

Virginia Commonwealth University Technology Services

Security Standard for Web Servers and Applications

Effective Date: August 1, 2007

Compliance Date: May 1, 2008

Revisions:

Version	Date	Revision Issuance
1	June 2007	Initial draft
2	July 2007	Modifications and adjustments
3	January 2008	Modifications and adjustments

Scope:

This standard addresses the security posture of the World Wide Web environment at VCU and focuses on the requirements for the identification, classification and protection of **confidential data** accessed through web applications, the certification of web servers, web application administrators, the hardening of backend database servers and the accumulation of web server logs in a central repository for monitoring and analysis.

Applied Industry Best Practices of:

- SANS Software Security Institute
- Center for Internet Security Consensus Security Benchmarks
- Open Web Application Security Project (OWASP)
- National Institute of Standards Technology (NIST)

Requirements of the Standard

S1.0 - Protection of Confidential Data

S1.1 – Confidential data is prohibited from being stored persistently on Internet-accessible (i.e., public facing) web servers. Confidential data is identified in the **Electronic Confidential Information and Privacy Standard** and the **VCU Data**

Classification Guidelines. Examples of data that would typically be classified as confidential include:

- Protected Health Information
- Education-Student Records
- Financial Records
- Contract Information
- Personnel-Employee Records
- Social Security Numbers
- VCU Card Number
- Personally Identifiable Data
- Application and database IDs (logon credentials)
- Research and Intellectual Information
- Technical Information (including passwords)
- Facility and plant operations security information (floor plans, building control systems and communications systems).
- Investigative and court information

S1.2 - Departments must register each web application that accesses confidential data and is on a public facing (i.e., Internet-accessible) web server. Information about the location of such data will be made available to technical staff that has a need to know as part of their support responsibilities. The registration/inventory system is provided by Technology Services and is restricted to authorized personnel. This inventory can be accessed through the IT Professionals' intranet.

S1.3 – Websites that process confidential information must be authorized by the VCU Chief Information Officer. The form for obtaining this authorization is at the end of this standard. In addition to fulfilling the requirements for public facing web servers listed in this standard, the following are the requirements for websites that process confidential information:

- Encryption technology such as SSL must be used for the login authentication screen and for all access to confidential data.
- Access to these websites requires the use of eID authentication (see S1.4 below)
- Remote administrative access to web servers that process confidential data must be via VPN.

S1.4 – eID username and password authentication must be encrypted whenever used in order to protect these credentials from exposure. SSL should be used when sending authentication credentials.

S2.0 – Web Certification Process

S2.1 - All public facing web servers must be certified using the following certification process:

- A security checklist for the server operating systems and for the web server running on that operating system are provided on the VCU security website (<http://www.ts.vcu.edu/security/checklists.htm>). The checklist must be completed by the system administrator and the web server administrator and signed by both to indicate compliance. The checklists will then be submitted to the Information Security Group and vulnerability scans of the server will be performed to confirm compliance with the security settings.
- Web servers that are public facing will be re-certified on an annual basis.

S2.2 - All web applications that are publically accessible must be certified using the following certification process:

- The web application security checklist is available on the VCU security website (<http://www.ts.vcu.edu/security/sysadmins.html>). The checklist includes industry standard security settings for web applications and requires a statement of business need for those applications that are public facing. The checklist also includes security settings for backend database connectivity used by the web application. The checklist must be completed by the web application technician who is responsible for the application. The signed checklist will then be submitted to the Information Security Group and a web application vulnerability scan will be performed to confirm compliance with the security settings.
- Externally developed web applications that reside on VCU web servers must abide by the web application certification process and will be subject to the same web application vulnerability scans to confirm compliance

S2.3 - Web application administrators must be certified using the certification process described below. Web application administrators are responsible for the security of the web applications and must ensure that web application programmers/developers under their supervision maintain a level of security expertise that includes up-to-date knowledge of web application security and techniques for secure web programming.

- Web application administrators must demonstrate their skill and knowledge of secure web application programming by achieving certification on either the SANS GIAC Web Application Security (GWAS) exam or the SANS Software Security Institute Exam in the specific programming language being used. Information about these certifications is available on the VCU security website. A similar industry standard certification for secure web application programming can be used to satisfy the certification requirement but must be approved by the Information Security Officer.
- Certifications must be kept current, which is critically important due to the changing nature of web technology and security threats.

S2.4 – Web application programmers/developers must keep up-to-date with emerging security threats that affect web applications and must complete annual security awareness training on secure web application development that is provided by Technology Services.

S3.0 – Web Application Databases

S3.1 – The following requirements apply to database servers that interface with web applications:

- Desktop Database Management Systems such as Microsoft Access may not be used for enterprise web applications and may not be used to store confidential information.
- A Database Management System must be housed on a dedicated server and must not reside on a server that has multiple functions such as one that also operates as a file server, web server or domain controller.
- The Center for Internet Security (CIS) Security configuration settings for SQL Server and Oracle should be used as a check on running systems and as a standard when configuring security settings for new systems.
- Enterprise database servers must reside on a protected server virtual network such as SRVNet.
- Web applications that connect to backend database servers must do so with encrypted credentials so that the password for the application account is never visible in any HTTP application code.

S4.0 – Security Logging

S4.1 – Public facing web servers should have logging enabled and should be configured to send pertinent log data to Technology Services' MARS (Technology Services' Monitoring, Analysis and Response System) so that events can be correlated and anomalies detected.

Implementation Guidelines

See VCU security website for information on the inventory system, security checklists and web certifications.

Enforcement

Violation of this standard could result in the removal of a website from the VCU network or in personnel disciplinary actions.

Exceptions

Requests for exceptions to the requirements of this standard should be made to the VCU Chief Information Officer. Please use the Security Standard Request for Exception form that is located on the VCU security website and send the completed form to the VCU Chief Information Officer.

Review Frequency: Annually or as needed

Authority: VCU Chief Information Officer
VCU Information Security Officer

In Compliance with: VCU Academic Policy: Security of Electronic
Confidential Information
COV ITRM Information Technology Security
Management Standard SEC501-01
VCU Computer and Network Resources Use Policy

**Virginia Commonwealth University
Technology Services**

**Request for Authorization
To Process Confidential Data
On an Internet Facing Web Server**

This form is to be used to request authorization to provision a web application that processes confidential data and resides on a web server on the Internet facing portion of the VCU network. The confidential data must not be stored on the web server. See the VCU Web Security Standard for information on the security requirements for public facing web servers.

Please complete all the information below and confirm compliance with each of the security requirements listed by entering a check mark for each requirement. Send the completed form to the Chief Information Officer with a copy to your department head. The request will be reviewed, and you will be notified of approval.

Date of request: _____

Application: _____

Identify Confidential Data Involved:

Contact Information:

Name	
Department	
Email Address	
Phone	

- Web server is registered in the VCU Server Inventory on the IT Professionals Intranet.**
- Web application that processes confidential data is registered in the VCU Applications with Sensitive Information database on the IT Professionals Intranet.**
- Encryption technology such as SSL is used for login authentication screen and for all access to confidential data.**
- eID username and password encrypted authentication is used for access to website that processes confidential data.**
- Remote administrative access to web server that processes confidential data is via VPN.**

Explain any extenuating circumstances:

- Approved**
- Rejected**

Date: _____

Authorized Signature of CIO: _____