

UW Medicine  
Computing Device Inventory Directions

**Computer Inventory Workbook Directions**

The Computer Inventory workbook is designed to help you organize the information that is collected when you conduct the inventory.

**Collecting the information:** There are three different methodologies available to assist you in collecting important inventory data for each system. Review the following tools and determine the best methodology for collecting data in your area and communicate this information with any individual(s) that you are going to assign to complete the inventory.

Computer Inventory Workbook – In some areas, it may be effective to distribute the Computer Inventory Workbooks to selected individuals who have sufficient knowledge of computer devices to easily gather the data. These individuals will input the inventory information directly into the spreadsheets and return them to the administrator (or designee) for further integration and analysis. The Inventory Workbook has separate spreadsheets to track the different types of computing devices:

- Workstations
- Servers
- Printers
- Other Devices
  - Network-connected devices - using wired or wireless technology
  - Examples include: client devices (WAP phones, PDAs, WorkPads); network connected medical devices (internet digital microscopes, scanning devices; and sonographs); and equipment control devices

Inventory Collection Paper Form – Some Administrators will find the paper form is the most effective method to use to collect information about each computing device. Individuals assigned to do this would physically locate and assess each device and write the data on the form. After completing a form for each of the computing devices, the data would then be transferred into the Computer Inventory Workbook.

Inventory Collection Web Form – This tool is similar to the paper form, but is run from a web link. This tool will automatically check for some of the information needed on PC workstations and fill the information into the web-form to assist the individual completing the form. The data automatically collected will be in a shaded field.

Individuals completing the inventory will complete the information while sitting at each workstation and electronically submit the completed form to the contact in the department who is collecting the inventory data. The data will also be sent to UW

**UW Medicine**  
**Computing Device Inventory Directions**

Medicine's Security Integration Team who will use this data to more quickly respond to security incidents.

The inventory results will be received by the department contact in the form of a "csv" (common separated values) file that can be opened in Excel. This can then be "cut and pasted" into the Computer Inventory workbook under the appropriate device tab.

**Data and Systems Analysis:**

After all of the computing devices have been inventoried, the data must be analyzed to effectively group your devices into "systems". When you have completed this analysis, then you should document your Systems and assign System Owners and System Operators in the Inventory Workbook.

Use the "Systems & SO-SO" spreadsheet to document:

[A] System Name:

Naming conventions: Bottom line, whatever works for you.

Recommendations:

- Designates location
- Designates primary use
- Designates user base

[B] System Owner:

Every system has an owner, the individual(s) that you identified as having responsibility, authority over, or a vested interest in maintaining the system, is probably the System Owner.

[C] System Operator:

System Operators administer and manage the daily activities of one or more electronic information systems, electronic databases, or electronic applications under the direction of the System Owner. In some cases the System Operator may also be the System Owner. These individuals usually have some level of competency and experience with the various systems that they operate. For example, a System Operator could be someone identified as being the "computer guru" of a unit. In other cases the operator functions could be contracted out.

[D] Information Security Survey:

Information Security Survey (ICR) number – you will receive this number when you complete the online survey

[E] Individual Who Completed Survey:

[F] Survey Date:

[G] System Specifics/Description:

Relationship between the devices inventoried and the systems as defined.

**UW Medicine**  
**Computing Device Inventory Directions**

**Help:**

For questions regarding the computer inventory, contact the appropriate person listed below:

- **School of Medicine:** Steve Herber, Security Engineer, Security Integration Team (SIT), UW Medicine IT Services, (206) 221-7262, [herber@u.washington.edu](mailto:herber@u.washington.edu)

If you do not have resources available within your department to complete the inventory, the following document lists vendors and UW support organizations which offer services for a fee: [List of Computer Support Vendors](#) (url).

**UW Medicine**  
**Computing Device Inventory Directions**

**The Inventory Workbook:**

There are five separate spreadsheets in the workbook.

1. Workstations (For information about desktops & laptops)
2. Servers (For information about computers that are used as servers)
3. Printers
4. OtherDevices (Network-connected devices - using wired or wireless technology - Examples include: client devices (WAP phones, PDAs, WorkPads); network connected medical devices (internet digital microscopes, scanning devices; and sonographs); and equipment control devices)
5. Systems&SO-SO (To document “systems” and the individuals designated responsible – the Systems Owners and Systems Operators)

The top of the “Workstations” sheet has the following

**Cell Information Collected**

[A1] Department: \_\_\_\_\_  
 [A2] Division: \_\_\_\_\_  
 [A3] Inventory Area: \_\_\_\_\_  
 [A4] Submit to: \_\_\_\_\_  
 [A5] Inventory Done By: \_\_\_\_\_  
 [A6] Due Date: \_\_\_\_\_

The information in these cells auto-populates the A1-A6 cells on the “servers”, “Printers” and “OtherDevices” sheets.

<b>Column</b>	<b>Data Elements</b>	<b>Explanation/Directions</b>
<b>[A]</b>	Device type	“ Workstations” this is a drop down for desktops and laptops. “Servers” & “Printers” will not distinguish in this field. “OtherDevices” – free text field to gather broad range of information like PDAs, WorkPads, internet digital microscopes, scanning devices; and sonographs.
<b>[B]</b>	Primary Use	Field used to capture the primary use of the device: General Office/ Patient Care/ Research/ Teaching/Other
<b>[C]</b>	Specify “Other” Primary Use	
<b>[D]</b>	Primary User	Field used to capture the name of the individual who is the primary user of the device
<b>[E]</b>	Device location	The physical location/room number of the device
<b>[F]</b>	Phone # close to	When there is a problem (like a compromised computer) the Security Infrastructure Team wants a phone number close to

**UW Medicine**  
**Computing Device Inventory Directions**

	device	the machine to attempt to reach someone
<b>[G]</b>	Device make	Collect name of brand name of device (pick list)
<b>[H]</b>	Specify "Other" Device make	
<b>[I]</b>	Device network connected?	This includes Wired, Wireless, Modem
<b>[J]</b>	Identification No.	Examples: Serial No. (The serial number assigned by manufacturer); Department Tag No. (If there was a departmental property tag assigned); UW Tag No. (If there was a UW property tag assigned)
<b>[K]</b>	OS (Operating system)	Drop down list provided <hr/> Finding Windows OS Version: Click Start - Run. Then type WINVER  Finding Macintosh OS version: Details at --> <a href="http://www.jmu.edu/computing/mac/about.shtml">http://www.jmu.edu/computing/mac/about.shtml</a> <hr/> * Part of Minimum Information Security Requirements *
<b>[L]</b>	Specify "Other" OS	
<b>[M]</b>	Security event logging & auditing enabled?	* Part of Minimum Information Security Requirements *
<b>[N]</b>	Patching frequency	Drop down list provided. Note: Policy requires that we ensure operating system and application patches and/or updates be applied in a "reasonably timely manner". <hr/> * Part of Minimum Information Security Requirements *

**UW Medicine**  
**Computing Device Inventory Directions**

<b>[O]</b>	IP address	<p>An identifier for a computer or device on the network. The UW network routes messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.</p> <hr/> <p>Find IP address in Windows 95/98:  Click Start - Run. Then run WINIPCFG</p> <p>Find IP address in Windows NT/2000/XP/2003  Click Start - Run. Then run CMD. In the cmd window run IPCONFIG</p> <p>Find IP address on Macintosh (pre OS X)  Apple Menu --&gt; Control Panels --&gt; TCP/IP Control Panel</p> <p>Find IP address on Macintosh OS X  Open System Preferences. Under Internet and Network, click 'Network'</p>
<b>[P]</b>	MAC Address	<p>Short for Media Access Control, a hardware address that uniquely identifies each node of a network.</p> <hr/> <p>All platforms: How to find MAC address:  Details at --&gt;  <a href="http://www.net.princeton.edu/enetAddress.howto.html">http://www.net.princeton.edu/enetAddress.howto.html</a></p>
<b>[Q]</b>	Firewall or network filter	<p>Drop down list provided</p> <hr/> <p>* Part of Minimum Information Security Requirements *</p>
<b>[R]</b>	Specify "Other" Firewall or network filter	
<b>[S]</b>	Protection against malicious software (Anti-Virus)	<p>Drop down list provided</p> <hr/> <p>Active &amp; up-to-date protection against malicious software  * Part of Minimum Information Security Requirements *</p>
<b>[T]</b>	Specify "Other" Protection against malicious software (Anti-Virus)	
<b>[U]</b>	PHI (Protected Health Information)	<p>Data Type - Mark all that apply</p>

**UW Medicine**  
**Computing Device Inventory Directions**

<b>[V]</b>	SSN (Social Security Numbers)	Data Type - Mark all that apply
<b>[W]</b>	Sensitive Student Information	Data Type - Mark all that apply
<b>[X]</b>	Intellectual Property	Data Type - Mark all that apply
<b>[Y]</b>	Critical Research Data	(If it is lost, you might as well clear your desk) Data Type - Mark all that apply
<b>[Z]</b>	non-sensitive public data	Data Type - Mark all that apply
<b>[AA]</b>	Specify "Other" Data Type	Data Type - Mark all that apply
<b>[AB]</b>	Specify "Other" Data Type	Data Type - Mark all that apply
<b>[AC]</b>	"Don't Know" Data Type	
<b>[AD]</b>	Data Classification Confidentiality	Drop down list: CONFIDENTIAL-High RESTRICTED-Moderate PUBLIC-Low <hr/> Confidentiality - Low/Public = Information that is either approved for general access, or by its nature, is not necessary to protect, and can be shared with anyone; Moderate/Restricted = information intended strictly for use by designated UW Medicine employees and agents, less sensitive than CONFIDENTIAL information, dissemination of this data shall only be made to UW Medicine workforce with an established "need-to-know"; High/CONFIDENTIAL = information very sensitive in nature that requires careful controls and protection, examples include: Personally identifiable information, medical records protected health information, workforce records, student records, social security numbers, legally protected University records, intellectual property.
<b>[AE]</b>	Data Classification Integrity	Drop down list: High Moderate Low <hr/> Integrity - Low = information or information systems that have a limited adverse effect to UW Medicine if changed, altered, or

**UW Medicine**  
**Computing Device Inventory Directions**

		<p>deleted. Moderate = information or information systems that have a serious adverse effect on UW Medicine if changed, altered, or deleted. High = information or information systems that have a severe adverse effect on UW Medicine if changed, altered, or deleted.</p> <hr/> <ul style="list-style-type: none"> <li>• Limited adverse effect:             <ul style="list-style-type: none"> <li>i. cause a degradation in mission capability to an extent and duration that UW Medicine is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;</li> <li>ii. result in minor damage to UW Medicine assets;</li> <li>iii. result in minor financial loss; or</li> <li>iv. result in no harm to individuals.</li> </ul> </li> <li>• Serious adverse effect:             <ul style="list-style-type: none"> <li>i. cause a significant degradation in mission capability to an extent and duration that UW Medicine is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;</li> <li>ii. result in significant damage to UW Medicine assets;</li> <li>iii. result in significant financial loss; or</li> <li>iv. result in harm to individuals that does not involve loss of life or serious life threatening injuries.</li> </ul> </li> <li>• Severe adverse effect:             <ul style="list-style-type: none"> <li>i. cause a severe degradation in or loss of mission capability to an extent and duration that UW Medicine is not able to perform one or more of its primary functions;</li> <li>ii. result in major damage to UW Medicine assets;</li> <li>iii. result in major financial loss; or result in harm to individuals involving loss of life or serious life threatening injuries.</li> </ul> </li> </ul>
<p><b>[AF]</b></p>	<p>Data Classification Availability</p>	<p>Drop down list:            High            Moderate            Low</p> <hr/> <p>Availability - Low = information or information systems that have a limited adverse effect to UW Medicine if a disruption of access to the information or an information system occurs. Moderate = information or information systems that have a serious adverse effect on UW Medicine if a disruption of access to the information or an information system occurs. High = information or information systems that have a severe adverse effect on UW Medicine if a disruption of access to the information or an information system occurs.</p> <hr/> <ul style="list-style-type: none"> <li>• Limited adverse effect:             <ul style="list-style-type: none"> <li>i. cause a degradation in mission capability to an</li> </ul> </li> </ul>

**UW Medicine**  
**Computing Device Inventory Directions**

		<p>extent and duration that UW Medicine is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;</p> <ul style="list-style-type: none"> <li>ii. result in minor damage to UW Medicine assets;</li> <li>iii. result in minor financial loss; or</li> <li>iv. result in no harm to individuals.</li> </ul> <ul style="list-style-type: none"> <li>• Serious adverse effect: <ul style="list-style-type: none"> <li>v. cause a significant degradation in mission capability to an extent and duration that UW Medicine is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;</li> <li>vi. result in significant damage to UW Medicine assets;</li> <li>vii. result in significant financial loss; or</li> <li>viii. result in harm to individuals that does not involve loss of life or serious life threatening injuries.</li> </ul> </li> <li>• Severe adverse effect: <ul style="list-style-type: none"> <li>iv. cause a severe degradation in or loss of mission capability to an extent and duration that UW Medicine is not able to perform one or more of its primary functions;</li> <li>v. result in major damage to UW Medicine assets;</li> <li>vi. result in major financial loss; or</li> <li>vii. result in harm to individuals involving loss of life or serious life threatening injuries.</li> </ul> </li> </ul>
<b>[AG]</b>	<b>Servers Only</b> Is it compliant with information security configuration & hardening guidelines & procedures?	
<b>[AH]</b>	<b>Servers Only</b> Maintained in a secure location?	Designated area that provides adequate physical security, environmental controls, and appropriate entry controls. Physically protected from unauthorized access, damage and interference.
<b>[AI]</b>	<b>Servers Only</b> Received Server System Certification?	To ensure compliance with the Server System Information Security Standard, all networks systems are subject to system security certification. This certification process evaluates the system security controls based on defined minimum requirements as well as controls deemed necessary through observance of industry best practices or risk analysis. Certification is conducted by UW Medicine IT Services Security Infrastructure Team (SIT) staff and accepted by the System Owner. Certification status is based on the following:

**UW Medicine**  
**Computing Device Inventory Directions**

		<p>1. Certified: Security measures meet or exceed our UW Medicine’s Information Security Standards.</p> <p>2. Provisional Certification: System exceptions have been requested and approved by the System Owner and Director of Security or the system is on “probationary status” under which identified security risks must be corrected according to a plan developed by the System Owner and Director of Security.</p> <p>3. Non-Certification: Certification is denied due to inadequate security measures that result in a risk to confidentiality, integrity, and/or availability that is too great for the system to be connected to the network.</p> <p>System(s) that fail certification (i.e. receive Non-Certification) are denied network privileges on UW production networks. For more information, please see documentation for the UW Medicine Server System Certification Process on the Security Infrastructure Team website (under SIT Services) <a href="https://security.uwmedicine.org/">https://security.uwmedicine.org/</a></p>
<p><b>[AJ]</b></p>	<p><b>Servers Only</b>  Backup &amp; recovery plan created &amp; Maintained?</p>	<p>Information Backup Standard  Back-up copies of essential business information and software must be made regularly.</p> <p>System Owners are responsible for ensuring that data backup occurs. This function is critical to contingency planning and to ensure proper recovery following a disaster or media failure. Frequency of backups will depend upon how often data changes and how important those changes are.</p> <p>System Owners and System Operators may consult with IT Services TSO (Technical Services Organization) to determine what backup schedule is appropriate. All data backups are stored according to data classification (See SEC02 Asset Classification and Control Policy) and UW records retention policies. Backup copies are to be tested to ensure that they are usable.</p> <p>The following control guidelines are recommended for System Owners and System Operators:</p> <p>A. A minimum level of back-up information includes:</p> <ol style="list-style-type: none"> <li>1. Accurate and complete records of the back-up copies and documented restoration procedures.</li> <li>2. Three generations or cycles of back-up information for critical data.</li> </ol> <p>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.</p> <p>C. Where practical, regularly test back-up media to ensure reliability for emergency use.</p>

**UW Medicine**  
**Computing Device Inventory Directions**

		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.
<b>[AK]</b>	Who provides technical support for this device?	Drop down list
<b>[AL]</b>	Name:	Of the individual who provides technical support for this device
<b>[AM]</b>	Phone:	Of the individual who provides technical support for this device
<b>[AN]</b>	Notes:	For your use