Web Application Security Policy

1.0 Purpose

Web application vulnerabilities represent a primary attack vector and pose significant risks to organizational security. Identifying and remediating vulnerabilities resulting from misconfigurations, coding errors, weak authentication, improper error handling, or information leakage is crucial before applications are deployed or updated. The purpose of this policy is to define the mandatory requirements for conducting web application security assessments within the organization. This policy aims to ensure that potential weaknesses are identified and mitigated, limiting the attack surface of web applications and services, protecting organizational data, and ensuring compliance with relevant security standards and change control processes.

2.0 Scope

This policy applies to all web applications developed, deployed, hosted, or managed by the organization, whether internal or external-facing. It applies to all individuals, groups, departments, and third-party vendors involved in the development, deployment, management, or assessment of these web applications. All web application security assessments requested or performed within the organization fall under the scope of this policy.

3.0 Policy Statements

3.1 Assessment Requirement and Authority

* All web applications within the scope of this policy are subject to security assessments as defined herein.
* Web application security assessments must be performed only by designated and qualified security personnel, either employed or contracted by the organization (hereafter referred to as the "Assessment Team").
* Assessment findings are considered confidential organizational information and must be distributed strictly on a "need-to-know" basis to personnel involved in the application's development, management, or remediation efforts. External distribution is prohibited without explicit executive approval (e.g., Chief Information Officer).

3.2 Assessment Triggers and Scope

Web applications must undergo security assessments based on the following criteria:

*   **New or Major Application Release:** A **Full Assessment** is required *before* final approval in the change control process and deployment into the production environment.
*   **Third-Party or Acquired Web Application:** A **Full Assessment** is required before integration into the organization's environment or network. Post-assessment, the application is subject to all requirements of this policy.
*   **Point Releases (Minor Functional Changes):** An appropriate assessment level (**Targeted** or **Quick**, potentially **Full** depending on risk) is required, determined by the Assessment Team based on the scope and potential security impact of the changes.
*   **Patch Releases (Bug Fixes, Minor Updates):** An appropriate assessment level (**Targeted** or **Quick**) is required, determined by the Assessment Team based on the risk associated with the patches or fixes. Security patches addressing known vulnerabilities require **Targeted** validation testing.
*   **Emergency Releases:** In documented emergency situations requiring immediate deployment, a security assessment may be temporarily bypassed with explicit approval from designated executive leadership (e.g., Chief Information Officer or delegated authority). However, the application carries assumed risk, and a **Full Assessment** must be scheduled and performed as soon as practicably possible post-deployment (e.g., within 30 days).

*   **Scoping:** Assessments will include all components and tiers of the application identified during scoping unless explicitly limited with documented justification approved before the assessment begins.

3.3 Risk Rating and Remediation

Security vulnerabilities identified during assessments will be risk-rated based on a standard methodology (e.g., OWASP Risk Rating Methodology). Remediation must occur according to the following requirements:

*   **High Risk:** Vulnerabilities rated as High must be remediated, or effective compensating controls must be implemented and approved by the Assessment Team/Information Security, **before** the application is deployed or allowed to remain in production. Failure to address High-risk issues may result in the application being denied deployment or taken offline immediately. Remediation validation testing is mandatory.
*   **Medium Risk:** Vulnerabilities rated as Medium must be reviewed, and a remediation plan with timelines must be developed and approved. Remediation should typically occur within the next planned release cycle (e.g., point/patch release) or within a defined timeframe (e.g., 60-90 days). Depending on the number and nature of Medium-risk findings, the Assessment Team/Information Security may require mitigation or delayed deployment. Remediation validation testing is mandatory.
*   **Low Risk:** Vulnerabilities rated as Low should be reviewed, documented, and scheduled for remediation as part of regular maintenance cycles or future releases based on available resources.

3.4 Assessment Levels

The Assessment Team will perform assessments at the following levels, as appropriate:

*   **Full Assessment:** Comprehensive testing for a wide range of known web application vulnerabilities (e.g., based on OWASP Testing Guide, OWASP Top Ten, SANS Top 25) using a combination of automated scanning tools and in-depth manual penetration testing techniques to validate findings and assess actual risk.
*   **Quick Assessment:** Primarily automated vulnerability scanning focused on common high-impact vulnerabilities (e.g., OWASP Top Ten) to provide a rapid risk overview. Manual validation may be limited.
*   **Targeted Assessment:** Focused testing on specific vulnerabilities (e.g., for remediation validation) or specific new/changed application functionality.

3.5 Approved Tools and Techniques

*   The Assessment Team will utilize a set of approved automated scanning tools and manual testing methodologies. *(The specific list of approved tools should be maintained internally by the Assessment Team).*
*   The Assessment Team reserves the right to use additional tools or techniques as necessary to investigate potential vulnerabilities, validate findings, and determine overall risk.

4.0 Integration with Change Control

*   Web application security assessments are an integral part of the organization's change control process.
*   Relevant assessment results and remediation status must be documented within the change control records before deployment approval for applicable releases (New, Major, Point, Patch).
*   Applications deployed without adhering to the assessment requirements of this policy may be subject to immediate removal from the production environment at the discretion of Information Security or executive leadership.

5.0 Compliance

5.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security, Internal Audit) will verify compliance with this policy through various methods, including review of change control records, audit of assessment reports and remediation tracking, penetration testing, internal/external audits, and review of application security program documentation.

5.2 Exceptions

Any exception to this policy (e.g., delaying an assessment beyond standard triggers) requires formal, documented justification, risk acceptance by appropriate business and IT leadership, and advance approval from the designated Information Security authority (e.g., Precision Computer Team).

5.3 Enforcement

Failure to comply with this policy may result in deployment delays, applications being taken offline, or other corrective actions. Non-compliance by personnel may lead to disciplinary action, up to and including termination of employment or contract.

6.0 Definitions

*   **Web Application:** A client-server computer program where the client (including the user interface and client-side logic) runs in a web browser.
*   **Vulnerability:** A weakness in a system, application, or process that could be exploited by a threat actor.
*   **OWASP (Open Web Application Security Project):** A non-profit foundation focused on improving software security. Known for resources like the OWASP Top Ten (list of critical web application security risks), Testing Guide, and Risk Rating Methodology.
*   **Penetration Testing:** A simulated cyber attack against a computer system to check for exploitable vulnerabilities.
*   **Remediation:** The process of fixing or mitigating identified vulnerabilities.
*   **Compensating Control:** An alternative security measure put in place when it is not feasible or practical to directly remediate a vulnerability according to standard requirements.

7.0 Related Policies and Standards

*   Change Management Policy
*   Secure Development Lifecycle (SDL) Policy / Standards
*   Vulnerability Management Policy
*   Risk Management Framework / Policy
*   Information Security Policy (Overall)
*   Third-Party Risk Management Policy

Revision #2
Created 28 August 2024 16:59:12 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery