PURPOSE AND SCOPE
This policy defines the requirements for reducing the information security risks associated with human error, theft, fraud, or misuse of electronic data or computing devices. Policy requirements in the areas of job definition, security awareness training, and workspace security have been developed to aid UW Medicine in reaching this goal.

This policy applies to all individuals designated as a UW Medicine workforce member; UW Medicine policies may also apply to any individual that is conducting business for or on behalf of UW Medicine.

UW Medicine workforce members are employees, trainees, students, volunteers, and other entities or persons who perform work for UW Medicine.

POLICY PRINCIPLES/STATEMENT
See POLICY.

DEFINITIONS
Defined within POLICY.

POLICY
All workforce members must adhere to these policy requirements and any other applicable University of Washington Administrative Policies.

I. User Account Maintenance (UAM)

UW Medicine workforce members may be given various accounts to perform their prescribed job functions. These accounts provide access to electronic data and must be managed to prevent misuse.
Requirement: (UAM-1) All UW Medicine workforce members must use strong passwords with their accounts. A strong password includes uppercase and lowercase letters, numbers, special characters and are at least 8 characters in length.

Requirement: (UAM-2) All UW Medicine workforce members must change the passwords associated with their accounts every 120 days.

Requirement: (UAM-3) All UW Medicine workforce members will be granted only as much access to Confidential data as is needed to complete their duties.

II. Administrator Privileges (AP)

Some job functions at UW Medicine require a workforce member to be granted administrator rights on computing devices.

Requirement: (AP-1) All UW Medicine workforce members who are granted administrator rights must only use their administrator access to perform administrator level job functions.

III. System Ownership (SO)

Computing systems at UW Medicine are required to have a system owner and system operator assigned to them to assure that proper security controls are implemented on all computing devices associated with that system.

Requirement: (SO-3) System owners must document the security controls, business continuity and disaster recovery plan, and perform a system level risk assessment for each of their assigned systems.

Requirement: (SO-4) System owners must verify that the documentation for each of their systems is up to date on an annual basis.

Requirement: (SO-5) System owners must ensure there is a system administrator or someone capable of performing system administration activities for each of their assigned systems.

IV. Computing Device Allocation (CDA)

All computing devices will be assigned to workforce members as needed, tracked by their managers, and wiped of all data upon re-allocation or transfer to surplus.

Requirement: (CDA-1) All supervisors (managers, directors, chairs, deans) must track computing device allocation for each workforce member that reports directly to them.
**Requirement**: (CDA-2) All computing devices that are being re-allocated to another UW Medicine workforce member or retired to surplus must first be reformatted to render any previous electronic data inaccessible.

**V. Computing Device Disposal (CDD)**

There are many times when computing devices are transferred or determined to be of no further use to UW Medicine.

**Requirement**: (CDD-2) All computing devices must be evaluated to see if they have any residual value after they are no longer needed for use at UW Medicine.

**Requirement**: (CDD-3) All computing devices must be transferred to authorized UW Medicine or UW departments for disposal.

**Requirement**: (CDD-4) Data that may have been previously stored on a computing device must be rendered inaccessible.

**VI. Internet Access Privileges (IAP)**

Most computing devices at UW Medicine have Internet access. This access is needed for conducting business operations; all other capabilities of the Internet are considered privileged.

**Requirement**: (IAP-1) All UW Medicine workforce members must only use internet access for business purposes or limited personal use when the cost to the institution is negligible.

**VII. Incident Response (IR)**

UW Medicine follows very strict incident response regulatory requirements and procedures for all computing security incidents.

**Requirement**: (IR-1) All UW Medicine workforce members must report any suspected or known information security incident to the designated office in the UW APS Information Security and Privacy Incident Reporting and Management Policy.

**REGULATORY/LEGISLATION/REFERENCES**
None.

**PROCEDURE ADDENDUM(s) REFERENCES/LINKS**
- University of Washington Administrative Policies
- UW APS Information Security and Privacy Incident Reporting and Management Policy

**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>Author</td>
<td>Owner</td>
<td>Auditor</td>
<td>Endorser</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

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