Document Reference Number	**UoG/ILS/IS 014**
Title	Policy for Web Application Security
Owning Department	Information and Library Services
Version	3.4
Approved Date	10/12/2024
Approving Body	IT Management Board (IM)
Review Date	09/12/2025
Classification	Internal - Confidential

Version Control

Version	Last Modified	Last Modified By	Document Changes
3.4	10/12/2024	Atif Siddique	Added version control.

Policy for Web Application Security

1.0 Introduction

1.1 Vulnerabilities in web applications account for a large portion of cyber-attacks other than malware, requiring the need to assess and remediate vulnerabilities in web applications before deployment, and ensure ongoing monitoring and maintenance of relevant security controls.

1.2 Web applications utilised by the university must comply with applicable frameworks and best practices to provide appropriate security controls and minimise risks to the university's information systems and data.

2.0 Reference to International Organisation for Standardisation (ISO) 27001

2.1 This policy complies with the university's information security strategy and draws upon the ISO 27002 Code of Practice.

3.0 Scope

3.1 This policy applies to all web applications used to conduct university operations. This includes applications developed in-house or customised for the university, cloud-based or on-premise.

4.0 Transport Layer Security (TLS) Requirement

4.1 The TLS protocol is used to secure communications in a wide variety of online transactions between web servers and client computers. Any network service that handles sensitive data should adequately protect that data using secure client authentication, data encryption and data integrity which TLS provides.

5.0 Requirements

5.1 TLS Configuration:

- University web servers must be configured with the recommended TLS configuration in line with the Policy for Use of Cryptographic Controls and Key Management.
- Where the implementation of the recommended TLS configuration will significantly hinder communications between connecting systems (servers and client computers), it may be permissible to retain the immediate lower configuration of the recommended TLS on web servers for a short period with the authority of the Associate Director – Technology & Operations or a nominee. Supplementary controls to mitigate any associated risks must be put in place and the web server must be updated to run the recommended TLS configuration as soon as it is practical.

5.2 Encryption:

- TLS certificates must be obtained from a Certificate Authority (CA) for production systems, and valid TLS certificates must be used for all sensitive information in transit between a web server, other supporting servers and clients.
- Where a self-signed certificate is recommended for use, this must be used only on web servers that are not Internet-facing.
- Sensitive data must be stored in databases on internal servers with appropriate firewalls and access restrictions in place. Encryption should be considered for stored sensitive data.
- Industry-standard algorithms and implementations must be used for applications using cryptography. A list of university-approved cipher suites can be found in the Policy for Use of Cryptographic Controls and Key Management. This list is updated as necessary.

5.3 Authentication and Authorisation

- University approved and supported authentication service must be used to authenticate users.
- Where systems contain sensitive information, multifactor authentication must be enabled if supported.
- Authentication and other sensitive transactions including data transmission must be done over secure connections. Authorisation credentials must be stored securely.
- Access to web applications that process sensitive data must be controlled at account login and must verify authorisation for each request.
- Least privileged access must be the standard when assigning access rights.

5.3.1 University Approved and Supported Authentication Methods

- AD (Active Directory) – Uses Kerberos authentication protocol and provides authentication to Windows desktops, Exchange email, remote desktop and any system that uses AD for authentication.
- ADFS (Active Directory Federated Service) – Is the Active Directory Federated Service and provides single sign-on that extends user authentication to systems and applications inside and outside the corporate firewall.
- Azure AD (Azure Active Directory) – provides sign-on via ADFS to Microsoft 365 and other SaaS applications with policy-driven conditional access.
- AD LDS (Active Directory Lightweight Directory Services) – Provides authentication to directory-enabled applications without the restrictions of Active Directory Domain Services.
- OpenAthens – Provides management platform for federated authentication using ADFS within and across organisations.
- EIS (Ellucian Identity Services) - provides a management platform for federated authentication using ADFS to the Ellucian and third party integrated online application.

5.4 Data Validation and Sanitisation

The following must be carried out to validate the data used within the university's web applications:

- Data input and output in a web application must be validated for expected values, including data that is passed to web browsers, database systems and command shells.
- Server-side validation must be used.
- Data received from another source must be validated to be trustworthy.
- All requests initiated by users must be validated.
- Data sanitisation or content filtering techniques must be implemented on web applications to modify untrusted contents to conform to a safe set of rules to prevent malicious activities such as content injection attacks.

5.5 Session management

- Session times for web application operations must be kept to the minimum duration necessary. Session timeouts should be appropriately strict with consideration for likely usage scenarios.
- A session must be disconnected after a specified period of inactivity, and disconnections must be server-based.
- To avoid sending 'hidden' data to a browser, secure session key/token must be used.

5.6 Securing cookies:

- "Secure flag" must be enabled on web applications to ensure cookies that contain sensitive data are transmitted only over secure channels (HTTPS).
- Sensitive data must not be stored in cookies, and cookies must be set to expire to invalidate session cookies when they expire.
- New cookies must be generated when users switch between non-encrypted (HTTP) communications to encrypted (HTTPS) communications.
- Users must be notified of the use of cookies when using university web applications.

5.7 Protect server error messages

A generic error message page must be displayed to users instead of web server error messages to prevent vulnerability exploitation.

5.8 Web applications must have up-to-date patches and where exceptions to this are required, they must be reviewed and signed off by the relevant ILS team and the Associate Director – Technology & Operations.

5.9 Audit logs must be maintained and stored securely for events relating to user activities, system operations, warnings, errors and handling, privilege elevation, failed and successful login attempts, etc. ideally for ninety days wherever possible. All university hosted web servers must have their clocks synchronized to a university time server. Cloud-hosted systems should sync to suitable time services. Refer to the Policy for Monitoring and Logging for more information.

5.10 Any development relating to existing web applications must be done within a test environment and not production. Development, test and UAT (User Acceptance Testing) environments must be reviewed and cleansed of sensitive data (where the business requirement permits), maintained and monitored appropriately, or decommissioned if no longer required.

6.0 Externally Accessible Systems

6.1 University hosted Internet-facing systems must be penetration tested before they go-live and access must be made available via the university's load balancers/WAF (Web Application Firewall).

7.0 Policy Compliance

7.1 All web applications used by the university as stated in section 3.0 must comply with the principles set out in this policy.

7.2 The Web Application Security Guidelines and Risk Assessment documents provide detailed information for implementing this policy.

7.3 The necessary steps to verify compliance with this policy shall be undertaken. This includes, but is not limited to, business tool reports, internal and external audits and feedback to the policy owner.

7.4 Failure to adhere to this policy may be addressed under the university's disciplinary processes and relevant contractor and third-party contractual clauses relating to non-conformance with the Information security policies.

8.0 Exception to policy

8.1 Exceptions to this policy must be reviewed and approved by the Executive Director and Chief Information Officer or a nominee.

9.0 Policy Review and Maintenance

9.1 This policy shall be reviewed annually and where necessary will be updated as part of the continual improvement process.

10.0 Related Policies and External Guidelines

- Information Security Policies and related documents
- Information Compliance Policies and related documents
- Web Application Security Guidelines and Risk Assessment
- Open Web Application Security Project (OWASP) Top 10 Application Security Risk
- Open Web Application Security Project (OWASP) Top 10 Application Security Risk in Detail
- National Institute of Standards and Technology (NIST) - Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations