



Risk Assessment Checklist

Please review this checklist when:

- Evaluating the information technology risk for a department.
- Changing the data management or technology management of your operation.
- Considering purchase of a new information technology resource.
- Considering the outsourcing of an information technology or data management operation.
- Staff or processes change, or on a regular audit basis, periodically or annually.
- Processing payment card, credit card or medical data.

All statements are designed for an answer or YES or TRUE. If you have answered NO to any question, or if you have any questions, please contact University Technology Services, Helpdesk, for assistance.

Domain: Personnel

1. Staff members have completed review of IT policies.
2. Staff members have completed security training on the UHR web site.
3. Staff members are aware of appropriate SSL/https web site usage.
4. Staff members are trained on the Desktop Emergency Guide information technology compromises and understanding reporting procedures.
5. Access to information technology resources and data are based on need to know and job responsibilities.
6. Passwords are protected, not written down, and kept confidential.
7. Staff members do not log on to any resource, then turn that resource over to another individual for use.
8. Accounts are immediately deactivated for terminated or transferred employees.

Domain: Infrastructure Assets

1. Key or critical department functions are documented.
2. Hardware assets are documented in an asset database, including system administrator, model number, serial number, operating system, purchase record. The record is stored internally, with a copy off-site.
3. Software assets are documented in an asset database, including license information, usage metrics, renewal date, and installation location.
4. All department functions and asset documentation are stored internally, with a recent (not more than 30 days old) copy off-site.
5. Systems are routinely backed up, with a verified and tested backup and restore procedure.

6. Backups are retained and cycled on a schedule approved by the data steward, and a copy is stored off site at a secure and approved location.

Domain: Data

1. Policy #860 Information Security has been reviewed and implemented.
2. All locations of confidential data used in departmental operations are known, documented and protected.
3. Confidential data are removed from information technology resources prior to reassignment or disposal of equipment.
4. Faculty members conducting research have determined if their research data are confidential and have protected the data accordingly.
5. Faculty and staff participating in federal, state, or grant agency operations or projects have determined if related data are confidential and have protected the data accordingly.

Domain: Communications

1. Confidential data are not distributed via email or instant messaging.
2. Secure file transmission or VPN are used for file transfer.
3. Cell phones have been purged of all data according to manufacturer's instructions prior to disposal or release.

Domain: Physical Security

1. Servers are protected by environmental controls, such as uninterruptible power supplies (UPS), surge protection, smoke detectors, fire suppression systems, water sensors, and temperature sensors.
2. All computers are in locations not easily accessible to outsiders.
3. Systems storing confidential data as defined in university Policy #860 are kept in a locked location with access restricted to authorized personnel.
4. Physical security has been reviewed with OUPD and/or Facilities.
5. Department carefully tracks access to keys.
6. Monitoring and surveillance solutions have been implemented where appropriate and in compliance with university Policy #674 Surveillance and Monitoring Technology.

Domain: Desktops, Laptops and Client Computing

1. Password-protection screen saver is enabled.
2. Firewall is installed.
3. Anti-virus software is installed and virus definitions up-to-date.
4. Operating system updates are performed on a regular basis.
5. Faculty and staff are aware of personal computer backup requirements and options.
6. Systems, copiers and storage devices are formatted and degaussed according to policy prior to equipment disposal, sale or donation.
7. Equipment is maintained to comply with the latest version of the Desktop Service Level Agreement.
8. Confidential data are not stored on laptops, or are stored with encryption enabled.
9. Publicly accessible computers are installed with a locked image, inability to store or cache personal data, and posted with a reminder to log out.

Domain: Server Considerations

1. Policy #880 Systems Administration Responsibilities has been reviewed and implemented.
2. Systems are regularly backed up, with a back-up copy stored off site, and restore processes tested and verified.
3. Vendor default passwords have been changed.
4. Unnecessary services and features have been disabled.
5. Operating system updates are performed on a regular basis.

Domain: Software Applications

1. All software is used in compliance with licensing and copyright.
2. Vendor security strategy reviewed annually.
3. Vendor default passwords have been changed.
4. Passwords comply with UTS posted password recommendations.
5. Vendor patch releases are promptly applied.

Domain: Network

1. Policy #850 Network Policy has been reviewed and implemented.
2. University network is used with care and respect for a shared resource.
3. Network has not been extended by using hubs or wireless access points without prior approval from University Technology Services.
4. Wireless network security has been reviewed.
5. VPN access is used for off-campus access.
6. Remote desktop access is limited and security of the desktop has been increased accordingly.

Domain: Payment or Credit Card Processing

1. Security audit completed with University Technology Services.
2. Related systems added to external vulnerability scanning agreement.
3. Staff members have completed cash handling training from Student Business Services.
4. UHR has verified that the employees have signed an agreement verifying they have read and understood the security policies and procedures, and that a background investigation (such as credit and criminal record check) has been done prior to the access to account numbers.
5. Risk Management has verified that any contractors or temporary employees with access to payment or credit card processing records or systems have appropriate contract protections in place.
6. Secure disposal of sensitive cardholder data and the retention period of such data prior to disposal have been verified.
7. Verify access control logging on the desktop or servers, including security review, successful and unsuccessful login attempts, access to audit logs, and root / administration access, and that logs are kept for one year.

8. Access control is defined on desktop, with the desktop access limited so that only the defined individual can access the desktop and then by unique username and password. Similar limited access must be implemented on relative servers.
9. A password protected screen saver that is enabled at 1 minute of inactivity is installed on all related desktops.
10. Verify that all passwords meet strong password requirements; minimum length of 8; mix of letters, numbers and special characters; password reuse limits; forced password change every 90 days; passwords stored in a hashed non-reversible form; account locked after 3 failed password attempts.
11. Cardholder processing, storage and transmission must be approved by both the data steward and the employee supervisor.
12. Verify that no remote access is allowed.
13. Verify account removal strategy for employee termination or contractor termination with the employee's supervisor and department director.
14. Verify ongoing account review requirements to ensure that malicious, out-of-date, unused or unknown accounts do not exist.
15. Verify that system installation procedures are documented, all unnecessary tools and services are removed, and that vendor default accounts, passwords and security settings are disabled or changed.
16. Verify that account numbers are sanitized before being logged in the audit log.
17. Verify that account numbers are not transmitted via email.
18. Verify that secure, encrypted communications are used for remote administration of production systems and applications.
19. Verify that all desktop operating systems, desktop office applications and any other software are regularly updated with the latest security-related patches.
20. Verify that there a virus scanner installed and regularly updated.
21. Verify that laptops are not used.
22. Verify backup procedures and that procedures are in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data.
23. Verify that all changes to the computer are formally documented, authorized, planned, and logged before being implemented.
24. Verify that the system clock is synchronized, and that logs include data and time stamp.
25. Verify that all media devices store cardholder data properly, are inventoried and are securely stored.
26. Verify that software used on the desktop was developed based on industry best practice and that information security included throughout the software development life cycle (SDLC) process.
27. If web applications are involved verify that the Open Web Application Security Project group (www.owasp.org) guidelines were taken into account in the development of Web applications
28. If web applications are involved verify that cookies are encrypted.
29. If web applications or database storage are involved, verify that UTS web servers are used, and if not, complete defined network and firewall assessments.

30. Verify that a security assessment, penetration test, or both performed on all Internet-facing applications in use.
31. Verify that if production data are used for testing and development purposes, that sensitive cardholder data are sanitized before usage.
32. Verify that all but the last four digits of the account number are masked when displaying cardholder data.
33. Verify that account numbers in the databases and in backup media are stored securely – for example, by means of encryption or truncation.
34. Verify that the CVC2/CVV2 or magnetic stripe data are not stored.
35. If an SQL database is used, verify that controls are implemented to prevent SQL injection and other bypassing of client side input controls.
36. Verify that transmissions of sensitive cardholder data are encrypted through the use of SSL version 3.0 or greater or other industry acceptable methods.
37. Verify that the wireless network is not used.
38. Verify that multiple physical security controls (such as badges, escorts, or mantraps) are in place that would prevent unauthorized individuals from gaining access to the facility and to equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data.
39. Verify that cardholder data are deleted or destroyed before physically disposed (for example, by shredding papers or degaussing backup media).
40. Verify that all cardholder data printed on paper or received by fax are adequately protected against unauthorized access.

Domain: Medical Data

1. Security audit completed with University Technology Services.
2. Related systems added to external vulnerability scanning agreement.
3. UHR has verified that the employees have signed an agreement verifying they have read and understood the security policies and procedures, have participated in HIPAA training, and that a background investigation (such as credit and criminal record check) has been done prior to the access to medical data.
4. Risk Management has verified that any contractors or temporary employees with access to medical data have appropriate contract protections in place.
5. Secure disposal of medical data and the retention period of such data prior to disposal have been verified.
6. Verify access control logging on the desktop or servers, including security review, successful and unsuccessful login attempts, access to audit logs, and root / administration access, and that logs are kept for seven years.
7. Access control is defined on desktop, with the desktop access limited so that only the defined individual can access the desktop and then by unique username and password. Similar limited access must be implemented on relative servers.
8. A password protected screen saver that is enabled at 1 minute of inactivity is installed on all related desktops.
9. Verify that all passwords meet strong password requirements; minimum length of 8; mix of letters, numbers and special characters; password reuse limits; forced

- password change every 90 days; passwords stored in a hashed non-reversible form; account locked after 3 failed password attempts.
10. Processing of medical data, including storage and transmission, must be approved by both the data steward and the employee supervisor.
 11. Verify that no remote access is allowed.
 12. Verify account removal strategy for employee termination or contractor termination with the employee's supervisor and department director.
 13. Verify ongoing account review requirements to ensure that malicious, out-of-date, unused or unknown accounts do not exist.
 14. Verify that system installation procedures are documented, all unnecessary tools and services are removed, and that vendor default accounts, passwords and security settings are disabled or changed.
 15. Verify that medical data are not transmitted via email.
 16. Verify that secure, encrypted communications are used for remote administration of production systems and applications.
 17. Verify that all desktop operating systems, desktop office applications and any other software are regularly updated with the latest security-related patches.
 18. Verify that there a virus scanner installed and regularly updated.
 19. Verify that laptops are not used.
 20. Verify backup procedures and that procedures are in place to handle secure distribution and disposal of backup media and other media.
 21. Verify that all changes to the computer are formally documented, authorized, planned, and logged before being implemented.
 22. Verify that the system clock is synchronized, and that logs include data and time stamp.
 23. Verify that all media devices store medical data properly, are inventoried and are securely stored.
 24. Verify that software used on the desktop was developed based on industry best practice and that information security included throughout the software development life cycle (SDLC) process.
 25. If web applications are involved verify that the Open Web Application Security Project group (www.owasp.org) guidelines were taken into account in the development of Web applications
 26. If web applications are involved verify that cookies are encrypted.
 27. If web applications or database storage are involved, verify that UTS web servers are used, and if not, complete defined network and firewall assessments.
 28. Verify that a security assessment, penetration test, or both performed on all Internet-facing applications in use.
 29. Verify that if production data are used for testing and development purposes, that medical data are sanitized before usage.
 30. Verify that medical data stored in a database and in backup media are stored securely – for example, by means of encryption.
 31. If an SQL database is used, verify that controls are implemented to prevent SQL injection and other bypassing of client side input controls.
 32. Verify that transmissions of medical data are encrypted through the use of SSL version 3.0 or greater or other industry acceptable methods.

33. Verify that the wireless network is not used.
34. Verify that multiple physical security controls (such as badges, escorts, or mantraps) are in place that would prevent unauthorized individuals from gaining access to the facility and to equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data.
35. Verify that computer screens are not visible to the visiting public.
36. Verify that medical data are deleted or destroyed before physically disposed (for example, by shredding papers or degaussing backup media).
37. Verify that all medical data printed on paper or received by fax are adequately protected against unauthorized access.