September 2019

Information Technology

Director of Information Technology

Version 1.0

Information Security Policy

ITPOL01

Academic excellence for
business and the professions

Contents

1. Overview

The University processes information in order to carry out its normal functioning. This may include confidential and personal information about businesses and individuals. Information is a valuable, costly, asset. Business continuance and academic progress is dependent on the integrity and availability of data. Steps will be taken to protect information assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional. This policy forms the key component of an information security management system (ISMS) which is a living document in support of these activities.

2. Scope and applicability

This policy applies to staff, students, alumni, contractors, consultants, temporary and visiting staff, including interns, retired staff, honorary staff, volunteers and other workers of the University, including all personnel affiliated with third parties who interact with the information held by the university in all its forms and its related information systems. This includes, but is not limited to, any systems or data attached to the University computer or telephony networks, systems supplied by the University or communications set to or from the University.
This policy applies to all people and assets in the execution of the original and supplemental University charters pertaining to IT. This policy is reviewed, maintained and updated by the Information Security Manager. This policy will be reviewed, at minimum, annually.

3. Normative references, subsidiary controls

- This document forms part of an ISO/IEC27001 aligned ISMS
- Controls 5 and 6 of ISO/IEC27002 are applicable
- All University IT security policies are subservient policies of this policy. Managerial authority for all subservient policies comes from this policy
- An Information Security Committee [1], comprising of management representatives from relevant parts of the organisation, shall coordinate the implementation of information security controls and approve subsidiary policies

4. Terms and definitions

For the purpose of this document, the terms and conditions given in ISO/IEC 27001 apply.

Standard IT taxonomy is used.

5. General policy – Information Security

The University is committed to protecting and securing the use of information and information systems under its control to protect and maintain the availability, integrity and confidentiality of this information.

- City, University of London undertakes to have in place procedures and controls to protect the information within its control;
- City, University of London will use a risk-based approach when assessing and understanding the risks associated with data and will use physical, personal, technical and procedural means to achieve appropriate and proportionate security measures;
- City, University of London will consider developments in technology and the costs of implementation in order to achieve a level of security appropriate to the nature and value of the information being held and the harm and damage which could result from a security breach;
- University academic staff, students and professional staff will be provided with access to data, which may include personal data, if it is required to perform their role or authorised requirements;
- City, University of London will provide guidance and training to academic staff, students and professional staff via a web-based system [2] to enable them to understand and carry out their responsibilities in respect of security, confidentiality and data protection;
- City, University of London IT will monitor academic staff, students and professional staff compliance with security obligations;
- City, University of London will use Cyber Essentials Plus, elements of ISO27001 and associated IT security standards as the guide for its information security governance;
- City, University of London will use elements of ISO9001 and associated standards as the guide for its quality assurance standards and governance;
- City, University of London will comply with the legislative and regulatory requirements placed upon it;
- All persons using the IT services of City, University of London are required to adhere to and be bound by English law. Specific reference is made here in context of data security to the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. Other acts of law are also applicable;
- The University will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

6. Roles and responsibilities

All users are responsible for data security, it is their duty to ensure university systems are used appropriately and securely. Any person who suspects misuse of University systems should report the matter to their manager, supervisor, or the IT Service Desk without delay.

7. Compliance

7.1 Compliance measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, video monitoring, and feedback to the policy owner.

7.2 Exceptions

Any exception to this policy must be approved by ExCo or the Director of IT in advance.

7.3 Non-compliance

Any reckless or wilful conduct by any person or persons using City, University of London's network and computer systems which undermines this policy or puts at risk the security of data (personally identifiable or not) may have disciplinary action taken against them. All such cases will be fully investigated according to the University's disciplinary procedures and may be reported to the regulatory authorities.

In the case of a criminal offence being committed, City, University of London will involve the appropriate authority.

8. Risk management

Risk management for each department / school is handled internally and recorded on the appropriate risk register.

9. Policy review

This policy will be reviewed by the process owners and updated alongside the security operating procedures on a regular basis, not to exceed 12 months.

10. Process owners

Director of IT

11. Review schedule

This policy, and its subsidiaries, shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations by the Information Security Manager and the Information Security Committee. Additional regulations may be created to cover specific areas as required.

12. Reference

[1] The Information Security Committee is currently on hold but will be reformed shortly.

[2] Metacompliance has been purchase for this purpose.

Document control

Change history			
Version	**Date**	**Author**	**Details of change**
1.0	30/10/2019	M Cann	Changed to live version

Document approval	
Approving Committee	**Approval Date**
Exco	**28/10/2019**

Document review		
Reviewer	**Role**	**Review Date**
Russell Best	Systems & Operations Manager	15/10/2019
Claire Priestly	Director IT	24/10/2019
M Cann	Information Security Manager	18/1/2022.