Web Application Security Policy

Version 1.0

Purpose

The purpose of this policy is to enforce that web applications maintain the security posture, compliance, risk management, and change control of the Marketplace Resources.

Scope

This IT policy, and all policies referenced herein, shall apply to all staff of the organisation, client and other stakeholders, authorized guests, and independent contractors (the “User(s)” or “you”) who use, access, or otherwise employ, locally or remotely, the Marketplace IT Resources, whether individually controlled, shared, stand-alone, or networked.

Policy Statement

- Web application security assessments must be performed to identify potential or realized weaknesses (e.g., insecure coding, inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage) as per the Vulnerability Management Policy.
- Web applications must follow regular security or out-of-band assessments if one of the following criteria are met:
    - New or significant application releases are subject to the Secure Software Development Life Cycle before approval of the change control documentation or release into the live environment.
    - Third-party or acquired web applications (i.e., commercial applications for which source code is not available) must be scanned when installed or upgraded. The vulnerabilities must be reported to Information Security and Assurance (ISA) and the vendor for correction.
- Shared accounts are prohibited, except where it is not technically possible to individually provision accounts.
- All Internet-facing web applications should deploy the Information Security and Assurance approved technical controls (e.g., Web Application Firewall (WAF) or Intrusion Prevention System (IPS)).

- Other security controls include but are not limited to, the following:
    - Access controls,
    - Configuration changes (you must submit non-agreed upon configuration changes to Information Security and Assurance for review),
    - Authentication (multi-factor authentication must be used for except where it is not technically possible),
    - Data protection (e.g., encryption, data masking),
    - Error handling and logging,
    - Input and output handling, and
    - Session management.

Definitions

IT Resources include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

Web Application Security is a branch of information security that deals specifically with the security of websites, web applications, and web services.

Related Policies and Procedures

Vulnerability Management Policy

Revision History

Version	Date	Description
1.0	07/31/2019	Initial policy
	08/17/2020	Periodic review, no changes

Policy Disclaimer Statement

Deviations from policies, procedures, or guidelines published and approved by Information Security and Assurance (ISA) may only be done cooperatively between ISA and the requesting entity with sufficient time to allow for appropriate risk analysis, documentation, and possible presentation to authorized University representatives.