

---

Department: UW Medicine Information Technology Services

Policy Number: SEC-09 – Information Security Risk Management Policy

Effective Date: June 11<sup>th</sup>, 2007

Review Date: April 27<sup>th</sup>, 2007

---

### **Purpose**

The Information Security program is committed to increasing shared awareness and responsibility for Risk management. It is the goal of this policy to establish the basis for a risk assessment and response process. .

### **Definitions**

See UW Medicine Information Security policy: *SEC-REF UW Medicine Information Security Program Glossary of Terms.*

### **Policy**

It is UW Medicine policy that a risk assessment is performed for all information systems System Owners are required to take appropriate actions to ensure the confidentiality, integrity, and availability of all ePHI that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information. conduct risk assessments on their system(s) and participate in the Annual UW Medicine Risk Assessment.

#### **I. Responsibilities:**

- A.** System Owners are responsible for risk assessment, reduction, and prevention for their systems including ongoing evaluation and risk management. This process includes methods for management, avoidance, mitigation, financing, and/or acceptance of the risk.

The System Owner may involve the System Operator and/or the Department Administrator/Manager as appropriate.

- B.** Risk assessments must occur, at the following times:

- At the inception of new systems, applications, facilities, etc. that may impact the security of UW Medicine Information or Information Systems.
- Before enhancements, upgrades, and conversions associated with critical systems or applications.

- When state or federal regulation requires risk determination.
- When UW Policies require it.

C. UW Medicine CIO is responsible for insuring an annual Risk Assessment is completed.

- The CIO may designate another individual, such as the Director of Network Security, or other official to complete this task.

## II. Components

### A) Risk Assessment

Risk assessment is used to determine potential threats and the risks associated with an IT system. (See UW Medicine Information Security Standard: *SEC-09.01 –Risk Assessment Guideline.*) . System Owners whose systems have information risk assessments producing HIGH risk to UW Medicine information or information systems must report the results to the IT Services Help Desk in order for SIT to conduct further evaluation and provide guidance.

### B) Risk Reduction and Prevention

Risk reduction methods include administrative, physical, and technical controls. If the risk assessment process discovers that a server, system or application has risks to information security, then controls should be implemented to reduce the risk level to appropriate levels. UW Medicine IT Services Security Infrastructure Team (SIT) can be consulted to recommend appropriate controls to reduce risks.

The methods to reduce risk and implement controls vary between systems using administrative measures, industry best practices, and appropriate information security technologies.

Dependent upon risk, equipment value, and the critical nature of the system, the System Owner may determine that it is prudent to purchase equipment insurance through the University Of Washington Office Of Risk Management,  
<http://www.washington.edu/admin/rmequip/>

---

### References:

- I. 45 CFR Part 164; Section 164.308(a) (1) (ii) (A) Risk Analysis, (B) Risk Management
- II. 45 CFR Part 164; Section 164.308(a)(8) Evaluation

**III.** NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems

---

---

UW Medicine IT Services: \_\_\_\_\_ Date: \_\_\_\_\_  
James S. Fine, M.D., CIO, ISO

---

---