HHS Information Security

PUBLIC

Web & Mobile Standard

Version (v) 2.01

TEXAS
Health and Human Services

Published

September 1, 2017

PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Publication Information

Authorized By:	HHS Chief Information Security Officer (CISO) Shirley Erp
Supersedes:	HHS Enterprise Information Security Web (EIS-Web) Minimum Security Requirements

Publication Version History

Numbering convention: Version. Revision as n.xx. Pre-publication drafts are 0.xx; first published version is 1.00; for minor revisions to a published document, increment the decimal number (ex. 1.01); for major content upgrades to a published document, increment the leading whole number (ex.2.00).

Revision	Date	Change Description
1.0	April 7, 2017	First published version of HHS Information Security Web Minimum Security Requirements.
2.0	August 8, 2017	Added new Texas Government Code (TGC) 2054.5516, Data Security Plan for Online and Mobile Application Requirements. This required updating the publication format, adding mobile application requirements, and adding additional information to the "Additional Resources" section.
2.01	September 1, 2017	Transferred publication to new standards template and added references to applicable information security controls.

Publication Review History

To satisfy the requirements of the Information Systems Security Program, a formal review of this document was conducted in accordance with HHS requirements on the following dates:

Revision	Date	Reviewer	Review Comments
1.0	April 7, 2017	Shirley Erp, Chief Information Security Officer	Authorized publication of v1.0
2.0	August 8, 2017	Shirley Erp, Chief Information Security Officer	Authorized publication of v2.0 for TGC 2054.516 compliance with verbal approval from CIO that document would go through formal governance process after initial publishing.
2.01	September 1, 2017	Shirley Erp, Chief Information Security Officer	

1. Introduction

1.1. Purpose

Websites, web applications, and mobile applications must comply with all state and federal requirements. Online applications should also comply with best practices for minimizing vulnerabilities and weaknesses. A risk-based approach should be used in implementing the requirements and best practices.

1.2. Background

The Texas Administrative Code (TAC) 202 mandated Department of Information Resources (DIR) Security Control Standards Catalog is a legislative mandate that defines requirements which must be implemented. Websites should be developed so they utilize the specified controls and existing sites that are not compliant should be remediated to address any shortcomings.

The Texas 85R House Bill (HB) 8, effective as of September 1st 2017, added a new section to Texas Government Code (TGC) Section 2054.516 that is relevant to Internet facing websites and mobile applications. The requirement includes both HHS internally maintained systems and HHS contracted systems. Contractors must be accountable for compliance of this requirement as a part of their contract deliverables.

> TGC Sec. 2054.516, Data Security Plan for Online and Mobile Applications:
>
> Each state agency, other than an institution of higher education subject to Section 2054.517, implementing an Internet website or mobile application that processes any sensitive personal information or confidential information must:
>
> 1. Submit a biennial data security plan to the department not later than October 15 of each even-numbered year to establish planned beta testing for the website or application; and
> 2. Subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

1.3. Scope

All information systems (whether HHS or contractor) that access, create, disclose, receive, transmit, maintain, or store HHS data via a website or mobile application.

1.4. Target Audience

The IS-Web & Mobile Standard is intended to serve a diverse audience of information systems, Information Owners, Information Custodians and Information Security staff. While all users of HHS information systems assets should be aware of security controls required by HHS Information Security, primary users of this document are the information system custodians of IT operations, system and database administrators, application developers, support, maintenance personnel, and Information Security Officers.

1.5. Alignment

The HHS Information Security Program makes extensive use of the information security guidance found in the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, Revision 4 (rev 4) and is based on the NIST SP 800-53 rev 4 suite of controls. The IS-Web & Mobile Standards also aligns with the requirements TAC 202 and TGC 2054.516.

1.6. Definitions

The terms used in the IS-Web and Mobile Standards are defined in Appendix B and the HHS Information Security (IS)-Definitions document which can be found on the HHS IS Security Website page.

2. Standards

The following list is based on SANS web application security best practices and represents a set of minimum standards for a web or mobile application. These standards are in addition to the information security controls required for the information system per the appropriate security baseline defined in HHS Information Security Standards and Guidelines (ISSG) Security Controls. Web or mobile applications hosting confidential information may have additional requirements depending on the data types and impact to the organization.

Application(s) managed by Contractors that access, create, disclose, receive, transmit, maintain, or store HHS Confidential Information additionally require a Data Use Agreement (DUA) and Information Security and Privacy Initial Inquiry (SPI).

If further security concerns are identified, then a full risk assessment and a validated system security plan may be requested to ensure compliance and that HHS data is protected appropriately.

Please contact infosecurity@hhsc.state.tx.us for further questions or assistance. Hyperlinks to Common Weakness Enumeration (CWE) documents have been added to provide supplemental information where relevant.

2.1. Validate User Input

<table>
<tr><th colspan="2">Security Standard(s):</th></tr>
<tr><td colspan="2">Std.1 - User input form fields need to be tested for malicious commands (e.g. SQL injection).
Std.2 - Ensure user data is in the proper format before being accepted by the application.
Std.3 - SQL queries should be crafted with user content passed into a bind variable and should avoid creation by dynamic string concatenation.</td></tr>
<tr><th>Supplemental Information:</th><th>IS Control(s):</th></tr>
<tr><td>CWE-159, Failure to Sanitize Special Element
CWE-144, Improper Neutralization of Line Delimiters</td><td>SI-10, <i>Information Input Validation</i></td></tr>
</table>

CWE-89, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	

2.2. Display Generic Error Messages

Security Standard(s):	
Std.1 - Error messages should not reveal details about the internal functionality of the application. Std.2 - Turn-off debugging on production webservers.	
Supplemental Information:	**IS Control(s):**
CWE-209, Information Exposure Through an Error Message	SI-11, *Error Handling*

2.3. Store User Password Using a Strong, Salted Hash

Security Standard(s):	
Std.1 - User passwords must be stored using secure hashing techniques with strong algorithms (e.g. PBKDF2, bcrypt, scrypt). Std.2 - FIPS and NIST Special Publications specify a number of approved cryptographic algorithms.	
Supplemental Information:	**IS Control(s):**
CWE-257, Storing Passwords in a Recoverable Format	IA-05(01), *Password-Based Authentication*

2.4. Don't Hardcode Credentials

Security Standard(s):	
Std.1 - Never allow credentials to be embedded directly within the application code. While it can be convenient to test application code with hardcoded credentials during development this significantly increases risk and should be avoided.	
Supplemental Information:	**IS Control(s):**

CWE-798, Use of Hard-coded Credentials	IA-05(07), *No Embedded Unencrypted Static Authenticators*

2.5. Use HTTPS Everywhere

Security Standard(s):	
Std.1 - Ideally, HTTPS should be used for your entire application. Std.2 - If you have to limit where it's used, then HTTPS must be applied to any authentication pages as well as to all pages after the user is authenticated. Std.3 - If sensitive information (e.g. personal information) can be submitted before authentication, those features must also be sent over HTTPS.	
Supplemental Information:	**IS Control(s):**
CWE-311, Missing Encryption of Sensitive Data CWE-319, Cleartext Transmission of Sensitive Data CWE-523, Unprotected Transport of Credentials	SC-08, *Transmission Confidentiality and Integrity*

2.6. Utilize a Strong SSL Configuration on Servers

Security Standard(s):	
Std.1 - Weak ciphers must be disabled on all servers. For example, SSL v2, SSL v3, and TLS protocols prior to 1.2 have known weaknesses and are not considered secure. Std.2 - Disable the NULL, RC4, DES, and MD5 cipher suites. Std.3 - Ensure all key lengths are greater than 128 bits, use secure renegotiation, and disable compression.	
Supplemental Information:	**IS Control(s):**
Qualys SSL Labs offers free SSL Configuration testing: https://www.ssllabs.com/	SC-08, *Transmission Confidentiality and Integrity*

2.7. Only use Certificates from a Trusted Certificate Authority

Security Standard(s):	
Std.1 - HTTPS certificates should be signed by a reputable certificate authority (e.g. Entrust, Verisign, or an Active Directory CA server), avoid using self-signed certificates. Std.2 - The name on the certificate should match the fully qualified domain name (FQDN) of the website.	
Supplemental Information:	**IS Control(s):**
	SC-12, *Cryptographic Key Establishment and Management*

2.8. Store Database Credentials Securely

Security Standard(s):	
Std.1 - Embedding database credentials within source code is not acceptable. Std.2 - Connection strings containing database credentials which are stored in configuration files should be encrypted (e.g. use aspnet_regiis tool to encrypt IIS web.config files).	
Supplemental Information:	**IS Control(s):**
CWE-257, Storing Passwords in a Recoverable Format CWE-798, Use of Hard-coded Credentials	IA-05(07), *No Embedded Unencrypted Static Authenticators* SC(28), *Protection of Information at Rest*

2.9. Limit the Use of Storage of Sensitive Data

Security Standard(s):	
Std.1 - Conduct an evaluation to ensure that sensitive data is not being unnecessarily transported or stored.	
Supplemental Information:	**IS Control(s):**
	CA-02, *Security Assessments*

2.10. Implement a Strong Password Policy

Security Standard(s):	
Std.1 - A password policy should be created and implemented so that passwords meet specific strength criteria.	
Supplemental Information:	**IS Control(s):**
CWE-521, Weak Password Requirements Refer to the Identification and Authentication section of the HHS Information Security Standards and Guidelines (ISSG) for HHS password management standards.	IA-05(01), *Password-Based Authentication*

2.11. Ensure Sessions have Appropriate Expiration Controls

Security Standard(s):	
Std.1 - Avoid non-expiring session cookies and set a reasonable expiration time for idle sessions. This will help protect user sessions from misuse if the cookie is captured. Std.2 - New sessions should be generated each time a user is authenticated. Std.3 - Sessions should be destroyed when a user logs out.	
Supplemental Information:	**IS Control(s):**
CWE-613, Insufficient Session Expiration	AC-12, *Session Termination*

2.12. Perform Regular Code Reviews and Security Testing

<table>
<tr><th colspan="2">Security Standard(s):</th></tr>
<tr><td colspan="2">Std.1 - Regularly review code looking for common issues like SQL Injection and Cross-Site Scripting.
Std.2 - Conduct security testing both during and after development to ensure the application meets security standards.
Std. 3 - Systems with Internet accessible website and mobile applications that process any sensitive personal information or confidential information must subject the website or mobile application to a vulnerability test and penetration test and address any vulnerabilities identified in the test.</td></tr>
<tr><th>Supplemental Information:</th><th>IS Control(s):</th></tr>
<tr><td>CWE-702, Weaknesses Introduced During Implementation</td><td>SA-11, <i>Developer Security Testing and Evaluation</i>
SA-11(01), <i>Static Code Analysis</i>
SA-11(02), <i>Threat and Vulnerability Analysis</i>
SA-11(05), <i>Penetration Testing</i>
SA-11(08), <i>Dynamic Code Analysis</i>
CA-08, <i>Penetration Testing</i></td></tr>
</table>

2.13. Apply the Principle of Least Privilege (Where Applicable)

Security Standard(s):	
Std.1 - Rights must be specifically added to an account to grant access to resources. Std.2 - If rights are not explicitly necessary, then access should be denied.	
Supplemental Information:	**IS Control(s):**
CWE-272, Least Privilege Violation CWE-250, Execution of Unnecessary Privileges	AC-06, *Least Privilege*

2.14. Validate the Security of External Resources

Security Standard(s):	
Std.1 - Third Party code libraries should be reviewed for bugs and security vulnerabilities before being included into a web application. Std.2 - External web based services used in the web application should be evaluated for security before use (e.g. Geolocation, Calendar, or Email services).	
Supplemental Information:	**IS Control(s):**
	SA-11, *Developer Security Testing and Evaluation*

3. Additional Resources

3.1. SANS - Securing Web Application Technologies [SWAT] Checklist

The SWAT Checklist provides an easy to reference set of best practices that raise awareness and help development teams create more secure applications. It's a first step toward building a base of security knowledge around web application security. Use this checklist to identify the minimum standard that is required to neutralize vulnerabilities in your critical applications.

https://software-security.sans.org/resources/swat

3.2. Open Web Application Security Project (OWASP)

OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted…. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas.

https://www.owasp.org

Appendix A. References

- **Texas Government Code 2054**, *Information Resources*, http://www.statutes.legis.state.tx.us/SOTWDocs/GV/htm/GV.2054.htm
- **Texas Administrative Code 202,** *Information Security Standards, https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202*
- **State of Texas 85th Legislative Session HB8,** *Relating to cybersecurity for state agency information resources*, effective September 1, 2017, https://legiscan.com/TX/text/HB8/id/1625019
- **Texas HHS Data Use Agreement (DUA),** https://hhs.texas.gov/sites/default/files//documents/doing-business-with-hhs/providers/long-term-care/nf/data-use-agreement.pdf
- **Texas HHS Information Security and Privacy Initial Inquiry (SPI),** https://hhs.texas.gov/sites/default/files//documents/doing-business-with-hhs/contracting/HHS_SPI.pdf
- **Texas HHS Data Classification Standard**
- **Texas HHS Information Security Standards and Guidelines (ISSG) Security Controls Catalog**

Appendix B. Terms and Definitions

Confidential Information: means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to CONTRACTOR or that CONTRACTOR may create, receive, maintain, use, disclose or have access to on behalf of HHS that consists of or includes any or all of the following:

(1) Client Information;

(2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information;

(3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;

(4) Federal Tax Information;

(5) Personally Identifiable Information;

(6) Social Security Administration Data, including, without limitation, Medicaid information;

(7) All privileged work product;

(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552

Sensitive Personal Information: A category of personal identity information as defined by §521.002(a)(2), Texas Business and Commerce Code.

(2) "Sensitive personal information" means, subject to Subsection (b):

(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) social security number;

(ii) driver's license number or government-issued identification number; or

(iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(B) information that identifies an individual and relates to:

(i) the physical or mental health or condition of the individual;

(ii) the provision of health care to the individual; or

(iii) payment for the provision of health care to the individual.