unavailability of departmental IT equipment/services (due to damage from burst waterpipes, power failure, hard drive failure, confiscation by law enforcement for cybercrime investigation, denial of service attack, need to rebuild OS, human error, theft, etc.) – consider short and long term scenarios</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> All assets identified in Step 1 		<ul style="list-style-type: none"> <input type="checkbox"/> Back up frequently <input type="checkbox"/> Test backups <input type="checkbox"/> Partnerships with other departments (instead of redundant equipment) <input type="checkbox"/> Service contracts <input type="checkbox"/> Parts on hand <input type="checkbox"/> Off-site backup, documentation <input type="checkbox"/> Interim manual procedures <input type="checkbox"/> Have ITC (HS/CS) manage or host services Win Unix <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
<p>B. Unavailability of central IT equipment/services or voice communication services (due to network failure, equipment failure, denial of service attack, telecom overloads, etc.) – consider short and long term scenarios</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> All assets identified in Step 1 		<ul style="list-style-type: none"> <input type="checkbox"/> Partnerships with other departments <input type="checkbox"/> Interim manual procedures <input type="checkbox"/> Vendor contracts for services <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
<p>6. Loss of Facilities</p>		
<p>A. Short term – building intact, but no access (due to structural problems, biological or chemical contamination, etc.)</p> <p>B. Long term – building completely or substantially destroyed (due to fire, earthquake, missile attack, etc.)</p> <p>Consider these assets:</p> <ul style="list-style-type: none"> All assets identified in Step 1 Paper copies of procedures, policies and plans Local backups Local software media and licenses Loss of people 		<ul style="list-style-type: none"> <input type="checkbox"/> Back up frequently <input type="checkbox"/> Test backups <input type="checkbox"/> Partnerships with other departments <input type="checkbox"/> Redundant equipment <input type="checkbox"/> Alternate space plans <input type="checkbox"/> Vendor contracts for services <input type="checkbox"/> Interim manual procedures <input type="checkbox"/> Off-site backup, media, licenses and documentation <input type="checkbox"/> Have ITC (HS/CS) manage or host services Win Unix <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
7. Other: _____		
Consider these assets: • _____ • _____		<input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____
Prepared by: Technical contact: Name: _____ Signature: _____ Title: _____ Date: _____		Approved by: Unit head Name: _____ Signature: _____ Title: _____ Date: _____

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
<p>B. Disaster Recovery Components</p>	
<p>1. List the team leader and members of your designated recovery team.</p> <p>Include name, title, responsibility, e-mail address and telephone number(s) of each member.</p>	
<p>2. Do you have the necessary University and departmental personnel contact lists?</p> <ul style="list-style-type: none"> • 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)? <p>See CIMP for official University notification procedures. (Those in the Health System should route notification through HS/CS.) All contacts with the public regarding the incident should be routed through University Relations (Media Relations in the Health System).</p>	
<p>3. Do you have hardware diagrams and system configurations, including physical and data security issues?</p>	
<p>4. Do you have infrastructure information about your facilities (requirements for power, cooling, network cabling, etc.)?</p>	
<p>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.)</p>	

	Documentation Location and/or Decision
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? <ul style="list-style-type: none"> • 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?	

	Documentation Location and/or Decision
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?	
18. Do your plans incorporate research groups that otherwise operate independently or ensure sure they have made plans of their own? For example, researchers who have critical data (i.e., highly sensitive or on which valuable grants depend).	
Prepared by: Administrative contact Name: _____ Signature: _____ Title: _____ Date: _____	Prepared by: Technical contact Name: _____ Signature: _____ Title: _____ Date: _____
Approved by: Unit head Name: _____ Signature: _____ Title: _____ Date: _____	

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.

A. 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.

2. Scope of the Mission Continuity Plan

INSERT here what your plan covers and does NOT cover.

3. 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.

4. Interfaces

INSERT here a list of any inbound or outbound interfaces to other systems required for the departmental application's operation.

5. 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.

6. 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.

7. Interim Manual Procedures (aka Downtime Procedures)

INSERT here references to existing documented procedures to be used during a system outage.

B. 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.

2. 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.

3. Vendor Contact List

INSERT here contact information (names, phone, email, US 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.

4. 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.

5. 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 (HS/CS, ITC or a Hot or Cold site vendor), notification procedures should be included.

C. 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 HS/CS, ITC or other entity on behalf of the department.

2. 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.

3. 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.

4. 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.

5. 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 HS/CS or ITC network team to detail and diagram any alternative network connections required.

D. 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.

2. 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.

3. 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.

4. 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.

5. 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.

E. 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.).

2. 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.

F. 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.

2. 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.

G. 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.

2. 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.

3. 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).

4. [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.

H. 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.

I. 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:

Unit Name: _____ Sub-Unit Name: _____

Evaluation and Reassessment Questions

Complete every three years or when there are significant changes to departmental IT assets or risk environment (see [Table 1](#): Critical Asset Criteria). The process gets easier because you are building on your earlier effort. All questions refer to the time period since the last evaluation.

A. Evaluation

1. Have you adequately protected what your analysis said you should?

2. Has there been any loss, unavailability, corruption or inappropriate disclosure of critical IT assets or data? If so, how effective was the response?

B. Reassessment

1. Have you changed your operating system?

Examples: Windows to UNIX/Linux, Windows XP to Windows 7, Mac OS to Windows

<p>2. Have you changed any critical applications?</p> <p><i>Example:</i> Migrated compliance database from Access to SQL Server.</p>	
<p>3. Are there any new critical data housed in your department?</p> <p><i>Note:</i> Data may be critical based on mission criticality, sensitivity or protected status.</p>	
<p>4. Are there any new state or federal standards or University policies or standards applicable to your department? If so, to which systems and/or data do they apply?</p>	
<p>5. What risk mitigation that you could not afford previously can you now afford, or – due to increased risk in that area – you can no longer afford not to mitigate?</p>	
<p>6. Are there any new technologies allowing for easier and/or cheaper mitigation for certain risks?</p>	
<p>7. Has there been an increase or decrease in the number of servers (physical and virtual) or systems?</p>	
<p>8. What interim risk mitigation measures have been put in place for new systems?</p>	

9. Are there any systems that are no longer mission-critical? If so, are there risk mitigation efforts that can be discontinued?	
10. What functions have been moved to central servers, so that you no longer have risk management responsibility for them?	
11. What functions have been moved to local servers, so that you now have risk management responsibility for them?	
12. What new functions has your department taken on in pursuit of its mission? Are any IT-asset-dependent?	
13. What old functions have become IT-asset-dependent?	
14. What relevant personnel turnover, additions or subtractions, or role changes have occurred?	
15. Do you have any long-term backups (archives) that need to be refreshed on new media (or destroyed)? (Please review and follow Records Management guidance regarding retention and disposition of records.)	
Prepared by: Administrative contact Name: _____ Signature: _____ Title: _____ Date: _____	Prepared by: Technical contact Name: _____ Signature: _____ Title: _____ Date: _____
Approved by: Unit head Name: _____ Signature: _____ Title: _____ Date: _____	