RIT Information Security

RIT Confidential (when completed)

Web Standard Compliance Checklist

Web server identification and location: ____

Completed by (please print): _____

Signature: _____ Date: _____

Manager's signature: _____ Date: _____ Next scheduled review date: _____

Web Standard Requirement	***Ref.***	**Initials**
General		
1. The web server complies with the server standard.	*(5.1.1)*	
2. Does the server contain RIT Confidential information and general access accounts? **YES** □ **NO** □ If **YES**, complete item **3**. If NO, go to item **4**.	*(5.1.2)*	
3. A documented plan for protecting the RIT Confidential information is located at _____	*(5.1.2)*	
4. No RIT Confidential information is recorded or stored in cookies	*(5.1.3)*	
Vulnerability Scanning		
5. Vulnerability scanning was completed on _____ and will be repeated on _____	*(5.1.4.1)*	
6. Vulnerability scanning follows a documented plan	*(5.1.4.1.1)*	
7. High risk issues have been remediated	*(5.1.4.1.3)*	
Patching		
8. Patch application is documented in the web content services maintenance process	*(5.1.5.1)*	
Minimum Encryption Levels		
9. ~~No less than SSL version 3/~~TLS is used whenever RIT Confidential information is passed	*(5.1.6.1)*	
10. Encryption follows best practices listed on the Information Security web site	*(5.1.6.2)*	
11. Any users accessing web services via SSL version 2 are presented with a statement of risk	*(5.1.6.3.2)*	
Application-level filtering		
12. Server-side applications filter client input on the server following practices listed on the Information Security web site	*(5.1.7)*	
Logging		
13. Web server access logs retain at least 2 weeks of information for all web sites hosted	*(5.2.1)*	
14. Access logs include the source IP address, full URL and timestamp as a minimum.	*(5.2.1.1)*	

Web Standard Requirement	*Ref.*	**Initials**
Access Controls		
Stateless User Authentication		
15. Session IDs are transmitted through SSL and employ appropriate security mechanisms.	*(5.3.1.1)*	
Web Services Administrator Access Control		
16. Configuration file write access is limited to a web services administrative user group.	*(5.3.2.1)*	
17. Web services administrative accounts are used solely for administering web services.	*(5.3.2.2)*	
Local Configuration File Use and Access Control		
18. Access to user modifiable configuration commands (e.g., .htaccess) is limited according to a documented plan.	*(5.3.3.1)*	
19. Appropriate access controls are provided for local configuration files.	*(5.3.3.2)*	
Development and Acquisition		
20. Is this a new product/deployment? **YES** □ **NO** □ If **YES**, complete item **21**. If NO, you are **DONE**.	*(5.4.1)*	
21. Security review completed by on		

After completing this checklist, please keep a copy with your web server documentation and make it available to the RIT Information Security Office on request.

For more information, contact:
RIT Information Security
585-475-4122
infosec@rit.edu
https://www.rit.edu/security/