Iowa Department of Administrative Services

Government's Partner in Achieving Results

DAS

Chester J. Culver, Governor
Patty Judge, Lt. Governor

Ray Walton, Director

State of Iowa Enterprise Web Application Security Standard

June 7, 2010

Purpose

This document provides the minimum security requirements for web applications developed, owned or managed by State agencies.

Overview

State agencies use web applications to offer services, collect and disseminate information. Cyber criminals increasingly target web applications to steal confidential data and spread malware. State agencies shall ensure that their web applications meet a minimum set of security requirements.

Scope

For the purpose of this standard, security is defined as the ability to protect the confidentiality, integrity, and availability of information processed, stored and transmitted by agencies via web applications. Information technology assets covered by this policy include those that process, store, transmit or monitor digital information.

This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level policies, standards, guidelines, processes and procedures.

Definitions

Selected terms used in the Enterprise Web Application Security Standard are defined below:

- **Application:** A computer program or set of programs that meet a defined set of business needs.
- **Availability**: Ensuring timely and reliable access to and use of information.
- **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Development:** Environment for incomplete versions of an application; initial deployment for testing; and informal testing by the project team.
- **Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Production**: Environment for final deployment of applications for usage by intended audience.
- **Test:** Environment for preparation for production deployment. Formal testing including functionality; performance; scalability; user acceptance and security is performed.
- **Web application**: An external application that is accessed via a web browser over the Internet.

Elements

The following are the elements of the Enterprise Web Application Security Standard.

1. **Social Security Numbers**:
   a. Social Security numbers shall not be used as a User Id or password during logon for web applications.
   b. Social Security numbers shall not be displayed in full on web applications beyond the initial data entry screen

2. **Development:** Agencies engaged in application development must implement separate development, test, and production environments for the applications they develop. Agencies involved in application hosting must implement separate test and production environments.
   a. Agencies must remove test data and accounts from production systems before these systems become live.

3. **Production Data:** Use of confidential data in test environments requires agency management approval.
   a. Test environments using confidential data shall meet standards equivalent to the production system.

4. **Coding Vulnerabilities:** Agencies shall develop web applications based on secure coding guidelines and eliminate common coding vulnerabilities. At a minimum agencies must meet the current Open Web Application Security Project (OWASP) guidelines http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project to prevent:
   a. Injection (SQL, LDAP, etc.)
   b. Cross-Site Scripting (XSS)
   c. Broken Authentication and Session Management
   d. Insecure Direct Object References
   e. Cross Site Request Forgery
   f. Security Misconfiguration
   g. Failure to Restrict URL Access
   h. Unvalidated Redirects and Forwards
   i. Insecure Cryptographic Storage
   j. Insufficient Transport Layer Protection

5. **Application Testing**: Agencies shall review and test web applications for security vulnerabilities using an automated web application scanning tool. Application review shall include source code and run time analysis.
   a. Web applications shall be scanned using all application roles (ex. user and admin).
   b. New web applications must be scanned before going to production.
   c. Existing web applications must be scanned annually and whenever significant changes are made to the application.
   d. Critical/high vulnerabilities identified by the web application scans shall be remediated.
   e. The web application review must be conducted by someone other than the developer.
   f. The Information Security Office shall maintain a list of criteria for approved web application scanning tools.

6. **Change Management**: Agencies shall implement a change management procedure for deployment of agency web applications. Separation of duties shall be implemented to prevent developers from publishing their own applications to the production environment.

7. **Encryption**: Web applications collecting or displaying confidential data must encrypt the data in transit.
    a. Data in transit shall be protected with SSL 3.1/TLS 1.0, equivalent or higher method of encryption.

8. **Log-on Banner**: Web applications which require a log-on shall have a log-on banner. The banner shall be approved by the agency's legal counsel and notify users that:
    a. Users are entering a State of Iowa system
    b. Access is limited to authorized use only
    c. Users consent to monitoring

9. **Access Control**: User authentication is required for all web applications that collect, transmit, display or store confidential data or where the integrity of the data must be maintained. Required access controls include:
    a. User ID: Each user must have a unique user ID.
    b. Access Review: User group roles and rights must be reviewed at least quarterly.
    c. Passwords:
        i. At least eight characters
        ii. A mixture of numbers, upper alphabetic and lower case letters
        iii. Include at least 1 special character
        iv. Changed at least every sixty days
        v. Passwords shall not be transmitted in clear text
    d. Log Off: Applications shall log off users after 20 minutes of inactivity.
    e. Failed Log-In:
        i. Accounts are locked after five failed login attempts within 60 minutes.
        ii. Users shall remained locked out for 24 hrs or until the account is reset by an administrator.
        iii. A message will display directing the user who to contact when this event occurs.

10. **Logs**: Web application logs must be collected and reviewed for security events. These logs must meet agency data retention requirements. Minimum security events to be logged include:
    a. Startup and shutdown
    b. Authentication
    c. Authorization/permission granting
    d. Process invocation
    e. Unsuccessful logins
    f. Unsuccessful data access attempt
    g. Data deletions
    h. Data transfers
    i. Application configuration change

11. **Application Firewall**: An application firewall shall be installed in front of all external web facing applications.

12. **Source Code**: Access to web application source code shall be restricted to authorized employees.

13. **Database**: Backend databases shall not be hosted on the same physical server as web applications in production.

14. **Training**: Web application developers must receive technical training annually in secure coding techniques.

15. **Service Providers**: Agency web applications developed\hosted by an Applications Service Provider or other third party must comply with the Enterprise Web Application Security Standard http://das.ite.iowa.gov/standards/enterprise_it/index.html.

16. **Inventory**: Agencies must provide the Information Security Office with a list of all web applications collecting confidential information.
    a. Application Name
    b. URL
    c. Application owner

17. **Security Audits**: The Information Security Office shall conduct periodic security reviews of a sample of state web applications.

Updates
This document will be reviewed at least every two years and updated as needed.

Effective Date This standard shall be effective September 30, 2010 for all new web applications and December 31, 2011 for all existing web applications.

Enforcement This standard shall be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation.