Document Reference Number	UoG/ILS/IS 006
Title	Policy for Third-Party Supplier Security
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. Added section on security reassessments.

Policy for Third-Party Supplier Security

1.0 Purpose

1.1 To ensure the data security requirements of third-party suppliers, their sub-contractors and the supply chain.

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 all third-party suppliers that process, store or transmit university data.

4.0 Principles

4.1 Third party suppliers shall meet the requirements of the university, legislation, and the relevant regulations for data security.

5.0 Third-Party Supplier Information

5.1 All third parties shall be registered and recorded as appropriate.

5.2 Third parties should be assessed for their criticality to the university and should be classified based on the data processed, stored or transmitted.

5.3 In addition, the following information shall be captured for all suppliers:

- Supplier name and contact details
- Service provided to the university
- What data they process, store or transmit
- Contract information, if applicable
- Assurance of suppliers' overall security posture

6.0 Third-Party Supplier Audit and Review

6.1 Where applicable, Information Security and Privacy Impact Assessments shall be undertaken as detailed in the university's Policy for Security & Privacy Assessments and Secure Data Handling. These assessments will assist in collecting the relevant information on suppliers and will help to identify any risks associated with the supplier or the service they provide, prior to engaging in a contract with the supplier.

6.2 Suppliers shall be reassessed periodically, though usually no sooner than two years from the initial assessment, to ensure they continue to meet the university's requirements for information security and data privacy.

6.2.1 The frequency of reassessments shall be commensurate with the level of risk associated with the supplier or the service they provide and shall consider the criticality of the supplier to the university's operations.

6.2.2 Where appropriate, the supplier shall implement corrective actions to address any identified deficiencies or vulnerabilities.

6.3 Where there is a major change to the risks associated with the supplier or the service they provide, security and privacy reassessments shall be undertaken to ensure they continue to meet the university's requirements for information security and data privacy.

7.0 Third-Party Supplier Selection

7.1 Third parties shall be selected based on their ability to meet the needs of the university as detailed in the Procurement Policy and Standard Procedures.

7.2 Prior to engaging a third-party supplier, information security and data privacy due diligence shall be carried out where necessary. This should include:

- An acceptable level of data security with risks identified, recorded and managed.
- Appropriate references
- Appropriate certifications
- Appropriate supplier agreements and contracts that include data security requirements.
- Legal and regulatory compliance.

8.0 Third-Party Supplier Contracts, Agreements and Data Processing Agreements

8.1 An appropriate contract, agreement and / or Data Processing Agreement must be in place and enforceable before engaging any third-party supplier to process, store or transmit confidential or personal information on behalf of the university.

8.2 Where possible, the university's data processing or data sharing templates should be used.

8.2.1 In instances where the university's data processing or data sharing templates are not used, all agreements shall be legally reviewed with reviews coordinated by the Legal Advisor (Information Compliance and Contracts).

8.2.2 Any amendments to the university's data processing or data sharing templates shall also be reviewed with reviews coordinated by the Legal Advisor (Information Compliance and Contracts).

8.3 Where necessary, third-party supplier contracts and agreements should include the right to audit.

8.4 All university policies apply to the third-party supplier.

8.5 Third-party suppliers are expected to have undertaken their own due diligence on their sub-contractors.

9.0 Third-Party Supplier Security Incident Management

9.1 Third-party suppliers shall have a Security Incident Management process in place.

9.2 Third-party supplier security incidents that impact the university must be reported to the university as per the contractual arrangement.

9.2.1 Third-party supplier security incidents shall be managed as part of the university's cyber incident response plan if necessary.

10.0 Third-Party Supplier End of Contract

10.1 At the end of the contract, the third party will confirm in writing that it has met its contractual and legal obligations for the retention of university information.

10.2 All third-party access to university systems and information shall be revoked.

10.3 Where applicable, all assets shall be returned to the university.

11.0 Policy Compliance

11.1 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.

11.2 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.

12.0 Exception to Policy

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

13.0 Policy Review and Maintenance

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

14.0 Related Policies, Procedures and Standards

- Information security policies and associated documents
- Information compliance policies and associated documents
- Procurement Policy and Standard Procedures