UW Medicine

INFORMATION TECHNOLOGY SERVICES

SECURITY

IT Services Policies, Standards and Guidance

Information Security Risk Management Standard

Department: IT Services

Policy Number: SS-06

Effective Date: April 26th, 2017

Revision Date:

Reviewer:

OBJECTIVE

Define the governance, process and risk levels used to manage risks to UW Medicine that result from threats to the confidentiality, integrity, and availability of information systems, facilities, and third party providers to UW Medicine

SCOPE

All information systems used to conduct business operations on behalf of UW Medicine, the facilities that house UW Medicine components, service providers of UW Medicine, and any other device or component that can pose a risk to UW Medicine operations.

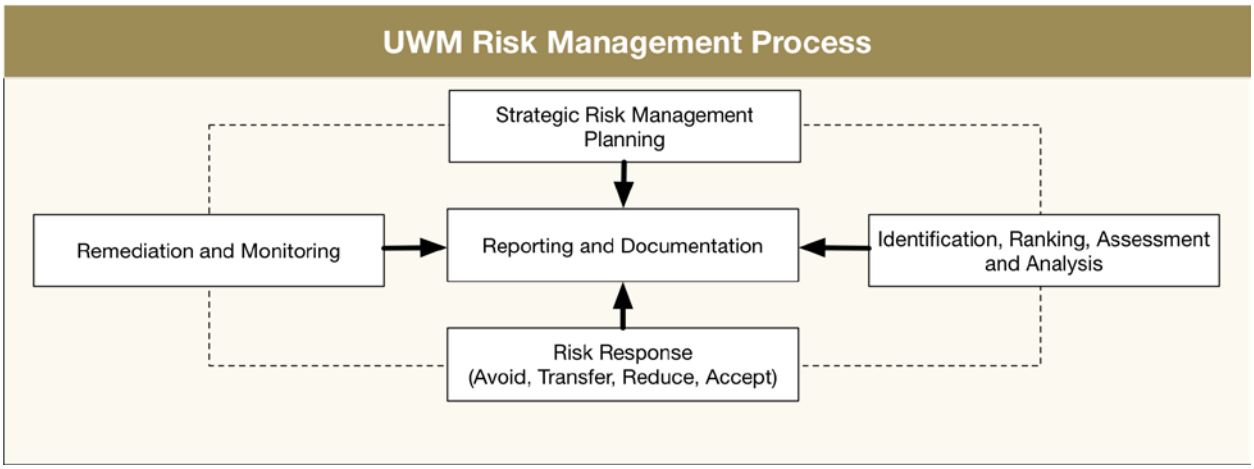
Standard

1. Risk Governance
    a. Chief Health Systems Officer (CHSO) – The CHSO has the authority and responsibility for reviewing and approving the risk response options (avoid, transfer, reduce, or accept)
    b. Security Program Executive Committee (SPEC) – SPEC has the authority and responsibility to review and approve the risk management program, establish risk tolerance levels and recommend the response options to the CHSO for risks that are discovered.
    c. UW Medicine Chief Information Security Officer (CISO) – The CISO has the authority and responsibility to develop and oversee the risk management program and provide documentation and reports on risks to executive leadership and SPEC
    d. UW Medicine Security (Security) – Responsible for completing risk ranking, assessments, working with system owners to find reasonable risk response options, and monitoring for changes to the threat environment.
    e. UW Medicine system owners – Responsible for participating in Security activities, documenting and implementing risk response plans, monitoring for changes their systems that affect security controls.

2. Risk Management Process

a. Risk management is the continuous process that allows UW Medicine to balance the operational impacts and economic costs of information security controls while enhancing capabilities and decreasing risks. The key elements of the risk management process include:
    i. Strategic risk management planning
    ii. Identification, ranking, assessment, and analysis
    iii. Risk response
    iv. Remediation and monitoring
    v. Reporting and documentation

b. The high level process is shown in the figure below.



3. Risk Impact – risk levels are established based on the table below:

Impact Level	Description

Severe	• **Strategic**
	  o Represents a significant threat to UW Medicine's mission and the safety or well-being of the UW Medicine community
	• **Operational**
	  o Sustainment issues related to essential UW Medicine services lasting > 1 day(s)
	• **Compliance**
	  o Significant compliance exposure or legal liability
	• **Financial**
	  o Annual loss of $1 million or more
	• **Reputational**
	  o Severe reputational harm including National media coverage > 1 week

High	• **Strategic**
	  o Represents a moderate threat to UW Medicine's mission and the safety or well-being of the UW Medicine community
	• **Operational**
	  o Sustainment issues related to essential UW Medicine services for 1 day or series of 12-24 hour outages

	• **Compliance**
	  o Moderate compliance exposure or legal liability
	• **Financial**
	  o Annual loss of $100,000 - $1 million
	• **Reputational**
	  o Moderate reputational harm including National media coverage < 1 week

Moderate	• **Strategic**
	  o Represents a low threat to UW Medicine's mission and the safety or well-being of the UW Medicine community
	• **Operational**
	  o Sustainment issues related to essential UW Medicine services < 1 day
	• **Compliance**
	  o Low compliance exposure or legal liability
	• **Financial**
	  o Annual loss of $10,000 - $100,000
	• **Reputational**
	  o Low reputational harm including Washington State media coverage

Low	• **Strategic**
	  o Represents a minimal threat to UW Medicine's mission and the safety or well-being of the UW Medicine community
	• **Operational**
	  o Localized disruption and no disruption of essential UW Medicine services
	• **Compliance**
	  o Minimal compliance exposure or legal liability
	• **Financial**
	  o Annual loss of $100 - $10,000
	• **Reputational**
	  o Minimal reputational harm

Minimal	• **Strategic**
	  o Represents a negligible threat to UW Medicine's mission
	• **Operational**
	  o Minimal disruption
	  o Negligible threat to safety or well-being of the UW Medicine community
	• **Compliance**
	  o Negligible compliance exposure or legal liability
	• **Financial**
	  o Annual loss of < $100
	• **Reputational**
	  o Negligible impact

4. Risk Likelihood – estimation of how likely a risk is to be realized within a given year as represented by the table below:

Risk Likelihood	Rate of Occurrence (Annual)	Description
Certain	75% - 100%	Very high chance of being realized each year
Probable	30% - 75%	Fair chance of being realized each year
Occasional	5% - 30%	Modest chance of being realized each year
Rare	0% - 5%	Small chance of being realized each year

5. Risk Velocity - Estimation on how fast the impact of the risk may affect UW Medicine entities

Velocity Level	Time to Impact	Reaction Time
High	Risk impact will be felt in less than 3 months after the occurrence	There will be little or no time for reaction and response planning before serious consequences of the risk are felt
Medium	Risk impact will be felt in 3 – 9 months after the occurrence	There will be limited time for reaction and response planning before serious consequences of the risk hit
Low	Risk impact will be felt in more than 9 months after the occurrence	There will be time for reaction and response planning before serious consequences of the risk hit

CROSS REFERENCE

SS-02 Risk Assessment Standard

ATTACHMENTS

None

REVIEW / REVISION DATES

TBD

UW Medicine Chief Information Security Officer: _____ Date: _____

UW Medicine CIO: _____ Date: _____