Application Security Policy

Sample Organization

Criteria satisfaction

Standard	Criteria Satisfied
TSC 2017	CC6.2

Document history

Date	Comment
Jun 1 2018	Initial document

Contents

1 Purpose and Scope

a. This application security policy defines the security framework and requirements for applications, notably web applications, within the organization's production environment.

b. This document also provides implementing controls and instructions for web application security, to include periodic vulnerability scans and other types of evaluations and assessments.

c. This policy applies to all applications within the organization' production environment, as well as administrators and users of these applications. This typically includes employees and contractors.

2 Background

a. Application vulnerabilities typically account for the largest number of initial attack vectors after malware infections. As a result, it is important that applications are designed with security in mind, and that they are scanned and continuously monitored for malicious activity that could indicate a system compromise. Discovery and subsequent mitigation of application vulnerabilities will limit the organization's attack surface, and ensures a baseline level of security across all systems.

b. In addition to scanning guidance, this policy also defines technical requirements and procedures to ensure that applications are properly hardened in accordance with security best practices.

3 References

a. Data Classification Policy

b. OWASP Risk Rating Methodology

c. OWASP Testing Guide

d. OWASP Top Ten Project

4 Policy

a. The organization must ensure that all applications it develops and/or acquires are securely configured and managed.

b. The following security best practices must be considered and, if feasible, applied as a matter of the application's security design:

   i. Data handled and managed by the application must be classified in accordance with the Data Classification Policy (reference (a)).

   ii. If the application processes confidential information, a confidential record banner must be prominently displayed which highlights the type of confidential data being accessed (e.g., personally-identifiable information (PII), protected health information (PHI), etc.)

   iii. Sensitive data, especially data specifically restricted by law or policy (e.g., social security numbers, passwords, and credit card data) should not be displayed in plaintext.

   iv. Ensure that applications validate input properly and restrictively, allowing only those types of input that are known to be correct. Examples include, but are not limited to cross-site scripting, buffer overflow errors, and injection flaws.

   v. Ensure that applications execute proper error handling so that errors will not provide detailed system information to an unprivileged user, deny service, impair security mechanisms, or crash the system.

vi. Where possible, authorize access to applications by affiliation, membership or employment, rather than by individual. Provide an automated review of authorizations on a regular basis, where possible.

vii. Ensure that applications encrypt data at rest and in transit.

viii. Implement application logging to the extent practical. Retain logs of all users and access events for at least 14 days.

ix. Qualified peers conduct security reviews of code for all new or significantly modified applications; particularly, those that affect the collection, use, and/or display of confidential data. Document all actions taken.

x. Implement a change management process for changes to existing software applications.

xi. Standard configuration of the application must be documented.

xii. Default passwords used within the application, such as for administrative control panels or integration with databases must be changed immediately upon installation.

xiii. Applications must require complex passwords in accordance with current security best practices (at least 8 characters in length, combination of alphanumeric upper/lowercase characters and symbols).

xiv. During development and testing, applications must not have access to live data.

c. Where applications are acquired from a third party, such as a vendor:

i. Only applications that are supported by an approved vendor shall be procured and used.

ii. Full support contracts must be arranged with the application vendor for full life-cycle support.

iii. No custom modifications may be applied to the application without confirmation that the vendor can continue to provide support.

iv. Updates, patches and configuration changes issued by the vendor shall be implemented as soon as possible.

v. A full review of applications and licenses shall be completed at least annually, as part of regular software reviews.

d. Web applications must be assessed according to the following criteria:

i. New or major application releases must have a full assessment prior to approval of the change control documentation and/or release into the production environment.

ii. Third-party or acquired applications must have a full assessment prior to deployment.

iii. Software releases must have an appropriate assessment, as determined by the organization's information security manager, with specific evaluation criteria based on the security risks inherent in the changes made to the application's functionality and/or architecture.

iv. Emergency releases may forego security assessments and carry the assumed risk until a proper assessment can be conducted. Emergency releases must be approved by the Chief Information Officer or designee.

e. Vulnerabilities that are discovered during application assessments must be mitigated based upon the following risk levels, which are based on the Open Web Application Security Project (OWASP) Risk Rating Methodology (reference (b)):

i. High - issues categorized as high risk must be fixed immediately, otherwise alternate mitigation strategies must be implemented to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the production environment.

ii. Medium - issues categorized as medium risk must be reviewed to determine specific items to be mitigated. Actions to implement mitigations must be scheduled. Applications with medium risk issues may be taken off-line or denied release into the production environment based on the number of issues; multiple issues may increase the risk to an unacceptable level. Issues may be fixed in patch releases unless better mitigation options are present.

iii. Low - issues categorized as low risk must be reviewed to determine specific items to be mitigated. Actions to implement mitigations must be scheduled.

f. Testing is required to validate fixes and/or mitigation strategies for any security vulnerabilities classified as Medium risk or greater.

g. The following security assessment types may be leveraged to perform an application security assessment:

i. Full - comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide (reference (c)). A full assessment must leverage manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered issues.

ii. Quick - consists of an automated scan of an application for, at a minimum, the OWASP Top Ten web application security risks (reference (d)).

iii. Targeted - verifies vulnerability remediation changes or new application functionality.

iv. To counter the risk of unauthorized access, the organization maintains a Data Center Security Policy (reference (c)).

v. Security requirements for the software development life cycle, including system development, acquisition and maintenance are defined in the Software Development Lifecycle Policy (reference (d)).

vi. Security requirements for handling information security incidents are defined in the Security Incident Response Policy (reference (e)).

vii. Disaster recovery and business continuity management policy is defined in the Disaster Recovery Policy (reference (f)).

viii. Requirements for information system availability and redundancy are defined in the System Availability Policy (reference (g)).