

**Comments**

*Use your browser's Back button to return to the CAT questionnaire.*

|  |  |
| --- | --- |
|  | |
| **Information Technology** | |
|  | |
| **Question :** | **1.** Are faculty and staff members familiar with the university’s information technology policies and guidelines? |
| **Comments:** | Due to the increased use of information technology resources, all employees are required to understand university policies and guidelines for the use of computers. This should include a general understanding of data security and appropriate uses of hardware and software. Requiring employees to certify that they read and understand relevant Policies and Standards is one method by which management can insure accountability and acceptance of enforceable standards. |
|  | |
| **Question :** | **2.** Are unit IT risk assessments conducted annually? |
| **Comments:** | A successful risk assessment hinges upon the accurate collection of information regarding system strengths, weaknesses, and capabilities. Risk is commonly represented by the probability and impact of occurrence. A risk assessment should be considered by management as an essential function to ensure that the organization is not impaired in the accomplishment of its mission and goals. All management levels should be involved in a risk assessment process; consideration should be given not only to the resources needed to accomplish the organization’s mission but also to ensure confidentiality, integrity, and availability of systems and data. |
|  | |
| **Question :** | **3.** Does a business continuity plan exist which identifies critical activities, backup files, programs, and alternative processing sites? |
| **Comments:** | Each unit should develop, document, and test a plan for continuing operations in the event of a catastrophe, or a serious computer malfunction or information security incident. For units that operate a local area network, such a plan should address the loss of one or more servers. The plan should address the possibility of losing a computer system for several days to several weeks. Staff should be familiar with what files are backed up regularly through the network and critical files that they may have to manually back up. A business continuity plan should be in place that addresses expected scenarios and be flexible enough to adapt to unexpected situations. In the event of a disaster, individuals involved in the recovery of a system or services should be well versed in the actions that they need to undertake. The plan should be documented in such a way that actions related to specific individuals are clearly outlined. |
|  | |
| **Question :** | **4.** Have change management procedures been established, including patch management, for portable computers, workstations, and servers? |
| **Comments:** | In a computing environment, with somewhat open and decentralized operations, a clear and logical path of authority regarding modifications to IT systems is critical. Ensuring only authorized changes are made reduces the risk of problems due to improper/out-of-date safeguards, software conflicts, and usability. Change management must include procedures to regularly identify and mitigate potential risks. Patch management solutions need to be comprehensive to cover updates at both the operating system level and installed applications to provide adequate protection against all types of software vulnerabilities. |
|  | |
| **Question :** | **5.** Are system security and application access logs enabled and reviewed periodically for unauthorized access and anomalies? |
| **Comments:** | System logs can assist management in the detection of program errors and system attacks. Procedures must be in place to ensure that system logs are periodically reviewed. Where possible, automated review should be enabled and alerts transmitted to appropriate staff. |
|  | |
| **Question :** | **6.** Are backups of operating systems, critical data, and key software programs made on a regular basis and stored at an off-site location? |
| **Comments:** | For computers that are operated by a unit (servers, stand-alone machines, etc.), a copy of the operating system (e.g., Windows, UNIX), programs, and critical data files should be stored in a location separate from the unit. This will allow easier recovery from a fire, flood, or other disaster that may destroy the unit’s site. Personnel should be educated about the need to maintain backups of their critical files that are not on the server. Restoring from backups should be periodically tested. |
|  | |
| **Question :** | **7.** Are documented procedures in place for reviewing and removing access to all production systems when an employee leaves the unit or is assigned to a different role within the unit? |
| **Comments:** | Each unit is required to have procedures to ensure that access to the system is revoked when employees terminate their employment with the unit. The removal of access should be completed immediately to reduce the risk of unauthorized activities. |
|  | |
| **Question :** | **8.** Is sensitive and restricted data managed by the unit (on networks, personal computers, and back up media), classified and protected by restricted access, encryption, or other controls? |
| **Comments:** | Most units have sensitive or restricted data. This may include student data, personnel data, employee evaluations, research data, patient data, etc. Access to this information should be restricted as needed. This may include storing information off a network, encrypting files, or perhaps making data ‘read only’ so that it cannot be altered or deleted. Backup files may be stored off site provided the confidentiality of the files are protected, such as encrypting the files. |
|  | |
| **Question :** | **9.** Are records of all software licensing agreements managed by the unit properly maintained? |
| **Comments:** | Legal rights to use software are granted in accordance with the terms and conditions of the license purchase. As with any other valuable asset, units must ensure that computer software is properly managed to reduce related costs. Among other things, management should develop procedures to ensure that records of all software licensing agreements are adequately maintained and that all purchased licenses are needed. |
|  | |
| **Question :** | **10.** Is antivirus software installed, operating and up to date for all computing resources (laptops, desktops, servers, etc)? |
| **Comments:** | Anti-virus software is required to be installed and maintained on every computer. It should be setup so that:   An auto update to the DAT file and scan engine is performed daily, and the user is unable to disable/delay the update without outside approval from the appropriate network administrator.   The scan runs at a regularly scheduled time, with the results of the scan reported back to the I.T. administrator in charge of the machine(s).   The user is unable to disable/delay the scheduled scan, without outside approval from the appropriate network administrator. |
|  | |

Top of Form



Bottom of Form



**References**

*Use your browser's Back button to return to the CAT questionnaire.*

|  |  |
| --- | --- |
|  | |
| **Information Technology** | |
|  | |
| **Question :** | **1.** Are faculty and staff members familiar with the university’s information technology policies and guidelines? |
| **References:** | *Office of Information Technology* Policies and Standards  <http://www.it.ufl.edu/policies/>  Chapter 6C1-1.0102 *University of Florida Regulations* Policies on Information Technology  <http://regulations.ufl.edu/chapter1/10102.pdf>  *UF Privacy Office* HIPAA & Privacy - General Awareness  <http://privacy.health.ufl.edu/training/hipaaPrivacy/instructions.shtml> |
|  | |
| **Question :** | **2.** Are unit IT risk assessments conducted annually? |
| **References:** | *Office of Information Technology* UF IT Security Risk Assessment Standard  <http://www.cio.ufl.edu/policies/security/uf-it-sec-risk-assessment.html> |
|  | |
| **Question :** | **3.** Does a business continuity plan exist which identifies critical activities, backup files, programs, and alternative processing sites? |
| **References:** | *Office of Information Technology* UF IT Security Continuance of Operations Standards  <http://www.it.ufl.edu/policies/security/uf-it-sec-cop.html> |
|  | |
| **Question :** | **4.** Have change management procedures been established, including patch management, for portable computers, workstations, and servers? |
| **References:** | *Office of Information Technology* UF Network and Host Security Standard and Procedures  <http://www.it.ufl.edu/policies/security/uf-it-sec-network.html> |
|  | |
| **Question :** | **5.** Are system security and application access logs enabled and reviewed periodically for unauthorized access and anomalies? |
| **References:** | *Office of Information Technology* UF Network and Host Security Standards and Procedures  <http://www.it.ufl.edu/policies/security/uf-it-sec-network.html> |
|  | |
| **Question :** | **6.** Are backups of operating systems, critical data, and key software programs made on a regular basis and stored at an off-site location? |
| **References:** | *Office of Information Technology* UF Guidelines for IT Workers to Protect Restricted Data on Backup Media  <http://www.it.ufl.edu/policies/security/documents/it-worker-backup-guidelines.pdf> |
|  | |
| **Question :** | **7.** Are documented procedures in place for reviewing and removing access to all production systems when an employee leaves the unit or is assigned to a different role within the unit? |
| **References:** | *Office of Information Technology* UF Network and Host Security Standard and Procedures  <http://www.it.ufl.edu/policies/security/uf-it-sec-network.html>  *Office of Information Technology* Information Technology Security Policy  <http://www.it.ufl.edu/policies/security/index.html>  SPICE Policies and Standards: User Account and Password Management  <https://security.health.ufl.edu/policies/#ts0005> |
|  | |
| **Question :** | **8.** Is sensitive and restricted data managed by the unit (on networks, personal computers, and back up media), classified and protected by restricted access, encryption, or other controls? |
| **References:** | *Office of Information Technology* UF IT Data Security Standard  <http://www.it.ufl.edu/policies/security/uf-it-sec-data.html> |
|  | |
| **Question :** | **9.** Are records of all software licensing agreements managed by the unit properly maintained? |
| **References:** | *Office of Information Technology* UF Network and Host Security Standard and Procedures  <http://www.it.ufl.edu/policies/security/uf-it-sec-network.html> |
|  | |
| **Question :** | **10.** Is antivirus software installed, operating and up to date for all computing resources (laptops, desktops, servers, etc)? |
| **References:** | *Office of Information Technology* UF Information Technology Security Principles  <http://www.it.ufl.edu/policies/security/introduction.html>  *Office of Information Technology* UF Network and Host Security Standard and Procedures  <http://www.it.ufl.edu/policies/security/uf-it-sec-network.html> |
|  | |

Top of Form



Bottom of Form