Applicability: UW Medicine

Policy Title: Computing Device and System Security Policy

Policy Number: SP-02

Superseded Policy(ies) or Entity Policy: N/A

Date Established: March 1, 2012

Date Effective: March 1, 2012

Dates Revised: March 1, 2012

Next Review Date: March 1, 2015

PURPOSE AND SCOPE
This policy defines the requirements for protecting UW Medicine computerized devices and information systems in accordance with regulatory requirement and University policy.

This policy applies to all computing devices and systems that use, access, transmit, or store UW Medicine electronic data. All UW Medicine computing devices must also meet the University of Washington Administrative Policy Statements.

Computing devices include but are not limited to: desktop and laptop computers, smart phones, tablet PCs, servers, and applications.

A computing system is any computing device or collection of devices that is used for UW Medicine business.

This policy applies to all UW Medicine workforce members.

POLICY PRINCIPLES/STATEMENT
See POLICY.

DEFINITIONS
Defined within POLICY.

POLICY
All computing devices and systems used to conduct UW Medicine business must meet the requirements below pertaining to the use, management, maintenance, and security of the device(s) in addition to all applicable University of Washington Administrative Policies.
I. Planning and Acceptance (PA)

Prior to purchasing a computing device or system, the security aspects must be evaluated and documented, including where the device will be housed, if it will be connected to a UW Medicine network, who will have access to the data, whether or not it will access, transmit, or store restricted or confidential data.

Requirement: (PA-1) Prior to purchasing a computing device that will be classified as confidential, system characterization and the proposed security controls must be documented according to the System Security Process Standard. Documentation must be maintained by the system owner and system operator.

II. Purchasing Computing Devices (PCD)

All computing devices within UW Medicine must have the appropriate documentation in place prior to purchase if the device(s) will be supported by the vendor or a non-UW Medicine workforce member.

Requirement: (PCD-1) Any computing device or system requiring vendor support that transmits, processes, or stores Protected Health Information (PHI) must have a Business Associate Agreement in place prior to the purchase.

Requirement: (PCD-2) If a vendor or other non-UW Medicine workforce will have access to Restricted or Confidential data, including but not limited to PHI, on a computing device or system, a Data Security Addendum must be signed by those non-UW Medicine workforce prior to purchasing of the system.

III. Security Agreements (SA)

Security agreements are any legal document, signed by a UW Medicine workforce member who has been granted signing authority, that pertains to a computing device or system.

Requirement: (SA-1) Appropriate security agreements must be signed by all third party vendors and authorized UW Medicine personnel prior to the purchase or lease of a computing device or system.

IV. Personally Owned Computing Devices (POCD)

UW Medicine recognizes the need for some workforce members to use personally owned devices to conduct business operations.

Requirement: (POCD-1) Any computing device that is personally owned by a UW Medicine workforce member, who is using it for UW Medicine business operations, and has it connected to
a UW Medicine network must insure that the computing device meets the same security policy
requirements any UW Medicine owned device must meet.

V. System Criticality (SC)

The criticality of a system helps to define its impact to business operations, how the business
continuity plan should be structured, and provides users of the computing device or system
expectations for performance.

Requirement: (SC-1) All computing devices and systems must have a criticality assigned based on its
importance to UW Medicine business operations. See the UW Medicine APOP – Policy for Use and
Access to Enterprise Data Center Facilities for details on how to determine your computing device or
systems criticality.

VI. Physical Security (PS)

UW Medicine has many publicly accessible areas. Access to computing systems must be restricted
based on the system’s criticality.

Requirement: (PS-1) All computing devices must have physical security controls in place
commensurate with their System Criticality and value. No computing device or system with
electronic data classified as Restricted or Confidential can be stored or hosted in a public area.

Requirement: (PS-2) All computing devices and systems must have controls in place to mitigate theft
and unauthorized access.

Requirement: (PS-3) All computing devices must have environmental controls in place to mitigate
damage caused by environmental threats such as moisture, fire, dust, and temperature.

Requirement: (PS-4) All system owners must keep a maintenance log that records who accessed the
hardware and for what purpose. Maintenance logs must be retained for a minimum of two
months.

VII. System Ownership (SO)

Collections of computing devices are more complex to manage and maintain than a single device.
System owners are responsible for all aspects of the system.

Requirements: (SO-1) All computing systems in use at UW Medicine must have a system owner
designated according to APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions.

Requirement: (SO-2) System Owners must be current UW Medicine workforce members.

VIII. User Access (UA)
User Access must be restricted using the principle of least privilege, and have the necessary authorization and authentication methods to restrict data access to only authorized users.

Requirement: (UA-1) All computing devices must have an authorization and authentication mechanism that meets the requirements of the classification of that system’s data.

Requirement: (UA-2) All computing devices must allow users to change their passwords at least 120 days. The system owner must enforce password rotation requirements and lock a user account if the password is allowed to expire.

Requirement: (UA-3) Workforce members will only be given access to data and resources they need to complete their assigned work.

Requirement: (UA-4) For workforce members terminated with cause, a process must be in place to remove user access immediately.

IX. Hardware Security (HS)

Requirement: (HS-1) All computing devices and systems must have a maintenance schedule implemented to insure the computing device or system is in proper running order to meet its business purpose.

X. Software Security (SS)

Requirement: (SS-1) All software used on UW Medicine computing device and systems must be kept up to date, evaluated for security vulnerabilities, and be supported either by the vendor or designated UW Medicine workforce.

Requirement: (SS-2) Off-the-shelf software must be updated regularly.

Requirement: (SS-3) Custom software must be assessed for vulnerabilities before being put into production.

Requirement: (SS-4) Unsupported software must not be installed on any UW Medicine networked computing device.

XI. Network Security and Protection Against Malicious code (NSMC)

All UW Medicine computing devices must be protected from malicious code and unauthorized access using the appropriate methodologies for the device or system.
Requirements: (NSMC-1) All UW Medicine computing devices connected to any University of Washington network must have security controls in place to prevent unauthorized access from network or code based attack vectors.

XII. Computing Device Disposal (CDD)

Many UW Medicine computing devices are resold to the general public to gather any residual value left in the computing device.

Requirement: (CDD-1) All computing devices must have all information rendered inaccessible in accordance with the Data Disposal Standard prior to being transferred to an authorized University department for disposal.

XIII. Event Logging (EL)

Depending on the type of computing device or system there are different types of event logs; not all computing devices will have event logging capabilities.

Requirement: (EL-1) All computing devices with event logging capabilities must have event logging enabled.

Requirement: (EL-2) All system administrators are responsible for maintaining and reviewing event logs.

Requirement: (EL-3) Event logs must be retained according to the system’s data classification.

XIV. Computing System Monitoring (CSM)

UW Medicine networks are constantly under attack by external sources. All systems must be monitored for signs of intrusion and/or unauthorized access.

Requirement: (CSM-1) All computing devices and systems regardless of criticality must be monitored for unauthorized access.

XV. Business Continuity (BC)

All computing devices and systems at UW Medicine play a role in business operations. It is very important for system owners and users of the computing devices and systems to understand that role.

Requirement: (BC-1) All computing devices and systems must have a written business continuity plan that outlines how business operations will continue in the event that the computing device or system fails.
Requirement (BC-2) The business continuity plan must contain sections addressing disaster recovery, emergency mode operations, testing and revision procedures, and applications and data criticality analysis.

XVI. System Level Risk Assessment (SLRA)

Risk Assessments are needed to identify gaps in security control coverage. Performing risk assessments on systems will identify vulnerabilities that can be mitigated by adding security controls.

Requirement: (SLRA-1) All computing systems must have a written risk assessment documented.

Requirement: (SLRA-2) System Level Risk Assessments must be updated at least annually or when there are changes to the system or the threat environment.

Requirement: (SLRA-3) All risks identified as a high classification must be mitigated. If mitigation is not possible, it must be reported to UW Medicine executive management.

XVII. Incident Response (IR)

When a computing device is involved in an incident it is extremely important to follow APS 2.5 Information Security and Privacy Incident Reporting and Management Policy, preserve the evidence, contain the damage, and recover business operations.

Requirement: (IR-1) All incidents must be reported to the office designated in the APS 2.5 Information Security and Privacy Incident Reporting and Management Policy as soon as they are discovered or suspected.

Requirement (IR-2) All incidents will follow the process outlined in the APS 2.5 Information Security and Privacy Incident Reporting and Management Policy and the procedures outlined in the Incident Response Plan (IRP).

REGULATORY/LEGISLATION/REFERENCES

None.

PROCEDURE ADDENDUM(s) REFERENCES/LINKS

- System Security Process Standard
- Data Security Addendum
- Data Disposal Standard
- UW Medicine APOP – Policy for Use and Access to Enterprise Data Center Facilities
- University of Washington Administrative policies (UW APS)
- UW APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions
- UW APS 2.5 Information Security and Privacy Incident Reporting and Management Policy
- Incident Response Plan (IRP)
ROLES AND RESPONSIBILITIES
Defined within POLICY.

AUTHORITIES

<table>
<thead>
<tr>
<th>Custodian</th>
<th>Responsible Officer</th>
<th>Implementation Officer</th>
<th>Administrative Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td><strong>Owner</strong></td>
<td><strong>Auditor</strong></td>
<td><strong>Endorser</strong></td>
</tr>
<tr>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Compliance</td>
<td>UW Medicine Executive Compliance Committee</td>
</tr>
</tbody>
</table>

APPROVALS

Approved By Dr. James S. Fine  
Chief Information Officer, UW Medicine  
Date

Approved By Johnese Spisso  
Chief Health System Officer, UW Medicine, &  
Vice President for Medical Affairs, University of Washington  
Date