Document Reference Number	**UoG/ILS/IS 010**
Title	Policy for Secure Development
Owning Department	Information and Library Services
Version	1.2
Approved Date	10/12/2024
Approving Body	IT Management Board (IM)
Review Date	09/12/2025
Classification	Public – non-sensitive

Version Control

Version	Last Modified	Last Modified By	Document Changes
1.2	10/12/2024	Atif Siddique	Added version control.

Policy for Secure Development

1.0 Purpose

1.1 To ensure information security is designed and implemented within the development lifecycle.

2.0 International Organisation for Standardisation (ISO) 27001 Reference

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 the development of bespoke company software solutions.

3.2 This policy applies to all staff and external developers who undertake development work on behalf of the university.

4.0 Principles

4.1 Secure software and system engineering principles and standards are implemented and tested.

4.2 Information security and privacy are by design and default.

5.0 Segregation of Environments

5.1 Development, test and production environments should be separated and should not share common components.

5.2 Environments and components should be isolated using network access controls.

5.3 There shall be a segregation of administrative duties between development, test and production environments.

6.0 Secure Development Coding

6.1 Software should be designed and developed based on industry standard secure coding guidelines and the Open Web Application Security Project (OWASP).

6.1.1 The NCSC government guidelines for secure development should be considered: https://www.ncsc.gov.uk/collection/developers-collection

6.1.2 The NIST Whitepaper on 'Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework' should be considered: https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

7.0 Development Code

7.1 Development Code Repositories

Development code shall be stored in a secure code repository that enforces and meets the requirements of the university's User Account and Access Management Policy.

7.1.1 Development code repositories shall enforce version control and appropriate version archiving.

7.2 Development Code Reviews

Development code should be reviewed prior to release by skilled personnel other than the code author / developer.

7.2.1 Code should be reviewed against the secure development coding guidelines, as specified in Section 6 of this policy.

7.2.2 Code reviews should employ manual and automated techniques where possible.

7.3 Development Code Approval

Development code should be approved before being promoted into test or production environments.

8.0 Testing

8.1 All pre-production testing shall be undertaken in a non-production environment.

8.2 Application security testing should be performed against the OWASP Top 10, where possible.

8.3 Test Data

Compliance with the university's Policy for Use of Real Data in Non-Production Systems must be ensured.

9.0 Promoting Code to Production

9.1 Code should be promoted to production by approved personnel and is subject to the documented change control process, as detailed in the university's Policy for IT Systems Change Management.

9.2 The production environment shall be backed up prior to the promotion of code to production to facilitate roll back for a failed change.

9.3 Test data shall be removed before the code is promoted to production.

10.0 Policy Compliance

10.1 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.

10.2 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.

11.0 Exception to Policy

11.1 Any exception to this policy must be approved by the Executive Director and Chief Information Officer or a nominee.

12.0 Policy Review and Maintenance

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

13.0 Related Policies, Procedures and Standards

- Information security policies and associated documents
- Information compliance policies and associated documents