March 29, 2010

Standard for Securing Web Technology Resources

Web technology resources have allowed the university community to become more productive and collaborative while allowing for more flexibility and decentralization. At the same time, cyber threats on Web technology resources now outnumber operating system threats.

The purpose of this standard is to establish the minimum security requirements for *Web technologies* at Virginia Tech that transmits or stores *university information*. University information stored in a digital or electronic format requires additional steps to ensure the protection of the information from loss, corruption, or inappropriate disclosure.

Terms in *italics* are defined under Definitions on page 4.

Scope of the Standard

This standard applies to any Web technology resource or service that:

- Is owned or managed by the university;
- Is connected to the university network;
- Connects to another university technology resource or service;
- Stores or transmits university information.

This standard applies whether the network connections are remote or campus-based. Special emphasis must be given to *covered data* as defined by the Standard for Storing and Transmitting Personally Identifying Information.

Standard

Departments and individual users must take appropriate actions to minimize security vulnerabilities that may exist on departmental and individual Web technology resources covered by this standard. The actions taken include the Web technology resource minimum requirements for the following:

1. Configuration

The Open Web Application Security Project (OWASP) identifies ten vulnerabilities in the "OWASP Top Ten Project." *Web applications*, *web servers*, and *web services* must be configured, protected, and maintained to address the vulnerabilities listed in the "OWASP Top Ten Project." Only those web services or applications specifically needed should be enabled. Web services, applications, and sample or default content must be disabled if not needed.

Web servers and web applications should not run with elevated privileges (e.g. "root" or "Administrator") and should remain segmented from the system processes when possible. Web based applications and services must provide auditable logs.

Web servers must be configured to adhere to Virginia Tech Policy 7025: Safeguarding Nonpublic Customer Information and Virginia Tech Policy 7010: Policy for Securing Technology Resources and Services.

For *third-party* Web technology resources:

- Software must be installed and configured in accordance with security recommendations such as the vendor's website, National Institute for Standards and Technology, Center for Internet Security, or OWASP.
- Default configurations must be reviewed for applicability to the Virginia Tech environment by the IT Security Office or an approved designated body.
- Default administrative passwords must be changed.

2. Maintenance, Updates, and Security Patching

Web server software, web applications, additional software modules, and application software must be kept up to date in accordance with security advisories and patches must be applied as promptly as possible. Web technology resources developed by vendors or third-party developers unresponsive to patching security vulnerabilities must be replaced with a secure alternative or additional controls designed to mitigate the security vulnerabilities must be implemented.

An auditable process must be used to allow developers to install new content or update existing content.

3. Specialized Content

Web technology resources that deal with special content must ensure that the security practices for those resources comply with special rules. These include the following:

Electronic protected health information

Any university unit covered by the Health Insurance Portability and Accountability Act (HIPAA) must ensure that the security of Web technology resources complies with HIPPA. The National Institute of Standards and Technology (NIST), published its "Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" (SP 800-66 REV 1), and, in conjunction with the United States Department of Health and Human Services, provides information to facilitate compliance.

Nonpublic customer financial information

University offices with responsibilities for nonpublic customer financial information must comply with university policy 7025, "Safeguarding Nonpublic Customer Information," a policy related to the Gramm-Leach-Bliley Act. Web technology resources that involve credit card transactions must comply with the Payment Card Industry Data Security Standard.

Personally identifiable information

In accordance with the Standard for Storing and Transmitting Personally Identifying Information, the covered data elements must be encrypted when stored or transmitted over the network.

Collection and handling of data during research activities

Virginia Tech's Institutional Research Board sets forth additional policies and procedures that govern university information collected during research activities. Web technology resources that collect or handle data on human subjects must comply with the Policy for Online Research Data Collection Activities and the Storage of Electronic Data Involving Human Subjects and Policy for the Storage and Transfer of Human Subjects Research Records.

References

- Policy for Securing Technology Resources and Services - http://www.policies.vt.edu/7010.pdf
- Safeguarding Nonpublic Customer Information- http://www.policies.vt.edu/7025.pdf
- Policy for Protecting University Information in Digital Form - http://www.policies.vt.edu/7105.pdf
- Administrative Data Management and Access Policy - http://www.policies.vt.edu/7100.pdf
- Standard for Protecting Sensitive University Information in Digital Form - http://www.it.vt.edu/publications/pdf/2_SensitiveDataStandardRevision1-signed.pdf
- Standard for Storing and Transmitting Personally Indentifying Information - http://www.it.vt.edu/publications/pdf/3_PIIStandardFinal13June-signed.pdf
- OWASP Top 10 Project -- http://www.owasp.org/index.php/OWASP_Top_Ten_Project
- Summary of HIPPA Privacy Rule- http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
- Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 REV 1). http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- Payment Card Industry Data Security Standard- www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Virginia Tech Institutional Research Board Policies and Procedures - http://www.irb.vt.edu/pages/policies.htm
- Research Policy for Online Research Data Collection Activities and the Storage of Electronic Data Involving Human Subjects- http://www.irb.vt.edu/documents/onlinepolicy.pdf
- Policy for the Storage and Transfer of Human Subjects Research Records -
- http://www.irb.vt.edu/documents/data_retention_transfer_policy.pdf
- Information Technology Security web site – http://security.vt.edu
- Virginia Tech computing resource site -- http://www.computing.vt.edu/

Definitions

University information includes information collected by or used by university personnel in the conduct of their university responsibilities. It includes information collected and used for learning, discovery, engagement, support, and administration. University information in digital form may exist in a variety of formats, ranging from highly structured elements in a database to unstructured, narrative information. University information includes information within the control of university personnel in the conduct of their job responsibilities, whether the information resides in university-owned digital systems or elsewhere. Further, university information may be gathered or used at the direction of the university but residing in applications hosted by vendors or other third parties.

Sensitive university information includes all university information that could cause physical, financial, or reputational harm to the university or to members of the university community if released inappropriately. Under Policy 7100, data classified as university-internal or as limited-access may be sensitive information.

Covered data as defined refers to six covered data elements—those university nonpublic data elements specified in this standard (Social Security number, credit card number, debit card number, bank account number, driver's license number, or passport number)—and the covered combination, the occurrence of name and date of birth carried together in a document.

Web technology or Web technology resource includes but is not limited to any web application or device used in the hosting, storage, or transmission of any Virginia Tech or affiliated information. Web technology resources include web applications, web services, and web servers.

Web applications refer to any application that has an interface accessible through a Web browser.

Web services refer to software programming interface that can be accessed over a network. A web application typically communicates with a web service.

Web servers refer to software, hardware, or a combination of both that is intended to serve content to an Internet browser using the Hypertext Transfer Protocol (HTTP) or Hypertext Protocol Transfer Secure (HTTPS), including but not limited to: Apache HTTP Server, Microsoft IIS.

Web-based service is a combination of web software technologies – web application, web service, web server – that collectively provide a service to the end user.

Third party systems as defined refer to hosted systems and vendor-provided services running on servers external to Virginia Tech, regardless of whether the system is purchased, leased, or donated. The definition does NOT include partners that receive transmissions of university data under requirements of law or regulation (for example, the Internal Review Service or the State Council of Higher Education for Virginia).

March 29, 2010

Approval

Approved, Vice President for Information Technology and Chief Information Officer, Earving L. Blythe

(Signed) Earving L Blythe

Digitally signed by Earving L Blythe
DN: dc=edu, dc=vt, c=US, o=Virginia Polytechnic Institute and State University, cn=Earving L Blythe, 0.9.2342.19200300.100.1.1=809628, serialNumber=571
Date: 2010.03.29 14:24:27 -04'00'

Date _____