MUSC Information Security - System Identification

Compliance Process Step: Document Current System Environment and Personnel

Instructions

Please refer to MUSC's *Risk Management Guidelines* for complete information on the purpose and scope of the *System Identification* documentation. The *Risk Management Guidelines* are published on the Web at http://www.musc.edu/security/guidelines.

The *System Identification* documentation serves to document your System's overall functions, its overall security requirements, its key personnel, its key hardware and software components, its boundaries, its dependencies on other systems, and its interfaces with other systems. This core information about the System itself is a prerequisite to the risk assessment process.

System Administrator: Name and e-mail address of the (lead) system administrator. This should also be recorded in the MUSC System Registry.

System Implementation Project Manager: The name and e-mail address of the project manager for the system's initial implementation, if known.

Functional Description of System: A statement of the System's high-level purpose in relation to MUSC's missions, and a brief list of the System's major functions.

Security Classification of System – Sensitivity: A brief summary of the System's confidentiality requirements.

Security Classification of System – Criticality: A brief summary of the System's availabiltiy requirements.

Purpose of Assessment: The stage in the System's life cycle at which the most recent risk assessment was (or is being) performed. If at the Post-Implementation Stage, also state the specific environmental, operational, regulatory, or policy change(s) that triggered the need for the post-implementation assessment.

Assessment Team Members: Names, e-mail addresses, and roles of the members of the risk assessment team.

MUSC Information Security - System Identification

Compliance Process Step: Document Current System Environment and Personnel

Instructions

System Diagram(s): Attach all relevant diagrams that show key system components, their inter-connections, and their connections to other systems. The diagram(s) should clearly define and demarcate the boundaries of the System.

System Components: Attach a current inventory of the System's key hardware and software components.

System Dependencies: The list of other systems and/or infrastructure components on which this System is known to be dependent for its operation.

System Interfaces: The list of interfaces that exist between this System and other systems.

MUSC Information Security - System Identification

System Name: **Prepared By:**

System Owner: **Date:**

System Administrator:	
System Implementation Project Manager:	
Functional Description of System:	
Security Classification of System – Sensitivity:	
Security Classification of System – Criticality:	
Purpose of Assessment:	
Assessment Team Members:	
System Diagrams:	(attach)
System Components:	(attach)
System Dependencies:	
System Interfaces:	