MUSC Information Security Policy Compliance Checklist for System Owners Instructions

This checklist can be used to identify gaps in compliance with MUSC's information security policies and standards, which are published on the Web at http://www.musc.edu/security.

Each of the 34 Compliance Requirements was derived from a straightforward reading of the 16 MUSC information security policies and their associated performance standards. Each Compliance Requirement is accompanied by some questions that you should ask when scoring your System against that particular requirement. These questions are intended to help you understand the actual compliance requirements.

For each Compliance Requirement, you should score your System's current degree of compliance with respect to that requirement, using the following scale:

0 = not implemented
1 = partially implemented
2 = implemented but not yet documented
3 = implemented and documented
NA = not applicable

You should record a Compliance Score of “NA” if and only if the Compliance Requirement does not apply to your System. The only Compliance Requirements that do not apply to all Systems that house protected informations are the requirements derived from the Workstation Use Policy (lines 11-14). If your System boundaries do not encompass any workstations, then these requirements do not apply to your System. If your System boundaries do encompass any workstations, then these requirements do apply.

We also encourage you to record comments for each Compliance Requirement, in the space provided. Your comments can be invaluable, particularly at later steps in the compliance process, to help other people understand why you scored your System against a particular requirement the way you did... and to help you remember!

For all requirements where a score of 3 is achieved, you should insert a copy of the relevant documentation into the “Current System Procedures and Other Controls” section of your binder, for later review by a compliance officer.

Conversely, a score lower than 3 should help guide you towards corrective action(s) to address that requirement, as you progress through subsequent steps in the compliance process; specifically, each checklist requirement with a score lower than 3 should eventually map to one or more Security Issues in your Risk Analysis Worksheet, and remedial action(s) to address the issue(s) should then be documented in your Security Plan Summary.

You may wish to print out a dated copy of the completed checklist and insert it into the “Assessments, Analysis and Plans” section of your binder. Your compliance officer may ask to review your completed checklist.

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
1	Risk Management	Risk assessments have been performed at appropriate points in the system's life cycle.	Which life cycle stage is your system in? Has a risk assessment for your System that meets MUSC standards been completed in this stage? In any previous stages?		
2	Risk Management	All of the System's risks that have been identified are being appropriately managed.	When the most recent risk assessment for your System was completed, was a security plan for your System developed? Has the security plan been approved? Is the security plan working?		
3	Evaluation	The effectiveness of the System's security measures is being monitored and evaluated.	How do you know that your System's security plan is working? Are your System's security procedures and other security controls being monitored and evaluated? By whom? How, and how often?		

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
4	Workforce Security	The System has procedures for ensuring that no workforce member is granted access to protected information without authorization.	Who authorizes new users to have access to your System? Who authorizes changes in access permissions for existing users? Once authorization is provided, what procedures are followed for adding and changing the actual user accounts in your System?		
5	Workforce Security	The System has procedures for ensuring that workforce members' access is terminated when their authorization is revoked.	How and when is authorization for access to your System revoked? When a user's authorization is revoked, how is the user's access to your System actually terminated?		
6	Awareness and Training	Each authorized user of the System has access to appropriate System-specific training resources and materials.	Do you provide training and documentation to your System's users, explaining their security responsibilities? Do all users have access to this documentation? Are all users aware of these responsibilities?		
7	Incident Response	Emergency contact information for the System has been made available to the CSIRT.	Have you registered your System in the MUSC System Registry, and have all your System's emergency contacts been listed there?		

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
8	Contingency Plan	A contingency plan for the System is maintained, meeting all risk management, business continuity, and regulatory requirements.	Do you have a System contingency plan that meets MUSC standards, including your downtime procedures and communication plan? Who maintains your contingency plan?		
9	Contingency Plan	The System's contingency plan is periodically tested.	Is your System's contingency plan tested? How often? How is it tested, and by whom?		
10	Contingency Plan	The System's contingency plan is revised as needed, in response to environmental, operational, policy and regulatory changes.	Who keeps your System's contingency plan up to date? Is any of the information in it no longer accurate or relevant? When was the plan last revised?		
11	Workstation Security	For any workstations within the System's boundaries, the list of authorized applications is evident to any prospective user of the workstations.	If your System includes any workstations, do the users know what the workstations may (and may not) be used for?		

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
12	Workstation Security	For any workstations within the System's boundaries, the authorized users of the workstation follow appropriate procedures for initiating, terminating and suspending their sessions on the workstations.	If your System includes any workstations, do you have procedures for users to login on the workstations, and are users trained to terminate their sessions appropriately (for example, by logging out)? Is there an inactivity timeout (automatic logout, or password lockout or screen saver) for all user sessions on the workstations?		
13	Workstation Security	Physical access to any workstations within the System's boundaries is restricted to authorized users of the workstations.	If your System includes any workstations, what would prevent an unauthorized user from gaining physical access to one of your workstations?		
14	Workstation Security	Visual access to the displays of any workstations within the System's boundaries is restricted to authorized users of the workstations.	If your System includes any workstations, what would prevent an unauthorized user from viewing information on one of your workstation's displays?		

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
15	Device and Media Controls	Appropriate procedures are used for erasing protected information from the System's media prior to disposal or re-use.	How do you securely erase (wipe) your System's disks and tapes prior to re-use or surplus? For other media such as cd-roms, how do you shred, destroy or otherwise render them unreadable, prior to any disposal of them?		
16	Device and Media Controls	Appropriate procedures are used to maintain the physical security of the System's devices and media during movement and storage.	How do you track the location of equipment containing protected information? If your System includes any mobile devices, how do you protect them from loss or theft? How do you track the movement of backup media? If a tape were lost or stolen, how would you know it, whom would you notify, and what would you be able to tell them about the tape?		
17	Device and Media Controls	Any maintenance contracts or other arrangements, used for servicing the System's devices and media, address the contractor's need to protect the confidentiality of any information that may exist on the devices and media being serviced.	If you have a maintenance contract that calls for a field service engineer to swap out an inoperable disk, how will the confidentiality of any protected information that is still stored on the (old) disk be protected?		

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
18	Access Control	The System has access control procedures to restrict access to the System's protected information to the authorized users of the information.	What are your System's access control procedures? Are they completely effective at preventing unauthorized access to your System?		
19	Access Control	Users of the System are assigned unique identifiers that enable tracking of their access to the System's protected information.	Does each user of your System have his own individual account? Can you track each instance of access to protected information in your System, to the individual responsible for the access?		
20	Access Control	Users of the System are trained in the proper procedures for the management of their passwords and other credentials.	Does your System have documented procedures for user management of their assigned passwords? Are all users trained on these procedures? Are all users aware of these procedures?		
21	Access Control	User sessions that may provide access to protected information are terminated after a reasonable period of inactivity.	Does your System enforce inactivity timeouts (automatic logouts) for all user sessions that provide access to protected information?		

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
22	Access Control	There is a procedure that exists to allow authorized users to obtain access to the System's protected information in an emergency.	In your System's contingency plan, what kinds of emergency scenarios have been considered? Do you have a way to provide access in each of these scenarios?		
23	Access Control	Encryption of the System's protected information, whether at rest or in transit, is used whenever reasonable and appropriate for restricting access to the information.	Do you know if and when your System's protected information should be encrypted? Is protected information being encrypted when it should? If not, why not?		
24	Network Access	System administrators follow applicable MUSC System Security Standards to configure and harden each of the System's networked components.	Does your System include any networked components? Is each component hardened in accordance with MUSC standards?		
25	Audit Controls	Procedures have been established and are being followed to collect and maintain appropriate records of System activity.	Does your System log user sessions, user access to records containing protected information, and other security related events?		
26	Audit Controls	An appropriate retention schedule for System activity records has been established and is being followed.	Do you have a retention schedule for your System's log records? How did you determine that schedule? Is it being followed?		

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
27	Audit Controls	System activity records are being regularly reviewed and analyzed for records of unauthorized activity involving or affecting the System.	Who reviews your System's log records? How are they reviewed, and how often?		
28	Audit Controls	Procedures have been established for making System activity records available for external review as required by MUSC policy.	Do you have a procedure for providing an authorized auditor or compliance officer with access to your System's logs?		
29	Person or Entity Authentication	Appropriate procedures and other controls are being used to authenticate each person or other entity seeking access to the System's protected information.	How do the people who access your System prove that they are who they say they are? If your System has automated interfaces with other systems, how is entity authentication handled within those interfaces?		
30	Data Integrity	Appropriate procedures and other controls are being used to protect the System's data against improper alteration or desctruction during storage, processing, or transmission over a network.	What would prevent the loss or improper alteration of your System's data during storage, processing, or transmission over a network?		

MUSC Information Security Policy Compliance Checklist for System Owners

System Name:

System Owner:

Prepared By:

Date:

	Applicable Policy and/or Standard	Compliance Requirement Derived from the Policy and/or Standard	Some Questions You Should Ask When Scoring Your System	Compliance Score	Comments
31	Encryption	Appropriate procedures and other controls are being used to encrypt the System's data during storage, processing, or transmission over a network.	Refer to #23. If your System does encrypt information, how, when and where is encryption being performed?		
32	Encryption	Appropriate procedures are being used for the management of any keys used for encrypting the System's data.	Refer to #23. If your System does encrypt information, how are you managing and protecting the keys that are used by your encryption processes?		
33	Documentation	All of the System's security management processes are appropriately documented, including risk assessments, risk management decisions and actions, and changes to the System's security procedures and other controls.	Do you have all of the security management documentation required by MUSC policies?		
34	Documentation	All of the System's security documentation is made available as needed to all authorized personnel, is periodically reviewed, is updated when appropriate, and is retained for a minimum of six years.	Do you manage and retain your security documentation in accordance with MUSC policies?		