DRAFT

Office Name: ___________________________	
Business 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.	
1. What's your department's mission?	
2. Identify essential business functions. **Note:** A business function is essential if disruption or degradation of the function prevents the agency from performing its mission, as described in the agency mission statement. 2A. Identify dependent functions, if any. Determine and document any additional functions on which each essential business function depends. These dependent functions are essential functions as well.	
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 you have identified above. Be sure to include individual, departmental, ITU and external (e.g., vendor) assets as appropriate. Complete System Asset documentation for each asset. *Examples*: •Servers (including those hosted by others) •Desktops/laptops/PDAs that host critical or protected data	Attach Completed System Asset Document

4. What IT software and data assets are critical to the performance of those key functions? Please list these assets, the corresponding Data Owner and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, ITU and external (e.g., vendor, federal and state data swapping) assets as appropriate. *Examples*: •*Academic*: instructional resources, student data, databases necessary to maintain a given research program •*Administrative*: protected student or financial data necessary for business operations and student services •*Health-related*: protected patient data, both clinical and research •External data provider	
5. 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, ITU and external (e.g. vendor) personnel as appropriate. *Examples*: • Server administrators • Database administrators	
6. Please use the following space to report any security concerns or questions that you feel are important.	
Prepared by: Departmental Risk Assessment Coordinator Name: ___________________________ Signature: ___________________________ Title: ___________________________ Date: ___________________________	
Approved by: Unit head Name: ___________________________ Signature: ___________________________ Title: ___________________________ Date: ___________________________	

DRAFT

DRAFT

Unit Name: ____________________			
Risk Assessment Questions: General These questions will help determine and evaluate threats to the resources identified through a business impact analysis, as well as adherence to general secure computing practices.			
	Yes	No	Documentation location or explanation for not following
A. Physical Security			
Staffing 1. Is there someone in addition to the police department, responsible for building security?			
2. Are procedures in place to review/change access permissions when an employee leaves the department?			
3. Do you conduct background checks on prospective employees? Current employees?			
Building Security 1. Can exit doors be opened only from the inside to prevent unauthorized entry?			
2. Are all computers located in areas that are not easily accessible to outsiders?			
3. Are mission critical systems located in a locked location to which access is restricted to authorized personnel only?			
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 authorized personnel the only ones with access to departmental keys?			

DRAFT

	Yes	No	Documentation location or explanation for not following
7. Are department servers physically secure in a separate area?			
8. Are there employee work areas that are separate from public areas? Are their signs posted to clarify this distinction?			
9. Is access to work areas only through a reception area?			
10. Is there any access to second story windows from the outside?			
11. Are all windows locked at the end of the day? Do all exterior windows have sturdy locks?			
12. If you have an alarm system, do all exterior windows and doors have contacts?			
13. If you have an alarm system do you test it on a routine basis?			
14. Do you have back-up power and/or auxiliary systems in the event of black-out?			
15. Are ventilation ducts and access points secured or blocked from unauthorized entry?			
16. Are reception and work areas designed to prevent unauthorized entry?			
17. Can workers observe individuals in waiting and other public access areas?			
18. Please use the following space to report any security concerns or questions that you feel are important.			

	Yes	No	Documentation location or explanation for not following
Physical Security Measures 1. Physical barriers (Plexiglas partitions, elevated counters to prevent people from jumping over them, bullet-proof customer windows, etc.)?			
2. Security cameras or closed circuit TV in high-risk areas?			
3. Alarm systems?			
4. Other security features such as metal detectors, X-ray machines, swipe card access, motion detectors?			
5. Are spaces with sensitive systems behind door locks? Cipher or other "sophisticated" locks?			
6. Key control and other access procedures in place?			
7. Information posted on how to obtain emergency assistance?			
Workplace Procedures 1. Is public access to the building controlled?			
2. Are visitors or clients escorted to offices for appointments?			
3. Are authorized visitors to the building required to wear ID badges?			
4. Are identification tags required for staff (omitting personal information such as the person's last name and social security number)?			
5. Do you have the make, model and serial numbers recorded for all equipment?			

DRAFT

DRAFT

	Yes	No	Documentation location or explanation for not following
6. Where is that information recorded? Who has access to it? It is available in a situation where you do not have access to your building?			
7. Are uninterruptible power supplies (UPS) with surge protection used on servers and other important hardware?			
8. Are surge protectors (at least) used on desktop computers?			
9. Are individual firewalls installed on any desktops, laptops or servers in the department?			
10. Are security events on desktops, laptops and servers reported to the ITU Support Center?			
11. Is there an accurate inventory of all computing equipment and software? If so, is a copy of the inventory stored off-site?			
12. Please use the following space to report any security concerns or questions that you feel are important.			
B. Account & Password Management			
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? i.e. Prohibit the storage of passwords in clear text.			
3. Do you explicitly grant physical and logical access to sensitive IT systems and data and the facilities that house them based on the principle of least privilege?			
4A. Do you have established policies and procedures for approving and terminating authorization to IT systems?			

	Yes	No	Documentation location or explanation for not following
4B. Do you lock an account automatically if it is not used for a predefined period? 4C. Do you disable unneeded accounts? 4D. Do you promptly remove access to sensitive data when no longer required?			
5A. Do you require that at least two individuals have administrative accounts to each critical IT system, to provide continuity of operations?			
6. Does the department disallow sharing accounts? (E.g., if multiple people need to review the same messages, use a listserv; for file servers, use group memberships rather than generic 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?			
9. Does the department assist users in selecting passwords that will ensure privacy while promoting regular use? (See the IT Security Office website Desktop Security Step 2)			
10A. Does the department educate users that they should not share or write down passwords? 10B. Does the department prohibit the transmission of identification and authentication data (e.g., passwords) without the use of industry accepted encryption standards?			
11A. Do you require the use of a non-shared and a unique password on each account on IT systems, including local, remote access and temporary accounts? 11B. Do you require passwords on mobile devices issued by the agency such as PDAs and smart phones. For mobile phones, use a pin number with a			

DRAFT

DRAFT

	Yes	No	Documentation location or explanation for not following
minimum of 4 digits?			
12. Does the department require that passwords be periodically changed?			
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?			
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 multiple tries to enter a password for a given account? (The George Mason Internal Auditors recommend locking out a user after three unsuccessful login attempts.)			
17. Does the department disallow modems attached to servers and desktops that can receive calls?			
18. Please use the following space to report any security concerns or questions that you feel are important.			
C. Virus Protection			
1. Is 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 their hard drives regularly, in addition to updating the virus definitions?			

DRAFT

	Yes	No	Documentation location or explanation for not following
4. If users become infected with a computer virus, do they know what to do?			
5. Has the department reminded users to open only attachments they are expecting?			
D. Data Backup and Recovery			
1. Are faculty and staff aware 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?			
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. Does the department comply with Commonwealth of Virginia Library archive requirements?			
6. Are backup needs periodically reviewed?			
8. Please use the following space to report any security concerns or questions that you feel are important.			
E. Operating Systems			
1. Are appropriate operating system updates and security patches being applied in a timely manner to all department computers and servers? Windows users can use Microsoft's Baseline Security Analyzer (MBSA).			
2. Have unnecessary services and features in desktop and server operating system configurations been disabled?			
3. Is the use of shared drives or folders between desktop computers (peer-to-peer sharing) prohibited or restricted?			

	Yes	No	Documentation location or explanation for not following
F. Application Software			
1. Are appropriate application software updates and security patches being applied in a timely manner to all department computers and servers?			
2. Has the macro security level been set to medium or high in MS Office applications?			
3. Have faculty and staff been instructed to place on-line orders only through secure Web sites?			
4. Does the staff have the appropriate level of access to applications based on their current responsibilities? (Need to know).			
5. Is application access promptly removed for employees who have left the department?			
6. Please use the following space to report any security concerns or questions that you feel are important.			
G. Confidentiality of Sensitive Data			
1. Are all locations of automated and manual sensitive data records in the department known?			
2. Is access to sensitive data under the department's control restricted?			
3. Is ownership of data clearly defined?			
4. Do data owners determine appropriate levels of data security required? Data Stewardship Policy 1114			
5. Is sensitive data removed from hardware, software and media prior to reuse or disposal according to Commonwealth Guidelines?			
6. Have the faculty who are conducting research determined if the data they are collecting should be classified as sensitive?			

DRAFT

	Yes	No	Documentation location or explanation for not following
7. Do the faculty and staff who administer sensitive data understand and follow appropriate federal, state, grant agency, or university policies for protecting and backing up data?			
8. Are student workers given access to sensitive teaching, research or administrative data? If so, is their use of such data monitored closely?			
9. Are user agreements clearly stating required authentication and protection levels established with all external agencies and institutions with which data are shared?			
10. Is the unencrypted transmission of sensitive data or memos through e-mail discouraged?			
11. Do web-enabled transactions that require user authentication, transfer sensitive data, or transfer funds use encryption, such as SSLv3?			
12. For employees who have remote access to the Banner aware that a Virtual Private Network (VPN) must be running to access these areas?			
13. 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?			
14. If the department has a wireless network, is the network encrypted? If so, what type of encryption is used?			
15. Are encryption key management policy and procedures in place to ensure the integrity and recovery of encryption keys?			
16. Please use the following space to report any security concerns or questions that you feel are important.			

DRAFT

	Yes	No	Documentation location or explanation for not following
H. Security Awareness and Education			
1. Do the faculty and staff fully understand their responsibility for computer security?			
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?			
4. Have University and department-specific security policies and procedures been documented and shared with all faculty and staff?			
5. Are faculty and staff keeping current on Mason on Alert and ITU Support Center Alerts?			
6. Are suspected violations of security appropriately reported to a designated system or departmental administrator?			
7. Do your computer support personnel attend S.A.L.T. meetings and 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?			
I. Publicly Accessible Computers (Computing lab, public kiosks, etc.)			
1. Are the computers created with a software image configured for the greatest practicable restrictions on disk access, software installation and user rights?			

DRAFT

	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?			
4. Is information posted (either by sign or login 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?			
J. Review and Response			
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 particularly sensitive systems and infrastructures 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 known 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 firewall technology have security logging turned on?			
7. Please use the following space to report any security concerns or questions that you feel are important.			

DRAFT

Prepared by:	Approved by: Unit head
Name: ____________________________	Name: ____________________________
Signature: ____________________________	Signature: ____________________________
Title: ____________________________	Title: ____________________________
Date: ____________________________	Date: ____________________________

DRAFT

Unit Name: ________________________

Risk Assessment Questions: Gramm Leach Bliley Act (GLBA) and Family Education Rights Privacy Act (FERPA) Supplement

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

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

All questions in this supplement apply to both GLBA- and FERPA-protected data unless specifically labeled.

	Yes	No	Documentation location or explanation for not following
A. Employee Training and Management			
1. Do you train employees to take basic steps to maintain the security, confidentiality and integrity of customer financial information and/or student information (hereafter "protected data")? • **[FERPA]** 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 your require security awareness training for all employees handling protected data?			
4. Do you limit access to protected data to those who have a business reason to see it?			
5. Please use the following space to report any security concerns or questions that you feel are important.			
	Yes	No	Documentation location or explanation for not following

DRAFT

DRAFT

B. Information Systems			
1. Do you store records in a secure area? • 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			
2. Do you provide for secure data transmission? • 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			
3. Do you dispose of protected data in a secure manner? • Shred or recycle protected information securely • Erase or destroy all media (diskettes, CD-ROMs, hard drives) containing protected data according to [Commonwealth Guidelines]			
4. Do you use audit and oversight procedures to detect improper disclosure or theft of protected data?			
5. Please use the following space to report any security concerns or questions that you feel are important.			
C. Detecting, Preventing & Managing Systems Failures			
1. Do you follow the best practices outlined in the main question set? • Timely installation of software patches • Automatic anti-virus checking and updating • Backup • Business continuity planning			

	Yes	No	Documentation location or explanation for not following
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. **[GLBA]** Do you notify the ITSO promptly if their non-public personal information is subject to loss, damage or unauthorized access?			
4. **[GLBA]** Do you ensure that all financial services contracts contain boilerplate language confirming third parties will maintain appropriate safeguards?			
5. Please use the following space to report any security concerns or questions that you feel are important.			

Prepared by:

Name: ___________________________

Signature: ___________________________

Title: ___________________________

Date: ___________________________

Approved by: Unit head

Name: ___________________________

Signature: ___________________________

Title: ___________________________

Date: ___________________________

DRAFT

DRAFT

Unit Name: ___________________

Business Continuity Questions

The development of a plan for restoration of resources identified in the business impact analysis and for interim manual processes for continuing critical business functions during the restoration process.

	Documentation Location and/or Decision
A. Downtime Procedures – (Business Continuity - Disaster Recovery)	
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? Note: Please repeat for each identified function.	
4. Please use the following space to report any security concerns or questions that you feel are important.	

	Documentation Location and/or Decision
B. Disaster Recovery Components	
1. Who are the 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 should be notified in case of a business continuity problem? • Who will be responsible for responding to a business continuity problem? • How will you contact them in an emergency situation (pager, cell phone, call lists)? See the Safety Office website for official University notification procedures. All contacts with the public regarding the incident should be routed through University Relations.	
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 wary 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.)	

DRAFT

	Documentation Location and/or Decision
6. Do you have a current inventory of your hardware, software and critical data files? Is it updated in real time?	
7. 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?	
8. Do you have a plan for emergency procurement?	
9. 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?	
10. 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.)	
11. Is system and recovery information stored off-site in a 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	
12. Do you test your plan annually? When was the last test?	
13. Do you update your plan after each test, or when there is a significant technology change?	
14. What training do you have for staff involved with the plan, including communicating and testing the plan?	

DRAFT

	Documentation Location and/or Decision
15. Do departmental personnel know what to do and whom to contact within the department and /or University if a computer security or a disaster incident should occur?	
16. Are recovery and continuing operations instructions written in simple, clear, complete sets of steps that upset, fatigued people could follow correctly?	
17. Do you have faculty or staff (e.g., researchers) who have critical data (e.g., on which valuable grants depend or which contain legally protected data) but provide their own computing support outside departmental resources? How do you ensure they are included your plans or adopt plans of their own?	
18. Please use the following space to report any security concerns or questions that you feel are important.	
Prepared by: Administrative contact Name: ____________________________ Signature: ____________________________ Title: ____________________________ Date: ____________________________	Prepared by: Technical contact Name: ____________________________ Signature: ____________________________ Title: ____________________________ Date: ____________________________
Approved by: Unit head Name: ____________________________ Title: ____________________________	Signature: ____________________________ Date: ____________________________

DRAFT