Web Based Application Standards

Enterprise

Bryan Shannon

Contents

Web Application Security Standard

Purpose

This document provides the minimum-security requirements for web applications developed, owned, and managed by Early Learning Ventures (ELV).

Overview

ELV use web applications to offer services, collect and disseminate information. Cyber criminals increasingly target web applications to steal confidential data and spread malware. ELV 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 ELV 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 ELV applications.

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 quality assurance team.
- **Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation (provides proof of data origin/integrity) 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**: Development team must implement separate development, test, and production environments for the applications they develop. Application hosts must implement separate test and production environments.
    a. Remove test data and accounts from production systems before these systems become live.
3. **Production Data**: Use of confidential data in test environments requires ELV management approval.
    a. Test environments using confidential data shall meet standards equivalent to the production system.
4. **Coding Vulnerabilities**: ELV 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**: ELV 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 if development team size allows.

6. **Change Management**: ELV shall implement a change management procedure for deployment of web applications. Separation of duties shall be implemented to prevent developers from publishing their own applications to the production environment if development team size allows.

7. **Encryption**: Web applications collecting or displaying confidential data must encrypt the data in transit. a. Data in transit (database-application-browser and vice-versa) shall be protected with SSL 3.1/TLS 1.0, equivalent or higher method of encryption.

8. **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 annually.

    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 35 minutes of inactivity.

    e. Failed Log-In:

        i. Accounts are locked after five failed login attempts without a successful login.

        ii. User accounts shall remain locked out for 1 hour or until the account is reset by an administrator.

        iii. A message will display directing the user who to contact when this event occurs.

9. **Logs**: Web application logs must be collected and reviewed for security events. These logs must meet 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 (when possible)
10. **Application Firewall**: An application firewall shall be installed in front of all external web facing applications.
11. **Source Code**: Access to web application source code shall be restricted to authorized employees.
12. **Database**: Backend databases shall not be hosted on the same physical server as web applications in production.
13. **Training**: Web application developers must receive technical training bi-annually in secure coding techniques.
14. **Inventory**: Provide the Information Security Office (or COO) with a list of all web applications collecting confidential information.
    a. Application Name
    b. URL
    c. Application owner
15. **Security Audits**: The Information Security Office (or COO) shall conduct periodic security reviews of a sample of supported web applications.

Updates

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

Effective Date

This standard shall be effective January 1, 2022 for all new web applications and Jan 1, 2023 for all existing web applications.

Note on Static Code Analysis (used in ELV Development)

PMD is a static source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth. It's mainly concerned with Java and Apex, but supports 12 other languages**.**

Authentication Security Standard

Overview

This Standard establishes the minimum requirements relating to Authentication for Information Technology systems and applications.

Purpose

ELV maintains a variety of data and information in its IT systems, including but not limited to confidential information, personally identifiable information, and other sensitive or regulated information. In order to protect this data, information, and systems, it is necessary to adequately Authenticate individuals prior to granting them access to such systems and applications. This ensures such individuals are the true individuals who are authorized to access ELV systems and applications and the data and information stored, processed, and accessed by and through the same.

Scope/Application

This Standard applies to all ELV web-based applications. This Standard shall be deemed to have been adopted by all web-based applications, Governance Documents augmenting but not diminishing this Standard may be adopted. In the event of any conflict or inconsistency between this Standard and any other Governance Document, this Standard shall prevail.

Definitions

In addition to any other terms specifically defined elsewhere in this Standard, select terms used in this Standard are defined as follows:

- **Administrator Account(s)** means an account with full\elevated privileges on a computer\device, system, or application.
- **Authentication** means the process of establishing confidence in the identity of users of information systems through one of the following methods:
    - Something the user knows (e.g., password);
    - Something the user has (e.g., phone); or
    - Something the user is (e.g., fingerprint).
      Collectively referred to as “Methods.”
- **Digital Certificate(s)** means a software token containing the user’s private key organization’s security controls. Any exchange across the internet is considered remote.
- **Multi-factor Authentication** means Authentication using two, or more, Methods. E.g., Google two-factor Authentication.
- **Remote** means an information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single

organization's security controls. Any exchange across the internet is considered remote.

- **System Account(s)** means an account that allows the direct connection of two or more IT systems or applications for the purpose of sharing data and other information resources.
- **User Account(s)** means an account with limited privileges to a computer\device, system, or application.

Sharing/Display

- User Accounts shall be assigned to a single individual, not a group or entity.
- Authentication information, including but not limited to passwords, shall not be shared with other Personnel (including but not limited to co-workers, managers, or help desk staff), Personnel, or any other third parties.
- Authentication information, including but not limited to Passwords, for User Accounts shall not be openly displayed, and systems and applications shall be configured to mask passwords during entry.

User Names/Passwords

- Default administrative and initial passwords for all computers/devices, systems, and applications shall be temporary, and must be changed during initial setup/use.
- Social security numbers or other similar identification numbers shall not be used as a user ID or password.
- Passwords shall be:
    - At least eight (8) characters for User Accounts (except for mobile devices, see Enterprise Mobile Device Security Standard).
    - At least ten (10) characters for accounts with elevated privileges, such as Administrator Accounts or System Accounts.
    - Comprised of a mixture of numbers, upper and lower-case letters, with at least one special character.
- Passwords shall NOT be:
    - Comprised of a single instance of a dictionary word. Concatenating multiple dictionary words (recommended three (3) or more), is acceptable.
    - Comprised of or include, in whole or in part, a user’s name or username/login.

- The same as any password used by the user on any personal systems/applications (e.g., banking, shopping, social networking – recommended but cannot be enforced).
- Displayed when entered.

- *Password Changes.*
  - **Password Changes:** Passwords must be changed whenever the user possesses a reasonable belief their password may have been compromised.
    For example, if:
    - The user, in either the employment context or in their personal life, has recently been the subject of a phishing attack or other cyber event;
    - The user has lost a device, whether ELV-issued or personal, on which their password was or other similar passwords were stored, or that contained information that could otherwise be used to discern a password;
    - The password has been or reasonably may have been stolen.
  - System & Administrator Accounts. Passwords for System and administrator Accounts should be changed at least every ninety (90) days.
  - Reuse. If/when any password is changed, any new password must be substantially different from the previous six (6) passwords used in connection with that account.

NOTE

ELV has elected to not adhere to all of these standards, specifically, administrative account passwords need only be 8 in length (not 10), passwords must be changed every 365 days (not 90), new passwords must be different than the previous (1) password (not 6).

Multi-factor Authentication

- Multi-factor Authentication shall be used for Remote network connections (e.g., VPN or remote desktop), and Remote administrator tasks.
- Multi-factor Authentication shall be used for all cloud-based email accounts as it relates to all users with a ELV-issued cell phone.
- Multi-factor Authentication shall include a user ID and password\PIN plus one or more of the following:
  - Digital Certificate;
  - Token\Smart card;

- Biometrics; or
- One-time authorization code (e.g., pre-printed codes, codes sent via text message, Google 2-step, email or phone call).

Encryption

Passwords and password recovery information shall be encrypted at rest and in transit both inside and outside of ELV.

Unsuccessful Login Attempts

User Accounts and Administrator Accounts shall be set to lock after five (5) consecutive unsuccessful login attempts. Such Accounts shall remain locked until they are reset by an individual authorized to do so through an Administrator Account.

NOTE

ELV has modified this requirement, the account is locked after five (5) consecutive unsuccessful login attempts, but become unlocked after an hour for the user to attempt to login.

Account Reset/Recovery

Before an administrator may reset/recover an account/password on behalf of a user or other administrator, the user or administrator for whom account recovery/reset is sought shall be verified as the individual who is authorized to access/use such account.

- Account administrators shall NOT request the following as verification information:
  - Social security number.
  - Employee ID number.
  - Mother's maiden name or answers to personal questions, such as "what was your first car?", which answers can be easily found via social media or social engineering.
- Account administrators may request and confirm the following or deploy the following methods as verification of a user's identity. Account administrators must utilize at least two (2) verification methods, including, by way of example only:
  - Request the user send a text message from a ELV-issued cell phone provisioned to that specific user;
  - Request the user place a call from a ELV-issued phone provisioned to that specific user;
  - Request the user send an email from a ELV-issued email account provisioned to that specific user;

- Request the user have his or her supervisor/manager do any of the foregoing and through such communication confirm the identity of the user initiating the request;
- Request the user provide an answer to a lookup secret (something a user has) previously distributed to the user. (NOT IMPLEMENTED)

Training

ELV Personnel, including but not limited to directors, officer, employees, interns, and board and commission members, and Vendor Personnel shall receive security awareness training covering passwords, social engineering\phishing, malware threats and reporting incidents.

Storage

- Smart cards, and tokens shall not be stored with the corresponding computer\mobile device to which they unlock/permit access.
- Tokens\smart cards shall be secured when not in use
- Except for hard copy emergency Administrator Account Authentication Information, which information shall be stored in a locked/secured area and restricted to authorized individuals, Authentication information shall not be written down.
- Users shall not use the “remember password” feature, or other similar feature, in any web browser or other system or application.
- Users shall not use any “password keeper,” “password wallet,” or other like software or application, unless such software has been pre-approved by the Office of the Chief Information Officer for use by Participating Agencies.

NOTE

ELV has elected to allow passwords to be remembered by the ELV mobile applications based on the user enabling Remember Me.

Cookies

Wherever possible, cookies shall be set to expire.

Disabling Accounts

User Accounts and Administrator Accounts shall be disabled when:

- The user leaves employment or has been placed on administrative leave.
- The accounts are inactive for more than ninety (90) days.

NOTE

ELV has elected to make user accounts inactive after three-hundred and sixty-five (365) days (not 90).

Inactivity Timeout

- User Accounts shall timeout after fifteen (15) minutes of inactivity requiring the user to re-Authenticate to access the account.
- Administrator Accounts shall timeout after five (5) minutes of inactivity requiring the user to re-Authenticate their password to access the account.

NOTE

ELV has elected to time-out user sessions after 35 minutes (not 15 or 5).

Logging

Logging of Authentication attempts, whether successful or failed, shall be in accordance with the Enterprise Logging Standard.

Vendors/Contractors

If ELV is utilizing Vendor Contractors or Vendor Personnel, ELV will make compliance with this standard a contractual obligation of such Vendor Contractors or Vendor Personnel.

Amendment

This Standard shall be reviewed at least every two (2) years and amended as needed. This Standard may be amended in the sole discretion of the COO, taking into consideration the advice and input of the CEO.

Vulnerability Management Standard

Purpose

This Standard establishes the minimum requirements for vulnerability management for web-based systems.

Overview

ELV maintains a variety of data in its IT systems, including confidential customer information. In order to protect data and systems it is necessary to identify and remediate vulnerabilities in those systems. Vulnerability scanning identifies security weaknesses within systems and allows ELV to prioritize their resources to the most critical areas. Timely remediation of vulnerabilities is critical to maintaining the availability, confidentiality, and integrity of information technology (IT) systems.

Scope

This standard applies to all ELV developed/managed web-based applications.

Definitions

Selected terms used in the Enterprise Vulnerability Management Standard are defined below:

- **Authenticated Scan**: Vulnerability scan conducted using system credentials.
- **Critical Vulnerabilities**: Vulnerabilities identified as critical by software\hardware vendors, EVMS scanning tool; or vulnerabilities with a CVSS[1] rating of 9.0 or higher.
- **Enterprise Vulnerability Management System (EVMS)**: Enterprise-wide system to:
    - Inventory software\hardware deployed,
    - Identify vulnerabilities in the software\hardware; and
    - Report on vulnerabilities using a common format.
- **External Scan:** Vulnerability scan conducted from outside the organization's perimeter firewall.
- **Internal Scan**: Vulnerability scan conducted from within the organization's perimeter firewall.
- **Remediation:** Correction of the vulnerability or elimination of the threat. Examples of remediation efforts include: installation of a software patch, adjustment of a configuration setting, or removal of affected software.
- **Vulnerability:** Software flaw or misconfiguration that causes a weakness in the security of a system. Vulnerabilities can be exploited by a malicious entity to violate policies—for example, to gain greater access or permission than is authorized on a computer.
- **Vulnerability Scan**: Scan to identify hosts/host attributes and associated vulnerabilities.[1] Common Vulnerability Scoring System (CVSS).

Elements

The following are the elements of the Enterprise Vulnerability Management Security Standard.

1. **Inventory**: ELV shall maintain an inventory of hardware, operating systems, and software applications deployed by ELV.
2. **Monitor**: ELV shall monitor security sources for vulnerability announcements, patch notifications, and emerging threats.
3. **Scans**: ELV shall conduct vulnerability scans of their network using an Enterprise Vulnerability Management System (EVMS) system.
    a. External, internal and authenticated scans shall be conducted.
    b. Scans shall be conducted following each minor software release.
    c. New systems and applications shall be scanned before going to production.
4. **Access**: Server administrators shall provide sufficient administrative access to allow the vulnerability scan engine to scan all services provided via their systems.
5. **Exceptions\Credentials**: Firewall exceptions and credentials used by the EVMS in performing vulnerability scans shall be deactivated when not in use.
6. **Remediation**: ELV or it's designated contractor shall remediate vulnerabilities identified (via scanning, vendor alert or the National Vulnerability Database) as follows:
    a. **High Risk\Critical Vulnerabilities with An Active Exploit**: Within 5 business days of discovery\notification;
    b. **High Risk\Critical Vulnerabilities with No Active Exploit**: Within 10 business days of discovery\notification;
    c. **Medium Risk Vulnerabilities**: Within 30 business days of discovery\notification.
    d. **All Others**: According to the ELV remediation\patch management schedule.
7. **Vulnerabilities**: ELV shall maintain a list of un-remediated vulnerabilities.
    a. ELV shall notify the COO monthly of un-remediated vulnerabilities.
    b. ELV shall accept responsibility for any un-remediated vulnerability in their systems.
8. **Training:** ELV shall train system administrators on vulnerability monitoring and remediation.

Updates

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

Effective Date

This standard was approved by the COO on Jan 1, 2023 and shall be effective May Feb 1, 2023.

Logging Security Standard

Purpose

This standard establishes the minimum requirements for collection, storage and review of log information.

Overview

Logging is needed to identify and respond to unauthorized activities on all systems, and also to capture exceptions as they occur.

Scope

This standard applies to all Early Learning Ventures LLC, Alliance CORE related systems.

Definitions

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

- **Event**: Something that occurs within a system or network.

Enterprise Logging Standard

1. **Logging:** All applications shall be capable of and configured to:
    1. Produce audit logs, and
    2. Offload audit log data to a log aggregation server (if one exists – N/A)
2. **Events:** At a minimum, the following events (successful and failed) shall be captured in audit logs:
    1. Authentication attempts,
    2. Attempts to use a privileged account,
    3. Attempts to change account passwords,
    4. The following shall be logged for each event:
        1. User/subject identity,
        2. Date and time of the event,
        3. Source of access,
        4. Duration of access,
        5. Actions executed, and
        6. Action result.
3. **Applications:** Application, including web services and database services, residing on servers that utilize cashed or separate authentication capabilities must also maintain

logs of all security, application and event related information. Web applications shall also meet the requirements of Enterprise Web Application Security Standard.

4. **Storage:** The System Administrator will ensure audit storage capacity is allocated in accordance with system configuration such that capacity is not exceeded.
5. **Log Access:** Audit records, audit settings, and audit reports shall be protected from unauthorized access, modification, and deletion.
6. **Alerts:** Where feasible systems shall be configured to provide real-time alerts for the following:
    1. Audit failure.
    2. Escalation of privileges
    3. Five (5) or more consecutive failed authentication attempts.
7. **Time Stamps:** Systems shall be configured to generate time stamps to include both date and time. The time may be expressed in Coordinated Universal Time (UTC) and utilize Network Time Protocol (NTP) time synchronization.
8. **Retention:** Audit logs shall be retained for a minimum of 45 days. Maximum log retention shall be set to meet agency contractual requirements.
9. **Review:** Audit logs shall be reviewed at least weekly. Alerts shall be reviewed daily.
10. **Providers:** Third party providers shall meet the requirements of this standard.

Updates

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

Effective Date

This standard was approved by the COO on Jan 1, 2023 and shall be effective Feb 1, 2023.