Policy
Third Party Access to Information and Information Systems

Document Filename	Third Party Access to Information and Information Systems.docx
Version	1.2
Information Classification	Open
Status	Approved
Date	19 October 2017
Policy Owner	Brian Fitzsimmons
Policy Contact	b.fitzsimmons@gcu.ac.uk

Document Approval and Version Control

Title		Name of Approvers			Date
Third Party Access to Information and Information Systems		Glasgow Caledonian University Executive Board			19/10/22017
Revision	**Status**	**Author (s)**	**Reviewed By**	**Approved By**	**Issue Date**
1.0	Draft	Brian Fitzsimmons	Mark Johnston, Hazel Lauder, Information Management Forum		
1.1	Draft	Brian Fitzsimmons	Information Governance Committee		
1.2	Approved	Brian Fitzsimmons		Executive Board	19/10/2017

Contents

1 Document Overview

1.1 Purpose

The purpose of this policy is to outline a series of controls, which will ensure effective information security when contracted third parties require access to University information. Effective use of and adherence to these controls will help ensure the confidentiality, integrity and availability of University information is maintained.

1.2 Scope

This policy applies to all University staff who have responsibility for the specification and management of University information systems and IT Services that are provided, supported, maintained or accessed by third party contractors.

1.3 Definitions

University: Glasgow Caledonian University is a Scottish Registered Charity, No. C021474 with its registered office at Cowcaddens Road, Glasgow G4 0BA, Scotland, UK.

Staff: Staff are salaried members of the University or individuals contracted by or to the University to provide a service.

Student: A person pursuing any course of study at the University.

Visitor: A visitor is anyone, not a member of staff or student, requiring access to University services or premises.

User: A member of staff, student or visitor who has been authorised by the University to use University IT Facilities and to gain access to University networks and information systems.

Information: The result of processing, manipulating, or organising data. Examples including but not limited to, text, images, sounds, codes, computer programmes, software and databases.

Information System: Any information processing system designed by or procured by and licensed to the University for Use in any of its IT Facilities.

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity: Property of accuracy and completeness.

Availability: Property of being accessible and usable upon demand by an authorized entity.

Contracted Third Party: An organisation or individual external to the University who has been contracted by the University to provide a service.

University IT Facilities: All University owned or leased accommodation which houses computer hardware or software which in turn is owned, leased or licensed to and operated by the University. This includes;

- Computer hardware and software owned by, leased or licensed to the University and connected to the University network (s) by whatever means
- Computer hardware and software owned by, leased or licensed to the University and not connected to the University network (s)
- All networking, data processing and information and communications systems, including connections to external computers or networks including systems accessed through commercial or other arrangements

1.4 Supporting Documents

Information Security Policy, Managing Third Party Access to University Information

2 Policy

The University will permit contracted third party access to University information, on-site or remotely, only where there are business reasons to do so and those reasons form part of a formal contract. The formal contract will include agreements that ensure the security of University Information, information systems and IT systems and protect and maintain the confidentiality, integrity, availability and value of University information.

All requests for contracted third party access to University information must be approved by the business lead responsible for that information. The responsible business lead, normally the Head of Department, will nominate a University member of staff who will have responsibility for managing the contracted third party's access. All access to University information must be set at a system level that will allow the contracted third party to carry out their activities as stated in the contractual agreement.

The University will only permit contracted third parties physical access to areas that contain IT hardware and other IT equipment such as on-site server rooms, when access to those areas has been agreed in advance with the relevant line managers. Access to these areas must be recorded and logged via the access control system.

The responsibility for reviewing and confirming that contracted third party access is still required lies with the University member of staff who manages the system or service that is provided, supported and or maintained by the contracted third party. Contracted third party system access rights must be reviewed and confirmed annually or more frequently as required.

For all contracted third party access to University information, the University and the contracted third party, must agree in advance a code of practise and non-disclosure agreement (s) that will protect University information assets and ensure working practises remain compliant. Where relevant, contracted third parties will be asked to provide a copy of their information security policies

Requests for on-site or remote contracted third party access to University information, must be recorded and managed as detailed in the ***Managing Third Party Access document.***

3 Review

The Information Governance Committee is responsible for keeping this policy current. This policy will be reviewed annually or more frequently as required.

4 Breaches of Policy

A breach of University policies, rules or regulations is considered as an issue of potential misconduct, which will be dealt with as a disciplinary matter under the University's Conduct & Capability policy. If there is anything in this policy that you do not understand, please discuss it with your line manager.

5 Information

If you have any questions regarding this policy please contact the University's Information Security Team via the IT Service Desk.

6 Policy Awareness

All individual users of University IT Facilities and information systems must comply with the appropriate information security policies, regulations, code of conducts, guidelines and practises and procedures including any external accountability.

It is a condition of use of the IT Facilities that a user's activity may be logged and or monitored and that information in their IT account, including but not limited to, files, images, documents, audio, videos, browsing history, communication history, may be accessed and processed with or without their consent as outlined in the ***Monitoring and Accessing Information policy.***

7 Guidance

For guidance and further information please go to

https://www.gcu.ac.uk/staff/it/itregulationspolicies/