Guide to the
Advanced System
Informal Compliance Review (ICR)
V1.0 11/01/2004
Table of Contents

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Question</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction:</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Q1:</td>
<td>As System Owner or System Operator have you received general level privacy</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>and information security training and have you signed a Privacy,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality, and Data Security Agreement upon becoming a workforce</td>
<td></td>
</tr>
<tr>
<td></td>
<td>member?</td>
<td></td>
</tr>
<tr>
<td>Q2:</td>
<td>As System Owner or System Operator have you completed the System Owner</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>&amp; Operator Policy Compliance Training?</td>
<td></td>
</tr>
<tr>
<td>Q3:</td>
<td>Are those individuals who are granted system admin privileges provided</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>with job specific information security training?</td>
<td></td>
</tr>
<tr>
<td>Q4:</td>
<td>Does your department provide information regarding guidelines and</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>responsibilities associated with their computer and network privileges</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and resources?</td>
<td></td>
</tr>
<tr>
<td>Q5:</td>
<td>Does your department provide direction for reporting information</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>security events, incidents, and/or malfunctions (information security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>breach, threat, weakness, and/or calculated violation of trust)?</td>
<td></td>
</tr>
<tr>
<td>Q6:</td>
<td>Has the Sanction Policy been reviewed?</td>
<td>3</td>
</tr>
<tr>
<td>Q7:</td>
<td>Have you reviewed the roles and responsibilities of System Owner,</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>System Operator, and Data Custodian for the information and information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>systems within your System?</td>
<td></td>
</tr>
<tr>
<td>Q8:</td>
<td>Has the Policy Exception Request process been reviewed?</td>
<td>3</td>
</tr>
<tr>
<td>Q9:</td>
<td>For your System have you documented the System Owner and System</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Operator?</td>
<td></td>
</tr>
<tr>
<td>Q10:</td>
<td>Have you applied the information classifications of &quot;Public&quot;, &quot;Restricted&quot;</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>or &quot;Confidential&quot; to data contained within or used by your system?</td>
<td></td>
</tr>
<tr>
<td>Q11:</td>
<td>Are the following principles applied during job definition and the</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>delegation of System responsibilities?</td>
<td></td>
</tr>
<tr>
<td>Q12:</td>
<td>Is the workspace for systems you are responsible for kept clear of</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>restricted or confidential material while unattended or not in use?</td>
<td></td>
</tr>
<tr>
<td>Q13:</td>
<td>Are the following controls observed:</td>
<td>3</td>
</tr>
<tr>
<td>Q14:</td>
<td>Are duplication devices locked (or protected from unauthorized use in</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>some other way) outside of normal working hours?</td>
<td></td>
</tr>
<tr>
<td>Q15:</td>
<td>Do you dispose of media containing protected health information,</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>proprietary information, and other confidential information in a secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and confidential manner?</td>
<td></td>
</tr>
<tr>
<td>Q16:</td>
<td>Are active computing sessions terminated or secured by an appropriate</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>locking mechanism, e.g. a password protected screen saver when</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unattended?</td>
<td></td>
</tr>
<tr>
<td>Q17:</td>
<td>Are active computing sessions terminated when the computing session is</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>finished?</td>
<td></td>
</tr>
<tr>
<td>Q18:</td>
<td>Where feasible, is an automatic logoff (configured to logoff idle users)</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>being used to protect applications with confidential information?</td>
<td></td>
</tr>
<tr>
<td>Q19:</td>
<td>Are all networked computer systems within your responsibility left</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>powered on after working hours, including weekends and holidays?</td>
<td></td>
</tr>
<tr>
<td>Q20:</td>
<td>Are the Server Systems you are responsible for being housed in secure</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>areas that provide adequate physical and environmental controls?</td>
<td></td>
</tr>
<tr>
<td>Q21:</td>
<td>Is there a defined security perimeter and appropriate entry controls</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>protecting your Server Systems from unauthorized access, damage and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interference?</td>
<td></td>
</tr>
<tr>
<td>Q22:</td>
<td>Where there is an opportunity for fraud and abuse is separation of</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>duties observed during the performance of operational responsibilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>such as:</td>
<td></td>
</tr>
</tbody>
</table>
Q23: Has the System Owner and/or System Operator determined an appropriate backup schedule?

Q24: If your Server Systems require back-ups, are the backups scheduled and run regularly?

Q25: Have backup copies been tested to ensure that they are reliable?

Q26: Is a Maintenance & Operations Log (kept by) System Operators or designees?

Q27: Do System Operators review logs of operational events?

Q28: Are faults reported to your Help Desk?

Q29: Is system logging being performed on systems with confidential data or systems that are critical to the UW Medicine network?

Q30: Do your Networked Systems (systems on the network using wired or wireless technology) comply with the minimum requirements of the Networked System Information Security Standard?

Q31: Does your system have active protection against malicious software?

Q32: Does your system use TCP/IP with an address obtained through an IT Services Help Desk or University of Washington Campus & Computing (C&C) Help Desk ticket or a sanctioned DHCP server?

Q33: Is your system using a secure and approved operating system?

Q34: Are the operating system and applications patched and updated in a reasonably timely manner?

Q35: Is your Server System compliant with information security configuration and hardening guidelines and procedures?

Q36: Has a Server Systems backup and recovery plan been documented?

Q37: Is the Server System is in a secure/locked location?

Q38: Have all Server Systems that you are responsible for, which contain confidential information, been certified by IT Services SIT (Security Infrastructure Team)?

Q39: Is software installed only by designated system administrators as authorized by the System Owner or System Operator?

Q40: Are system administrators using designated administrative accounts only for system administrative work and using regular user accounts all other times?

Q41: Is system administrator access limited to those who required it to fulfill their job function?

Q42: Where anti-virus software is the method for protection against malicious software, is it set to update itself frequently (daily interval suggested) with the notification function?

Q43: Are virus incidents reported to your Help Desk?

Q44: Is the destruction of information handled consistent with its classification whatever the media - documents, computing systems, mail, multimedia, postal services/facilities, and/or use of fax machines?

Q45: Is information designated for destruction maintained in a secure and confidential manner prior to its final destruction and is it destroyed in a manner that assures no possibility of reconstruction?

Q46: Where appropriate, is physical labeling used to control media?

Q47: Do you use the logging of media to support accountability?
Q48: Are periodic spot checks or audits conducted to determine if any controlled items have been lost and to ensure that these items are in the custody of individuals named in control logs? ........................................................................................................................ 3
Q49: Is all electronic media intended for reuse subjected to media disposal (re-use) processes, such as overwriting or degaussing, to ensure the media is properly sanitized and to prevent the disclosure of protected or confidential information? ........................................ 3
Q50: Is your information retained according to UW Retention policies? .................................. 3
Q51: Are appropriate system access controls in place? ................................................................. 3
Q52: If you provide access to your system, is access granted based on the “Principle of Least Privilege” and the “Principle of Separation of Duties” as well as "Minimum Necessary"? ................................................................. 3
Q53: If you provide access to your system, is there appropriate user account management in place? ............................................................................................................................................ 3
Q54: Is access to multi-user information services controlled through a formal user registration process? ................................................................................................................ 3
Q55: If you provide access to your system, is each user issued a unique username and password? ....................................................................................................................................... 3
Q56: Are your users aware of the password usage guidelines outlined within the policy? ........ 3
Q57: Do you instruct users to only access UW Medicine resources that they have been authorized to use and that are necessary to perform their official job functions? .......................... 3
Q58: Does your system have a technical access control mechanism of some kind that allows for authorization and allocation of system and data resources to individual users? .......................... 3
Q59: If you have external connections like a VPN, have they been reviewed by UW Medicine SIT to insure information security compliance? ................................................................................................................................. 3
Q60: Are the operating systems you employ set to ........................................................................ 3
Q61: Are your applications enabled to control user access to information and application system functions? ............................................................................................................................................ 3
Q62: Are controls enabled in your applications to provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls? .................................................................................................................................. 3
Q63: Do applications provide safeguards against compromising the security of other systems with which information resources are shared? .................................................................................................................. 3
Q64: Do applications provide access to only the owner; other nominated authorized individuals; or defined groups of users? ................................................................................................................................. 3
Q65: Are access control mechanisms such as Access control lists (ACLs), Constrained User Interfaces, Encryption, Port Protection Devices, Secure Gateways/Firewalls, Host-Based Authentication being used within the environment as security controls? .................................................................................................................................................................................................. 3
Q66: If your system transmits electronic Protected Health Information (ePHI) outside of the University of Washington, is encryption being used to protect the data in transit? .................. 3
Q67: Based on your information and information system classification, has a business continuity plan been developed? ............................................................................................................................................ 3
Q68: Have regular reviews and updates to the business continuity plan been scheduled to ensure their continuing effectiveness? ............................................................................................................................................ 3
Q69: Do you understand that as the System Owner and/or System Operator, you must abide by UW Medicine information security policies and avoid breaches of criminal and civil law as well as contractual obligations of security requirements? ............................................................................................................................................ 3
Q70: Does the use of the software and information resources on your Systems match the specifications of the various software licenses? ................................................................. 3
Q71: Are you aware of federal software copyright law and UW Medicine’s intent to take disciplinary action against workforce that breaches them? ................................................ 3
Q72: Do you maintain proof and evidence of ownership of licenses, master disks, manuals, etc.? ...................................................................................................................... 3
Q73: As System Owner or System Operator are you aware you are responsible for:........ 3
Introduction:

This guide is intended for System Owners and/or System Operators requiring additional clarification and assistance in completing an ICR (Informal Compliance Review) for their System(s). The guide includes the questions on the Advanced System ICR with additional information, compliance specifics, and resources for each.

In general regarding the Advanced System ICR Guide:
- If the question does not apply to your System mark 100% compliant and explain why not within the ICR comments field.
- It is recommended that the “Your Comments” field within the ICR be used to track your ongoing tasks, issues, or action steps.

Q1: As System Owner or System Operator have you received general level privacy and information security training and have you signed a Privacy, Confidentiality, and Data Security Agreement upon becoming a workforce member?

In order to be compliant with this question:
- The System Owner and Operator of advanced System have completed the following have on file a signed Privacy, Confidentiality, and Information Security Agreement.
- For those who use or disclose Protected Health Information (PHI): Within 30 days of hire, you have completed New Workforce Member Orientation and/or you have completed HCCS on-line HIPAA training.
- The System Owner and Operator of advanced System have completed the Departmental training. (required for all employees)

Resources:

a) Department. Manager training – Slide #14 - https://security.mcis.washington.edu/istk
b) PP04 Information Privacy, Confidentiality, & Security Training – https://know1.mcis.washington.edu/proj_hipaa/
c) Privacy, Confidentiality, and Information Security Agreement - https://security.mcis.washington.edu/istk

Q2: As System Owner or System Operator have you completed the System Owner & Operator Policy Compliance Training?

In order to be compliant with this question:
- For System Owners or System Operators on systems that have CONFIDENTIAL or RESTRICTED classification: System Owner / System Operator training is required.
- OR
If your system is not classified as CONFIDENTIAL or RESTRICTED, the System Owner/System Operator training is optional. If this is your circumstance, indicate this fact in the “Your Comments” field and mark 100% compliance.

Resources:

a) System Owner and Operator Training Sign-up -  

b) Attendees of the System Owner and Operator Training -  
https://security.mcis.washington.edu/istk/doc/SOSOattendees.xls

c) PP04-Information Privacy, Confidentiality, & Security Training –  
https://know1.mcis.washington.edu/proj_hipaa/

d) SEC01-Information Security Policy -  

Q3: Are those individuals who are granted system admin privileges provided with job specific information security training?

In order to be compliant with this question:
- Anyone who has an account with admin privileges must be aware of the security restrictions that need to be in place.

Note: Formal security training is encouraged for individuals with administrative privileges. This might include internally sponsored training, vendor instruction, or 3rd party training.

Note: The following should be considered:
- An account with admin privileges must only for tasks requiring administrative privileges; use another account for tasks not requiring administrative privileges.
- Every account must be associated with only one individual.

Resources:

a) PP04-Information Privacy, Confidentiality, & Security Training –  
https://know1.mcis.washington.edu/proj_hipaa/

b) SEC01-Information Security Policy -  

c) SEC05-Communications and Operations Management Policy -  

Q4: Does your department provide information regarding guidelines and responsibilities associated with their computer and network privileges and resources?

In order to be compliant with this question:
Your department needs to provide you with information about restrictions and resources available to you.

Note: This training may be accomplished by staff signing the “Privacy, Confidentiality, and Information Security Agreement” and “Your Role in Information Security” This is typically handled by the Department.

Resources:

a) This document is part of the Information Security Toolkit, https://security.mcis.washington.edu/istk (section 3.2 & 5.2)

b) Departmental Training material: https://security.mcis.washington.edu/istk/doc/InfoSecUserResponsibilityTrainingTemplat e.ppt

c) Privacy, Confidentiality, and Information Security Agreement - https://security.mcis.washington.edu/istk

d) Your Role In Information Security - https://security.mcis.washington.edu/istk/

e) PP04-Information Privacy, Confidentiality, & Security Training – https://know1.mcis.washington.edu/proj_hipaa/

Q5: Does your department provide direction for reporting information security events, incidents, and/or malfunctions (information security breach, threat, weakness, and/or calculated violation of trust)?

In order to be compliant with this question:

- Every department must have a procedure to report problems and issues with their systems. You must know who to report incidents to, be it the IT Services Help Desk or a departmentally provided Help Desk.

Resources:

a) The Information Security Toolkit, https://security.mcis.washington.edu/istk, has training material a department can use to address this issue: https://security.mcis.washington.edu/istk/doc/InfoSecUserResponsibilityTrainingTemplat e.ppt

b) PP04-Information Privacy, Confidentiality, & Security Training – https://know1.mcis.washington.edu/proj_hipaa/

Q6: Has the Sanction Policy been reviewed?

In order to be compliant with this question:

- System Owner and System Operator need to have reviewed the Sanction Policy and understand what may happen if policy is not followed and a security breach occurs. The Sanctions Policy is covered in both the System Owner/Operator Training and the Departmental Security Training.

Resources:

b) Departmental Training material: https://security.mcis.washington.edu/istk/doc/InfoSecUserResponsibilityTrainingTemplate.ppt
c) UW Medicine Privacy Policies - https://knowl.mcis.washington.edu/proj_hipaa/

Q7: Have you reviewed the roles and responsibilities of System Owner, System Operator, and Data Custodian for the information and information systems within your System?

In order to be compliant with this question:

- Have attended either the System Owner and System Operator Training or the Department Managers Training.
- Have reviewed the roles and responsibilities of System Owner, System Operator, and Data Custodian

Note: It is recommended that roles and responsibilities are discussed with the computer and data owner staff.

Resources:

b) Departmental Training material: https://security.mcis.washington.edu/istk/doc/InfoSecUserResponsibilityTrainingTemplat e.ppt
c) The Information Security Toolkit, https://security.mcis.washington.edu/istk
Q8: Has the Policy Exception Request process been reviewed?

In order to be compliant with this question:

- Both the System Owner and Operator have attended either the System Owner/Operator training or the Department Manager training
- Both the System Owner and Operator have reviewed the exemption standard.

Note: Systems may require policy exemptions if compliance with policy is either not possible or feasible. To file an exception request contact: mcos@u.washington.edu.

Note: You need to know what to do if you can't directly meet all the policies. The exception request process is reviewed in the System Owner/Operator training and in the Department Manager training material.

Resources:

a) System Owner and Operator Training Sign-up -

b) Departmental Training material:
   [https://security.mcis.washington.edu/istk/doc/InfoSecUserResponsibilityTrainingTemplate.ppt](https://security.mcis.washington.edu/istk/doc/InfoSecUserResponsibilityTrainingTemplate.ppt)

c) SEC01-Information Security Policy -

d) SEC01.02-Policy Exemption Standard -

Q9: For your System have you documented the System Owner and System Operator?

In order to be compliant with this question:

- You must have assigned an individual with the System Owner and System Operator role.

Note: The ICR itself can be considered adequate documentation for the roles of System Owner and System Operator. At the beginning of the ICR the information regarding System Owner and Operator is required.

Resources:

a) SEC01-Information Security Policy -
Q10: Have you applied the information classifications of "Public", "Restricted" or "Confidential" to data contained within or used by your system?

In order to be compliant with this question:
- Choose one of the following risk assessment classifications for your system:

<table>
<thead>
<tr>
<th>Confidentiality Classification Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low</strong></td>
</tr>
<tr>
<td>PUBLIC: This is information that is either approved for general access, or by its nature, is not necessary to protect, and can be shared with anyone. A breach of the confidentiality of public information is expected to have a <strong>limited adverse effect</strong> on UW Medicine operations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EXAMPLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>General public information, published reference documents (within copyright restrictions), open source materials, approved promotional information, press releases.</td>
</tr>
</tbody>
</table>

Resources:

- SEC02-Information & Information System Classification Policy - [https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC02-Info&InfoSystemClassification_Policy.doc](https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC02-Info&InfoSystemClassification_Policy.doc)
- SEC02.00.01-Information & Information System Classification Guideline - [https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC02.00.01-Info&InfoSystemClassification_Guideline.doc](https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC02.00.01-Info&InfoSystemClassification_Guideline.doc)
Q11: Are the following principles applied during job definition and the delegation of System responsibilities

a) “Principle of Least Privilege”
b) “Principle of Separation of Duties”;
c) “Minimum Necessary”?

In order to be compliant with this question:

- Apply Principle of Least Privilege, and
- Apply Principle of Separation of Duties, and
- Apply Minimum Necessary.

Note:
Job separation is an important aspect of protecting our computing resources.

**Principle of Least Privilege**: Access privileges for users are limited to what is necessary to be able to complete their assigned duties or functions [i.e. to be able to do their job].

**Example**: Staff with financial duties only does not need access to PHI data.

**Principle of Separation of Duties**: When it involves the ‘potential’ for fraud, abuse, or other harm, whenever practical, no one person is responsible for completing or controlling a task, or a set of tasks, from beginning to end.

**Example**: Billing for services -- Because there is clearly an opportunity for fraud or abuse, no one person should be responsible from beginning to end.

**Principle of Minimum Necessary**: Access to protected health information should be “limited” to the health information required to perform a business activity or achieving an authorized requestor’s specified purpose.

Minimum necessary is based upon the “need to know” principle, which directs that when a user accesses protected health information, the information accessed is required for the user’s job function, role and job responsibilities.

**Example**: Individuals working in ophthalmology do not need access to the pathology system.

**Resources**:

- SEC05-Communications and Operations Management Policy -

Q12: Is the workspace for systems you are responsible for kept clear of restricted or confidential material while unattended or not in use?

To be compliant with this question you must:
Keep restricted or confidential material protected when unattended or not in use.

Note: Where appropriate, store paper and computer media, such as floppy disks, hard drives, tape cassettes, etc. in suitable locked cabinets when not in use or when unattended.

Resources:

a) SEC03-Workforce Information Security Policy.doc -

Q13: Are the following controls observed:

a. Clear protected health information or critical business information from printers immediately; and
b) Protect incoming and outgoing mail points and unattended fax machines from unauthorized access?

To be compliant with this question you must:

• Have no CONFIDENTIAL or RESTRICTED information, or
• If you have CONFIDENTIAL or RESTRICTED information you need to do the following:
  o Where applicable printers, copiers, fax machines, and other data duplication devices need to be in areas that are locked and not available to the public when unattended.

Note: If you have restricted information, do you manage to keep unauthorized people from the printer, fax, and mail areas? Verify and audit that staff are following appropriate procedure by clearing protected health information or critical business (restricted or confidential) information from printers immediately.

Resources:

a) SEC03-Workforce Information Security Policy.doc -
b) SEC03.02-Workspace Information Security Standard -

Q14: Are duplication devices locked (or protected from unauthorized use in some other way) outside of normal working hours?

To be compliant with this question you must:

• Have no CONFIDENTIAL or RESTRICTED information, or
• If you have CONFIDENTIAL or RESTRICTED information you need to do the following:
Duplication devices need to be in areas that are locked and not available to the public when unattended.

Duplication devices need to be in areas that are under observation during the day when they are available.

Note: If you have CONFIDENTIAL or RESTRICTED information, have you locked down the copy devices to stop unauthorized copies of the data?

Resources:

a) SEC03-Workforce Information Security Policy.doc -
   https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC03-
   WorkforceInformationSecurity_Policy.doc

b) SEC03.02-Workspace Information Security Standard -
   https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC03.02-
   WorkspaceInformationSecurity_Standard.doc

Q15: Do you dispose of media containing protected health information, proprietary information, and other confidential information in a secure and confidential manner?

To be compliant with this question you must:

- Have no CONFIDENTIAL or RESTRICTED information on transportable media such as hard copy (paper), CD, floppy, or zip disk, OR

- Where CONFIDENTIAL or RESTRICTED information are included:
  - **Paper Documentation** – need to be shredded, pulped or otherwise obliterated in a manner that prevents reconstruction.
  - **Microfilm and Microfiche** - must be pulverized **.
  - **Laser Disks** - used in write once-read many (WORM) document imaging applications shall be pulverized.
  - **Floppy Disks** - shall be pulverized.
  - **Compact Disks** - shall be pulverized.
  - **Magnetic Tape & Video Tape** - preferred method for destroying computerized data is magnetic degaussing. If destruction is not achieved by degaussing, it must be executed in an alternative manner that assures that the information cannot be reconstructed.
  - **Hard Drives** - To assure that computerized data is destroyed when equipment is decommissioned, use a three pass binary overwrite of the entire disk will reasonably assures that the information cannot be reconstructed. An alternative to this process is that the hard drive is removed from the device and pulverized.
  - **Carbon Rolls** (from printers or fax machines) The method for destroying carbon rollers removed from printers or fax machines is to send them to Environmental Services for destruction by autoclaving.

Note: **Pulverized**: Reduced (as by crushing, beating, or grinding) to very small particles that can not be reconstructed or used in any combination to reconstruct the original.

Resources:
Q16: Are active computing sessions terminated or secured by an appropriate locking mechanism, e.g. a password protected screen saver when unattended?

To be compliant with this question you must:

- Terminate active computing sessions on Workstations, or
- Secure active computing sessions on Workstations with an appropriate locking mechanism.

Note: A password protected screen saver on a Workstation is an example of a locking mechanism.

Resources:


Q17: Are active computing sessions terminated when the computing session is finished?

To be compliant with this question you need to:

- All users are trained to terminate active computing sessions per the “Your Role in Information Security” training.

Resources:

a) This document is part of the Information Security Toolkit, https://security.mcis.washington.edu/istk/
b) Training material a department can use to address this training issue: https://security.mcis.washington.edu/istk/doc/InfoSecUserResponsibilityTrainingTemplate.ppt
Q18: Where feasible, is an automatic logoff (configured to logoff idle users) being used to protect applications with confidential information?

To be compliant with this question you must:

- Not have CONFIDENTIAL or RESTRICTED information stored on the system, or
- If your system does store CONFIDENTIAL or RESTRICTED information, set your system to log off after 15min of idle time.

Note: The UW Medicine policy has been revised to include both CONFIDENTIAL as well as RESTRICTED information.

Resources:

a) SEC03-Workforce Information Security Policy.doc -
b) SEC03.02-Workspace Information Security Standard -

Q19: Are all networked computer systems within your responsibility left powered on after working hours, including weekends and holidays?

To be compliant with this question you must:

- Your department is part of an AMC domain or the IT Services’ active directory AND your machines are logged off but left ‘on’, or
- You are NOT a part of an AMC domain or the active directory AND you follow the direction of those responsible for support (i.e. the maintenance of security patches, updates, etc.).

Resources:

a) SEC03-Workforce Information Security Policy.doc -
b) SEC03.02-Workspace Information Security Standard -

Q20: Are the Server Systems you are responsible for being housed in secure areas that provide adequate physical and environmental controls?

To be compliant with this question you must:

- If your System does not contain any Server Systems mark 100% compliant, or
- Locate Server Systems in computing facility meeting UW Medicine policy, or
- Take part in a hosting or co-location solution, such as the ones offered by IT Services or C&C.
Note:

Environmental controls:
- UPS and power conditioning
- Backup generator power
- Temperature monitoring and cooling
- Fire/smoke detection and suppression systems
- Protection from water damage
- Seismic protections (Examples: Rack stabilization, equipment fixed to racks)
- No food or drink allowed in facility

Physical access controls:
- Defined perimeter and signage
- Controlled access points (Example: Locking doors)
- Access logging (Examples: Magnetic swipe cards, clip board)
- Vendor and guest access only while accompanied by authorized staff
- Logging equipment moving in and/or out
- Surveillance (Examples: Onsite staff, & video cameras)

Resources:

- For hosting consultation contact:
  - IT Services - IT Services Helpdesk -
    [https://helpdesk.mcis.washington.edu](https://helpdesk.mcis.washington.edu) (mcsos@u.washington.edu)

Q21: Is there a defined security perimeter and appropriate entry controls protecting your Server Systems from unauthorized access, damage and interference?

To be compliant with this question you must:
- If your System does not contain any Server Systems mark 100% compliant, or
- Locate Server Systems in computing facility meeting UW Medicine policy, or
- Take part in a hosting or co-location solution, such as the ones offered by IT Services or C&C.

Note: The standard says: Server Systems will be housed in specially designated areas that provide adequate physical security and environmental controls. Such areas will have a defined security perimeter, with appropriate entry controls. They will be physically protected from unauthorized access, damage and interference.
Advanced System ICR Guide

Resources:

a) For hosting consultation contact:
   - IT Services - IT Services Helpdesk -
     https://helpdesk.mcis.washington.edu (mcsos@u.washington.edu)
   - C&C - http://depts.washington.edu/cae/ or help@cac.washington.edu.

b) SEC04-Physical Information Security Policy -
   https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC04-
   PhysicalInformationSecurity_Policy.doc

c) SEC04.01-Secure Server Location Standard -
   https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC04.01-
   SecureServerLocation_Standard.doc

d) SEC04.00.01-Physical Security Guideline -
   https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC04.00.01-
   Physical_Guideline.doc

Q22: Where there is an opportunity for fraud and abuse is separation of duties observed during the performance of operational responsibilities such as:

a) Operational responsibility or privilege for network infrastructure systems, computer systems, and security systems will not be granted to any single member of the operational staff;

b) Individuals other than those performing system administration perform review of system audit logs;

c) Test systems are separate from production systems;

d) Cross training of operations staff to provide depth and backup, and to reduce individual dependence.

To be compliant with this question you must:

- Your System does not have opportunity for fraud and abuse, or
- Have some auditing process in place to ensure that no single individual with privileged system access can abuse his/her access by altering data. This includes the following:
  - More than one person in the department will have privileged access to the system, and
  - The individuals with privileged access will be audited by other individuals in the department, and
  - Test systems are separate from production systems, and
  - Cross training will occur to reduce dependence on single individuals in critical roles.

Resources:

a) SEC05-Communications and Operations Management Policy -
   https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05-
   CommunicationsOperationsManagement_Policy.doc

Q23: Has the System Owner and/or System Operator determined an appropriate backup schedule?
To be compliant with this question you must:

- Your Server System does not need to be backed up i.e. the need for Integrity and Availability are rated as low, or
- If you Server System requires a backup
  - have a regular schedule for backing up the Server System(s) has been implemented, or
  - Take part in a backup solution, such as the ones offered IT Services, C&C, or a 3rd party.

Note: The following control guidelines are recommended for System Owners and System Operators:

a) A minimum level of back-up information includes:
   1) Accurate and complete records of the back-up copies and documented restoration procedures.
   2) Three generations or cycles of back-up information for critical data.

b) Give back-up information an appropriate level of physical and environmental protection consistent with its information classification. The controls and media handling standards applied to media at the main site need to be extended to cover the back-up site.

c) Where practical, regularly test back-up media to ensure reliability for emergency use.

d) Regularly check and test restoration methodology to ensure effectiveness and to ensure that restoration can be completed within the time allotted in the operational procedures for recovery.

Resources:

a) For a backup solution contact: IT Services Helpdesk -
   - IT Services - IT Services Helpdesk -
     https://helpdesk.mcis.washington.edu/ (mcsos@u.washington.edu)
   - C&C - http://depts.washington.edu/cac/ or help@cac.washington.edu.

b) SEC05-Communications and Operations Management Policy -

Q24: If your Server Systems require back-ups, are the backups scheduled and run regularly?

To be compliant with this question you must:

- If your System does not contain any Server Systems mark 100% compliant.
- Your Server System does not need to be backed up i.e. the need for Integrity and Availability are rated as low, or
- If you Server System requires a backup
  - have a regular schedule for backing up the Server System(s) has been implemented, or
  - Take part in a backup solution, such as the ones offered IT Services, C&C, or a 3rd party.

Resources:
Q25: Have backup copies been tested to ensure that they are reliable?

To be compliant with this question you must:
- Your Server System does not need to be backed up i.e. the need for Integrity and Availability are rated as low, or
- If you Server System requires backups ensure it is tested.

Resources:

a) For a backup solution contact: IT Services Helpdesk - https://helpdesk.mcis.washington.edu/ or C&C - http://depts.washington.edu/cac/

Q26: Is a Maintenance & Operations Log (kept by) System Operators or designees?

To be compliant with this question you must:
- Log maintenance and operations performed for the System

Note: Logs include, as appropriate:
- Full name of workforce member or vendor representative performing the maintenance or operations;
- Starting and finishing times of activity;
- System errors and corrective action taken;
- What the maintenance or operations actions where taken;
- The name of the person making the log entry if different from the person performing the work.

Note: Logs can be written into a binder or stored electronically as long as the integrity and availability of the logs can be reasonably assured.

Resources:


Q27: Do System Operators review logs of operational events?
To be compliant with this question you must:
• System Operator reviews system logs on a regular schedule, or a designated individual reviews system logs on a regular schedule

Resources:

a) SEC05-Communications and Operations Management Policy -

Q28: Are faults reported to your Help Desk?

To be compliant with this question you must:
• Report failures and problems to a departmentally designated computing help desk. If your department does not have a help desk, send a report of the problem to the IT Services Help Desk at: mcsos@u.washington.edu.

Note: Your Department training should have identified the Help Desk to which faults are to be reported.

Resources:

a) SEC05-Communications and Operations Management Policy -
b) SEC11-Incident Response Policy -

Q29: Is system logging being performed on systems with confidential data or systems that are critical to the UW Medicine network?

Note: UW Medicine policy has been revised to state that all Networked Systems must have logging enabled.

To be compliant with this question you must:
• Operating system logging, such as Windows event logs, Macintosh syslog, or UNIX syslog, is enabled and logging events.

Note: If system logging is not currently enabled, create a plan that includes what it will take to turn it on, what might be impact of the change, and who will do the work.

Resources:

a) Windows Server Administration Guide
b) SEC05-Communications and Operations Management Policy -
Q30: Do your Networked Systems (systems on the network using wired or wireless technology) comply with the minimum requirements of the Networked System Information Security Standard?

To be compliant with this question you must:

- Remove the computer system from the network and ensure that it will not be connected to the network, or
- Meet the Minimum Information Security Requirements.

1. All Networked Systems must meet the following requirements:
   - Active network filtering or firewall
   - Protection against malicious software (See SEC-05.01 Protection Against Malicious Software Standard)
   - Approved network protocols
   - Approved network protocol addressing
   - Approved network media (encompasses Ethernet and Wireless)
   - A secure and approved operating system and operating system services
   - Current operating system and application patches and/or updates
   - Enabled logging and auditing capabilities

2. Additional Requirements for Server Systems:
   - Compliance with information security configuration and hardening guidelines and procedures
   - Data classification (See SEC02 Information and Information System Classification)
   - Backup and recovery plan (See policy section with SEC05, Information Storage & Backup Standard)
   - Appropriate environmental & physical security (See SEC-04.01 Secure Server System Location Standard)
   - Certified for production use in compliance with the Server System Certification Standard (See policy section VIII. Server System Certification Standard)

Resources:

a) SEC05-Communications and Operations Management Policy -

b) Windows Workstation Minimum Security Requirements -
https://know1.mcis.washington.edu/manuals/SEC05.00.00.01-WindowsWorkstationMinimumSecRequirements.doc

c) Windows Server Minimum Security Requirements -
https://know1.mcis.washington.edu/manuals/SEC05.00.00.02-WindowsServerMinimumSecRequirements.doc
Q31: Does your system have active protection against malicious software?

To be compliant with this question you must:

- For a Microsoft Windows system this means installing anti-virus software; the recommendation is McAfee Anti-Virus.
- For a Macintosh OS system this means installing anti-virus software; the recommendation is Dr. Solomon's Virex for Macintosh.
- For a Unix or Linux system this means installing file integrity software such as Tripwire.

Note: Recommendations, potential costs for set-up and maintenance are to be found in the information Security Toolkit: https://security.mcis.washington.edu/istk/

Resources:


b) Windows Workstation Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.01-WindowsWorkstationMinimumSecRequirements.doc

c) Windows Server Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.02-WindowsServerMinimumSecRequirements.doc

d) Macintosh Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.03-MacintoshMinimumSecRequirements.doc

e) UNIX Workstation Minimum Security Requirements – https://know1.mcis.washington.edu/manuals/SEC05.00.00.04-UNIXWorkstationMinimumSecRequirements.doc

f) UNIX Server Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.05-UNIXServerMinimumSecRequirements.doc

g) Printers Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.06-PrintersMinimumSecRequirements.doc
Q32: Does your system use TCP/IP with an address obtained through an IT Services Help Desk or University of Washington Campus & Computing (C&C) Help Desk ticket or a sanctioned DHCP server?

To be compliant with this question you must:

- Obtain a static IP address through an IT Services Help Desk or University of Washington Campus & Computing (C&C) or
- Obtain a dynamic IP address obtained through an IT Services Help Desk or University of Washington Campus & Computing (C&C) or other sanctioned DHCP server, or
- This does not apply, and it can be marked 100% compliant if:
  - You are logically separated from the UW IP network subnets (such as using NAT), or
  - You are using non-routable address such as a 192.168.x.x.

Resources:

a) SEC05-Communications and Operations Management Policy -


c) IT Services Helpdesk - [https://helpdesk.mcis.washington.edu/](https://helpdesk.mcis.washington.edu/)

Q33: Is your system using a secure and approved operating system?

To be compliant with this question you must:

- Be using an approved OS (listed below).

**Note:** Operating System versions are to be those supported by the operating system vendors.

For Microsoft Windows Workstations
- Windows 2000 Professional
- Windows XP Professional

For Microsoft Windows Server
- Windows 2000 Server
- Windows 2003 Server

For UNIX Workstations
- Red Hat Linux
- Sun Solaris versions 8 and 9
- HP Tru 64
- IBM AIX

For UNIX Servers
- RedHat Linux
- Sun Solaris versions 8 and 9
- HP Tru 64
- HPUX
- IBM AIX
Other Operating Systems
  o HP VMS
  
For Macintosh
  o Macintosh OS 9
  o Macintosh X (10)

Resources:

a) The approved list including potential costs for set-up and maintenance are to be found in the information Security Toolkit: https://security.mcis.washington.edu/istk
c) Windows Workstation Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.01-WindowsWorkstationMinimumSecRequirements.doc
e) Macintosh Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.03-MacintoshMinimumSecRequirements.doc
f) UNIX Workstation Minimum Security Requirements – https://know1.mcis.washington.edu/manuals/SEC05.00.00.04-UNIXWorkstationMinimumSecRequirements.doc
g) UNIX Server Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.05-UNIXServerMinimumSecRequirements.doc
h) Printers Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.06-PrintersMinimumSecRequirements.doc

Q34: Are the operating system and applications patched and updated in a reasonably timely manner?

To be compliant with this question:
  • Have your system set to automatically patch (e.g. YUM for Linux, Windows Update for Windows, etc.), or
  • Have a regularly defined schedule where systems are manually patched. When determining the appropriate patching schedule the severity of the patch and the impact to the system should be evaluated.

Resources:

b) Windows Workstation Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.01-WindowsWorkstationMinimumSecRequirements.doc

c) Windows Server Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.02-WindowsServerMinimumSecRequirements.doc

d) Macintosh Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.03-MacintoshMinimumSecRequirements.doc

e) UNIX Workstation Minimum Security Requirements – https://know1.mcis.washington.edu/manuals/SEC05.00.00.04-UNIXWorkstationMinimumSecRequirements.doc

f) UNIX Server Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.05-UNIXServerMinimumSecRequirements.doc

g) Printers Minimum Security Requirements - https://know1.mcis.washington.edu/manuals/SEC05.00.00.06-PrintersMinimumSecRequirements.doc

Q35: Is your Server System compliant with information security configuration and hardening guidelines and procedures?

To be compliant with this question you must:

- Follow an appropriate security configuration guide (departmental or UW Medicine).

Note: If your System does not contain any Server Systems mark 100% compliant.

Resources:

a) For installing and configuring your computers, such as the one found at: http://security.uwmedicine.org/DocsFAQs.asp

b) These guidelines may be found at: http://security.uwmedicine.org/DocsFAQs.asp


Q36: Has a Server Systems backup and recovery plan been documented?

To be compliant with this question:

- You must have a plan for how to backup and recover your systems appropriate to your risk level.

Note: If your System does not contain any Server Systems mark 100% compliant.

Note: If your backup and recovery is outsourced then check with the service provider for additional information when creating the backup and recovery plan.
Note: The following control guidelines are recommended for System Owners and System Operators:

a) A minimum level of back-up information includes:
   1. Accurate and complete records of the back-up copies and documented restoration procedures.
   2. Three generations or cycles of back-up information for critical data.

b) Give back-up information an appropriate level of physical and environmental protection consistent with its information classification. The controls and media handling standards applied to media at the main site need to be extended to cover the back-up site.

c) Where practical, regularly test back-up media to ensure reliability for emergency use.

d) Regularly check and test restoration methodology to ensure effectiveness and to ensure that restoration can be completed within the time allotted in the operational procedures for recovery.

Resources:

a) For a backup solution contact: IT Services Helpdesk - https://helpdesk.mcis.washington.edu/ or C&C http://depts.washington.edu/cac/


Q37: Is the Server System is in a secure/locked location?

To be compliant with this question you must:
- If your System does not contain any Server Systems mark 100% compliant, or
- Locate Server Systems in computing facility meeting UW Medicine policy, or
- Take part in a hosting or co-location solution, such as the ones offered by IT Services or C&C.

Note:

Environmental controls:
- UPS and power conditioning
- Backup generator power
- Temperature monitoring and cooling
- Fire/smoke detection and suppression systems
- Protection from water damage
- Seismic protections (Examples: Rack stabilization, equipment fixed to racks)
- No food or drink allowed in facility

Physical access controls:
- Defined perimeter and signage
- Controlled access points (Example: Locking doors)
- Access logging (Examples: Magnetic swipe cards, clip board)
- Vendor and guest access only while accompanied by authorized staff
- Logging equipment moving in and/or out
- Surveillance (Examples: Onsite staff, & video cameras)
Resources:

- For hosting consultation contact:
  - IT Services - IT Services Helpdesk -
    https://helpdesk.mcis.washington.edu (mcsos@u.washington.edu)
  - C&C - http://depts.washington.edu/cac/ or help@cac.washington.edu.
- SEC04-Physical Information Security Policy -
  https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC04-
- PhysicalInformationSecurity_Policy.doc
- SEC04.01-Secure Server Location Standard -
  https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC04.01-
  SecureServerLocation_Standard.doc
- SEC04.00.01-Physical Security Guideline -
  https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC04.00.01-
  Physical_Guideline.doc

Q38: Have all Server Systems that you are responsible for, which contain confidential information, been certified by IT Services SIT (Security Infrastructure Team)?

To be compliant with this question you must:
- If your System does not contain any Server Systems mark 100% compliant, or
- Have all Server Systems with advanced requirements meet certification.

Note: Server Systems with minimum security requirements are not required to be certified.

Resources:

- Follow the “Instructions for Requesting a Server Security Certification” Available under Services on the Security Infrastructure Team website: https://security.uwmedicine.org/
- SEC05-Communications and Operations Management Policy -
  https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05-
  CommunicationsOperationsManagement_Policy.doc

Q39: Is software installed only by designated system administrators as authorized by the System Owner or System Operator?

To be compliant with this question you must:
- Ensure software is installed by designated and authorized system administrators.

Note: Recommended Remediation should include:
- Restricting administrator access to only those who are authorized,
- Do not permit regular users to install software on their computers
- Having a list of designated Users who can install software on the System.

Resources:
Q40: Are system administrators using designated administrative accounts only for system administrative work and using regular user accounts all other times?

To be compliant with this question you must:

- Ensure that system administrators are using their designated administrative accounts only for system administrative work.

Resources:

a) SEC05.01-Protection Against Malicious Software Standard - https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.01-ProtectionAgainstMaliciousSoftware_Standard.doc

Q41: Is system administrator access limited to those who required it to fulfill their job function?

To be compliant with this question you must:

- Restrict administrator access to only those who need this functionality.
- Only allow administrative access to individuals that require privileged access to do their jobs.
- Only use administrative access accounts when required by the task at hand.

Resources:

b) SEC05.01-Protection Against Malicious Software Standard - https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.01-ProtectionAgainstMaliciousSoftware_Standard.doc

Q42: Where anti-virus software is the method for protection against malicious software, is it set to update itself frequently (daily interval suggested) with the notification function installed so that the user, and where appropriate, the administration group, is aware of virus incidents/ actions?

To be compliant with this question you must:

- Set software that protects your system from malicious code to update automatically.
Where appropriate, the notification function must be installed so that the user and System Operator are made aware of virus incidents and actions.

Resources:

a) SEC05-Communications and Operations Management Policy -

b) SEC05.01-Protection Against Malicious Software Standard -
https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.01-ProtectionAgainstMaliciousSoftware_Standard.doc

Q43: Are virus incidents reported to your Help Desk?

To be compliant with this question:

- Those viruses that are identified but not removed successfully by the anti-virus software are reported to your Help Desk.

Note: If the anti-virus reports a virus but is able to remove/delete the virus there is no need to report it unless otherwise instructed by your Help Desk.

Resources:

a) SEC05-Communications and Operations Management Policy -

b) SEC05.01-Protection Against Malicious Software Standard -
https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.01-ProtectionAgainstMaliciousSoftware_Standard.doc

c) SEC11-Incident Response Policy -

Q44: Is the destruction of information handled consistent with its classification whatever the media - documents, computing systems, mail, multimedia, postal services/facilities, and/or use of fax machines?

To be compliant with this question you must:

- Have no CONFIDENTIAL or RESTRICTED information, or
- If you have CONFIDENTIAL or RESTRICTED information you need to do the following:
  - media, such as CDs, floppys, zipdisks, etc. need to be destroyed before disposal.

Note:

Requirements for disposal of media when PHI and proprietary information are included:

- Paper Documentation – need to be shredded, pulped or otherwise obliterated in a manner that prevents reconstruction.
• Microfilm and Microfiche - must be pulverized [1].
• Laser Disks - used in write once-read many (WORM) document imaging applications shall be pulverized.
• Floppy Disks - shall be pulverized.
• Compact Discs - shall be pulverized.
• Magnetic Tape & Video Tape - preferred method for destroying computerized data is magnetic degaussing. If destruction is not achieved by degaussing, it must be executed in an alternative manner that assures that the information cannot be reconstructed.
• Hard Drives - To assure that computerized data is destroyed when equipment is decommissioned, use a three pass binary overwrite of the entire disk will reasonably assures that the information cannot be reconstructed. An alternative to this process is that the hard drive is removed from the device and pulverized.
• Carbon Rolls (from printers or fax machines) The method for destroying carbon rollers removed from printers or fax machines is to send them to Environmental Services for destruction by autoclaving.

[1] Pulverized: Reduced (as by crushing, beating, or grinding) to very small particles that can not be reconstructed or used in any combination to reconstruct the original.

Resources:

a) UW Surplus will chop CDs and floppies for you, but it is not cost effectual to do so. You can buy a $75.00 shredder that will shred CDs and floppies from office supply stores.
b) SEC05.02-Media Handling Standard - 
https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.02-MediaHandling_Standard.doc

Q45: Is information designated for destruction maintained in a secure and confidential manner prior to its final destruction and is it destroyed in a manner that assures no possibility of reconstruction?

To be compliant with this question you must:
• Store media to be disposed in a secure location until it is destroyed.

Note: Examples of secure locations for paper and hard drives include locked doors or filing cabinets.

Resources:

a) SEC05.02-Media Handling Standard -
https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.02-MediaHandling_Standard.doc

Q46: Where appropriate, is physical labeling used to control media?

In order to be compliant with this question you must:
• Use labeling as appropriate.

Note: It is strongly recommended that if RESTRICTED and CONFIDENTIAL information is contained on removable media physical labels are used to help in tracking.
Q47: Do you use the logging of media to support accountability?

In order to be compliant with this question you must:

- Have a tracking system such as a log in place, where it is recorded who, when, where, and what restricted or confidential data has been taken from the place of work on removable media; or
- Have no removable media with CONFIDENTIAL or RESTRICTED information; or
- Ensure your media doesn’t move outside of its primary storage (room) location.

Note: A log can be electronic or hardcopy. Logs may include control numbers (or other tracking data), times and dates of transfers, names and signatures of individuals involved, and other relevant information.

Resources:

a) SEC05.02-Media Handling Standard -
   https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.02-MediaHandling_Standard.doc

Q48: Are periodic spot checks or audits conducted to determine if any controlled items have been lost and to ensure that these items are in the custody of individuals named in control logs?

In order to be compliant with this question you must:

- Conduct spot checks to ensure that labeled media has not been removed from the place of work unless appropriately logged; or
- You are compliant if logs.

Resources:

a) SEC05.02-Media Handling Standard -
   https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.02-MediaHandling_Standard.doc

Q49: Is all electronic media intended for reuse subjected to media disposal (re-use) processes, such as overwriting or degaussing, to ensure the media is properly sanitized and to prevent the disclosure of protected or confidential information?

In order to be compliant with this question you must:
• Not store restricted or confidential data on removable media (such as CDRW, floppy, or zip disk); OR

• Ensure that media containing CONFIDENTIAL or RESTRICTED has been either overwritten or degaussed before reuse.

Note: *Overwrite*. Overwriting uses a program of 1s, 0s, or a combination of both to write onto the media. Media must be overwritten three times. Overwriting is not to be confused with merely deleting the pointer to a file (which typically happens when a *delete* command is used). Overwriting requires that the media be in working order.

*Degauss*. Degaussing magnetically erases data from magnetic media. Two types of degausser exist: strong permanent magnets and electric degaussers.

Note: Reformatting media DOES NOT constitute over-writing.

**Resources:**

a) Security Infrastructure Team (SIT) - [https://security.uwmedicine.org/tools](https://security.uwmedicine.org/tools)

b) SEC05.02-Media Handling Standard -

**Q50: Is your information retained according to UW Retention policies?**

In order to be compliant with this question, you must:

• Follow the policies provided by UW Records Management Services.

Note: This applies to electronic media such as disks as well as hardcopy (paper).

**Resources:**

a) UW Records Management Services:

**Q51: Are appropriate system access controls in place?**

In order to be compliant with this question:

•

Note: This question applies to both physical security and electronic security.

Access to Server Systems should include:

• Defined perimeter and signage

• Controlled access points (i.e. Locking doors)

• Access logging (i.e. Magnetic swipe cards)

• Vendor and guest access only while accompanied by authorized staff

• Logging equipment moving in and/or out
Q52: If you provide access to your system, is access granted based on the “Principle of Least Privilege” and the “Principle of Separation of Duties” as well as "Minimum Necessary"?

In order to be compliant with this question:
- Follow the “Principle of Least Privilege”
- Follow the “Principle of Separation of Duties”
- Follow with "Minimum Necessary".

Note:

**Principle of Least Privilege**: Access privileges for users are limited to what is necessary to be able to complete their assigned duties or functions [i.e. to be able to do their job].

**Example**: Staff with financial duties only do not need access to PHI data.

**Principle of Separation of Duties**: When it involves the ‘potential’ for fraud, abuse, or other harm, whenever practical, no one person is responsible for completing or controlling a task, or a set of tasks, from beginning to end.

**Example**: Billing for services -- Because there is clearly an *opportunity* for fraud or abuse, no one person should be responsible from beginning to end.

**Principle of Minimum Necessary**: Access to protected health information should be “limited” to the health information required to perform a business activity or achieving an authorized requestor’s specified purpose.

Minimum necessary is based upon the “need to know” principle, which directs that when a user accesses protected health information, the information accessed is required for the user’s job function, role and job responsibilities.

**Example**: Individuals working in ophthalmology do not need access to the pathology system.

Resources:


Q53: If you provide access to your system, is there appropriate user account management in place?

1) Effective administration: identification, authentication, and authorization of users;
2) Periodic verification of the legitimacy of current accounts and access authorizations;
3) Timely modification or removal of access for those individuals that have been reassigned, promoted, or who are no longer a member of the UW Medicine Workforce.

In order to be compliant with this question, you must:

- Ensure all users that authenticate to your System have a valid reason to do so;
- Ensure all users that access your System have appropriate levels of access based on current role.

Note: This question refers to System Owners providing access to their System. User account management is the responsibility of the System Owner. If provisioning of access to your System is outsourced, the System Owner still must ensure appropriate account management.

Resources:


Q54: Is access to multi-user information services controlled through a formal user registration process?

In order to be compliant with this question, you must:

- Not be running a service that provides CONFIDENTIAL or RESTRICTED information, or
- Have a process that includes authentication, authorization, and validation of users.

Resources:


Q55: If you provide access to your system, is each user issued a unique username and password?

In order to be compliant with this question, you must:

- Not be running a service that provides CONFIDENTIAL or RESTRICTED information, OR
- Use unique user accounts and user a password.
Resources:


Q56: Are your users aware of the password usage guidelines outlined within the policy?

In order to be compliant with this question, you must:

- Not need to use passwords on your System (public data or alternate means of authentication), OR
- Ensure that Users have been made aware of password usage requirements (for example through signing the Privacy Confidentiality and Information Security Agreement)

Resources:

a) Privacy Confidentiality and Information Security Agreement - https://security.mcis.washington.edu/istk/

Q57: Do you instruct users to only access UW Medicine resources that they have been authorized to use and that are necessary to perform their official job functions?

Note: This is now handled by Department Managers. Mark 100% compliant.

Q58: Does your system have a technical access control mechanism of some kind that allows for authorization and allocation of system and data resources to individual users?

In order to be compliant with this question, you must:

- Not need to use technical access control mechanisms for authorization on your System (public data or alternate means of authorization and allocation of System resources), or
- Require a username and password to login. (Examples of technical access control mechanisms may include: operating system accounts such as AD or local account, SecurID, or UW NetID and passwords)

Note: All approved operating systems may have technical access control mechanisms built-in.

Note: Technical access control mechanisms would include authentication to verify the identity of Users and authorization to determine access. Technical access control can occur at the application or the operating system level.

Resources:
Q59: If you have external connections like a VPN, have they been reviewed by UW Medicine SIT to insure information security compliance?

In order to be compliant with this question, you must:

- Not offer external connections like a VPN; or
- SIT has reviewed your external access system.

Notes: Connecting to application such as email is not within the scope of this question.

Resources:

a) SEC05.04-Remote Access Standard -

b) SEC06-Access Control Policy -

Q60: Are the operating systems you employ set to
1) Identify and verify the identity, and if necessary the terminal or location, of each authorized user;
2) Record successful and failed system logons;
3) Provide appropriate means for authentication; if a password management system is used, it must ensure quality passwords;
4) Where appropriate, restrict the connection times of users;
5) Differentiate level of privilege?

In order to be compliant with this question, you must:

- For Systems with RESTRICTED or CONFIDENTIAL information:
  - Require a unique username for each user
  - Enable recording of successful and failed logons
  - Use good passwords, if passwords are used (compliant with UW Medicine best practices)
  - Restrict User to specific hours (working hours versus non-working hours) as appropriate
  - Assign account privileges based on need. (for example administrative tasks would require administrative privileges whereas access to a standard application may not.)

- For System with no RESTRICTED or CONFIDENTIAL information:
  - Use good passwords, if passwords are used (compliant with UW Medicine best practices)
Assign account privileges based on need. (for example administrative tasks would require administrative privileges whereas access to a standard application may not.)

Resources:

a) SEC06-Access Control Policy -

Q61: Are your applications enabled to control user access to information and application system functions?

In order to be compliant with this question, you must:

- Not have RESTRICTED of CONFIDENTIAL information; or
- Control user access at operating system or application level based on the capabilities of your System.

Note: The use of Role Based access ensures the observance of the Principle of Minimum Necessary.

Resources:

a) SEC06-Access Control Policy -

Q62: Are controls enabled in your applications to provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls?

In order to be compliant with this question, you must:

- Ensure unintentional access has not been granted by evaluating the application based on best practices and known application exploits.

Note: This question is asking about applications that may grant unintentional access (backdoors). For example when Microsoft SQL Server is installed it automatically grants all Windows administrators full database access.

Resources:

a) SEC06-Access Control Policy -
Q63: Do applications provide safeguards against compromising the security of other systems with which information resources are shared?

In order to be compliant with this question, you must:

- Not share information resources with other Systems; or
- Deploy appropriate safeguards:
  - Limit or eliminate shared administrative service accounts;
  - Ensure intersystem authentication processes are properly protected (for example limiting access to read-only if only read access is required).

Resources:

a) SEC06-Access Control Policy -

Q64: Do applications provide access to only the owner; other nominated authorized individuals; or defined groups of users?

In order to be compliant with this question, you must:

- Not have RESTRICTED or CONFIDENTIAL information; or
- Ensure all users that access your System have appropriate levels of access based on current role.

Note: If you use file permissions to secure your RESTRICTED or CONFIDENTIAL data, make sure that the applications you use to access that data do not over-ride those security permissions.

Resources:

a) SEC06-Access Control Policy -

Q65: Are access control mechanisms such as Access control lists (ACLs), Constrained User Interfaces, Encryption, Port Protection Devices, Secure Gateways/Firewalls, Host-Based Authentication being used within the environment as security controls?

In order to be compliant with this question, you must:

- Mark this question 100% whether or not you have implemented any additional access control mechanisms.

Note: Per UW Medicine policy these access control mechanisms are to be considered. Documenting the additional access control mechanisms will be beneficial for audit purposes.

Resources:
Q66: If your system transmits electronic Protected Health Information (ePHI) outside of the University of Washington, is encryption being used to protect the data in transit?

In order to be compliant with this question, you must:
- Not have ePHI information, or
- Not transmit ePHI information outside of the University of Washington, or
- Encrypt ePHI being transmitted outside of the University of Washington.

Note: This question focuses only on electronic information being transmitted via data networks. This does not include transportation of physical media which is covered in SEC05.02 Media Handling Policy.

Resources:

b) SEC05.05-Cryptographic Controls Standard - [https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.05-CryptographicControls_Standard.doc](https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC05.05-CryptographicControls_Standard.doc)


Q67: Based on your information and information system classification, has a business continuity plan been developed?

In order to be compliant with this question, you must:
- Have the System classified as LOW for availability; and
- Not have ePHI;
- Develop a plan that protects your system based on the risks.

Note: If you have moderate or high availability needs you must have a business continuity plan.

Resources:

a) SEC02-Information & Information System Classification Policy - [https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC02-Info&InfoSystemClassification_Policy.doc](https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC02-Info&InfoSystemClassification_Policy.doc)
b) SEC02.00.01-Information & Information System Classification Guideline - [https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC02.00.01-Info&InfoSystemClassification_Guideline.doc](https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC02.00.01-Info&InfoSystemClassification_Guideline.doc)
Q68: Have regular reviews and updates to the business continuity plan been scheduled to ensure their continuing effectiveness?

In order to be compliant with this question, you must:

- Have the System classified as LOW for availability; and
- Not have ePHI;
- Review the business continuity plan to ensure appropriateness.
- Update the business continuity plan based on needs.

Resources:


Q69: Do you understand that as the System Owner and/or System Operator, you must abide by UW Medicine information security policies and avoid breaches of criminal and civil law as well as contractual obligations of security requirements?

In order to be compliant with this question, you must:

- Read and understand which regulations and policies apply to your system, and
- Understand the legal ramifications of non-compliance, and
- Follow the policies that apply to your system.
  - If your System can not meet a policy or standard you must apply for an exemption.

Resources:

a) SEC08-Compliance Policy - https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC08-Compliance_Policy.doc

Q70: Does the use of the software and information resources on your Systems match the specifications of the various software licenses?

In order to be compliant with this question, you must:

- Ensure that you have an appropriate quantity and the correct type of licenses for your software.
Q71: Are you aware of federal software copyright law and UW Medicine’s intent to take disciplinary action against workforce that breaches them?

In order to be compliant with this question, you must:
- Be aware that the University of Washington actively supports copyright laws, and
- Attend System Owner and Operator Training or
- Attend Department Manager Training.

Note: Software and information resources provided through UW for use by students, faculty, and staff may be used on computing equipment only as specified in the various software licenses. It is against UW policy for you to copy or reproduce any licensed software except as expressly permitted by the software license.

You may not use unauthorized copies of software on UW Medicine owned computers OR on personal computers ‘housed’ in UW facilities.

Unauthorized use of software, images, music, or files is regarded as a serious matter and any such use is without the consent of the UW Medicine.

If abuse of computer software, images, music, or files occurs, those responsible for such abuse may be held legally accountable as well as held personally accountable for violation of the UW Medicine policy.

Resources:

a) SEC08-Compliance Policy - https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC08-Compliance_Policy.doc

Q72: Do you maintain proof and evidence of ownership of licenses, master disks, manuals, etc.?

In order to be compliant with this question, you must:
- Be aware that the System Owner must maintain (keep track of) appropriate licenses for the System.
- Ensure that you have an appropriate quantity and the correct type of licenses for your software.

Resources:

a) SEC08-Compliance Policy - https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC08-Compliance_Policy.doc
Q73: As System Owner or System Operator are you aware you are responsible for:
   a) Implementing the Incident Response Policy at the appropriate management level;
   b) Providing the time, budget, and resources for Incident Response to be implemented as a part of normal business planning and;
   c) Demonstrating the courage to care and commitment to incident prevention by ensuring that this process is followed?

In order to be compliant with this question, you must:
   • Be reporting security incidents to Your Helpdesk; and
   • Appropriate time, budget, and resources have been allocated for the System for Incident Response.

Resources:

   a) SEC08-Compliance Policy -
      https://know1.mcis.washington.edu/manuals/AMC_SecurityPolicy/SEC08-Compliance_Policy.doc

   a) SEC11-Incident Response Policy -