October 2019

Information Technology

Director of Information Technology

Version 1.0

Cloud Computing Policy

ITPOL04

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 its integrity and continued availability. Steps will be taken to protect information assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional. This policy forms part of an information security management system (ISMS) which is a living document in support of these activities.

The cloud [1] *(see reference section)* computing and managed services are a constantly evolving environment, where it can be particularly difficult to secure data. It is for this reason two categories of data are defined in this document. 'Sensitive', is the term used for data containing personally identifiable or commercially sensitive data. 'Non-Sensitive', is the term used to describe data containing neither personal nor commercially sensitive data.

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 where pertaining to IT. This policy is reviewed, maintained and updated by the Director of IT. This policy will be reviewed, at minimum, annually.

3. Normative references, subsidiary controls

- This document forms part of an ISO/IEC27001 aligned ISMS
- Controls A.8.2.1, A.9.2.1, A.11.1.1 of ISO/IEC27002 are applicable
- NCSC Cloud Security Principal. https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles
- All university IT security policies form the one aligned ISMS suite governed by the Information Security policy (POL01)

- ExCo shall oversee 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.

5.1 Data Sensitivity

Any data intended for cloud processing must be categorised according to its sensitivity. The two categories are as follows:

Sensitive

Any data that contains **any** personally identifiable information or commercially sensitive data must be categorised as sensitive.

Non-sensitive

Any data that does not contain personally identifiable information or commercially sensitive data will be categorised as non-sensitive.

5.2 Cloud providers

Sensitive data

Only suppliers who can satisfy the 14 requirements [2] of the National Cyber Security Centre (NCSC) cloud security principals may process and hold sensitive data on behalf of City, University of London. Any exceptions to this policy will need formal approval through the exceptions process.

Non-sensitive data

Any cloud provider that has been vetted through the standard IT procurement process including Technical Design Authority (TDA) may process and hold non-sensitive data.

6. Roles and responsibilities

All users of information systems are responsible for the security of data in their charge and care, 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 the Information Security Manager or 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 Data Protection Officer 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 may result in disciplinary action being 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. References

[1] Cloud Definition.

Cloud is a term used to describe a global network of servers, each with a unique function. The cloud is not a physical entity, but instead is a network of remote servers around the globe which are linked together and meant to operate as a single ecosystem. These servers are designed to either store and manage data, run applications or deliver content or a service such as streaming videos, web email, office productivity software or social media. Instead of accessing files and data from a local or personal computer, you are accessing them online from any Internet-capable device.

Azure.microsoft.com. (2019). *The Cloud – Definition | Microsoft Azure*. [online] Available at: https://azure.microsoft.com/en-gb/overview/what-is-the-cloud/ [Accessed 22 Oct. 2019].

[2] NCSC 14 Cloud principals.

The 14 principals are listed here:

- 1. Data in transit protection

  User data transiting networks should be adequately protected against tampering and eavesdropping.

- 2. Asset protection and resilience

  User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

- 3. Separation between users

  A malicious or compromised user of the service should not be able to affect the service or data of another.

- 4. Governance framework

  The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

- 5. Operational security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

- 6. Personnel security

  Where service provider personnel have access to corporate data and systems a high degree of confidence is required in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

- 7. Secure development

  Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise City data, cause loss of service or enable other malicious activity.

- 8. Supply chain security

  The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

- 9. Secure user management

  Tools should be made available for City IT services to securely manage the use of the provided service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of resources, applications and data.

- 10. Identity and authentication

  All access to service interfaces should be constrained to authenticated and authorised individuals.

- 11. External interface protection

  All external or less trusted interfaces of the service should be identified and appropriately defended.

- 12. Secure service administration

  Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

- 13. Audit information for users

  Audit records should be provided allowing access to be monitored to the cloud service and the data held within it. The type of audit information available will have a direct impact on the ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

- 14. Secure use of the service

  The security of cloud services and the data held within them can be undermined if the service is used poorly. Consequently, certain responsibilities will fall on City IT when using the service in order for the data to be adequately protected.

  Ncsc.gov.uk. (2019). [online] Available at: https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles [Accessed 22 Oct. 2019].

Document control

Change history			
Version	Date	Author	Details of change
1.0	**30/10/2019**	**M Cann**	**Live document version change**

Document approval	
Approving Committee	Approval Date
ExCo	28/10/2019

Document review		
Reviewer	Role	Review Date
Claire Priestley	Director of IT	24/10/2019