Application Security Policy

Statement of Policy
Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective
The policy and associated guidance provide an organized approach for all instances and stages of development initiated for WashU departments or schools. Based on the project requirements applications are developed in-house, with a third party or (commercial off the shelf) COTS. This policy will cover all instances to ensure the appropriate security controls are implemented for applications developed for WashU.

Applicability
This policy is applicable to all WashU applications, systems and network segments.

Audience
The audience for this policy is all WashU faculty, staff and students. It also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “WashU community”.

Roles & Responsibilities

Policy
Secure development practices will be established, implemented, and documented for all applications developed or purchased to include appropriate security controls to prevent unauthorized access or modification of the system or information coded or stored.

Open Web Application Security Project (OWASP) and OWASP Secure Coding guidelines will be followed.
Information Security Office (ISO) will establish the required controls for applications that will access, store, transmit or manipulate protected and confidential information. These controls are required for all life cycle stages of development.

- Test environments will be separate from the production environment.
- Separation of duties will be established and monitored to ensure conflicting roles and access to all phases of the development and implementation process is not granted.
- A risk assessment will be performed prior to production for all applications that will store, access, create and/or transmit confidential or protected information.

Policy Compliance
The ISO will measure the compliance to this policy through various methods, including, but not limited to - reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the ISO in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources or the Office of Student Conduct.

Related Policies
Information Classification Policy
Encryption Policy

Reference
Open Web Application Security Project (OWASP)
OWASP Secure Coding
OWASP Code Review Guide

Policy Review
This policy will be reviewed at a minimum every three years.

Title: Application Security Policy
Version Number: 2.0
Reference Number: SI-01.01
Creation Date: February 2, 2011
Approved By: Security and Privacy Governance Committee
Approval Date: April 6, 2016
Status: Final
Scheduled Review Date: March 1, 2022
Revision Date: February 26, 2019
Revision Approval Date: March 15, 2019
Policy Owner: Information Security Office