# Web Application Security Policy

Last revised: October 2017
Last reviewed: January 2019
**Next review: January 2020**

Information Security Branch, Ministry of Central Services

*This document specifies the Web Application Security Policy of the Government of Saskatchewan.*

## Purpose:

The purpose of this policy is to define web application security assessments within the Government of Saskatchewan (GoS). Web application security assessments are performed to identify potential or realized weaknesses as a result of inadvertent misconfigurations, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of GoS services available both internally and externally as well as satisfy compliance with any relevant policies in place.

## Scope:

This policy applies to all GoS web application security assessments requested by any individual, group, or department for the purpose of maintaining the security posture, compliance, risk management, and change control of technologies in use at GoS.

All web application security assessments will be performed by Information Security Branch, under the direction of the Chief Information Security Officer. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of the GoS is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

## Definitions:

The following definitions apply to the Web Application Security Policy:

**Risk Level:** Information Security Branch will assign a level of risk in accordance with the following definitions:

- **High** – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
- **Medium** – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- **Low** – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

**OWASP Risk Rating Methodology:** Open Web Application Security Project (OWASP) is an unbiased source of information on the best practices for improving the security of software.

## Policy Statements:

The following policy statements apply to the Web Application Security Policy:

Web applications are subject to security assessments based on the following criteria:

- **New or Major Application Release** – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- **Third Party or Acquired Web Application** – will be subject to full assessment after which it will be bound to policy requirements.
- **Point Releases** – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- **Patch Releases** – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- **Emergency Releases** – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

All security issues that are discovered during assessments must be mitigated based upon the Risk Level assigned. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater. The following security assessment levels shall be established by the Information Security Branch:

- **Full** – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
- **Quick** – A quick assessment will typically consist of an automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
- **Targeted** – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

Other techniques and tools may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

## Compliance and disciplinary action

In cases where it is determined that a breach or violation of GoS policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Ministry, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

## Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.