Integrated Research
Campus

UNIVERSITY OF LEEDS

A.17.0 Information Security Aspects of Business Continuity Management

Document Information

Reference	ISMS 27001
Category	Information Security Management System (ISMS) Documents
Title	A.17.0 Information Security Aspects of Business Continuity Management
Purpose	Policies for Business Continuity
Owner	Information Governance Management Group (IGMG)
Author	Charles Hindmarsh
Compliance	ISO 27001
Review plan	Annually
Related Documents	University of Leeds Information Protection Policy ISMS Mandatory Clauses A.5.0 Information security policies A.6.0 Organisation of information security A.7.0 Human resources security A.8.0 Asset management A.9.0 Access control A.10.0 Cryptography Controls A.11.0 Physical and environmental security A.12.0 Operations security A.13.0 Communications security A.14.0 Systems acquisition, development and maintenance A.15.0 Supplier Relationships A.16.0 Information security incident management A.18.0 Compliance

Version History

Version	Date	Update by	Change description	Approved By	Date
1.0	27/06/2016	Samantha Crossfield / David Batty	Initial version	Barry Haynes (Chair of IGMG)	20/10/2016
2.0	12/10/2018	Charles Hindmarsh	New ISMS layout	Andy Pellow (Chair of IGMG)	22/03/2019
2.0	13/08/2019	Charles Hindmarsh	Tables renumbered	Andy Pellow (Chair of IGMG)	25/09/2019

Contents

Introduction

The Integrated Research Campus (IRC) is a University of Leeds (UoL) IT Service. It provides secure technical infrastructure and services for research data handling, analytics, application processing and development.

Purpose

This document sets out the Business Continuity Plan (BCP) within the IRC Information Security Management System (ISMS).

Applicability

The Business Continuity Plans (BCP) are managed by the Secretariat and are mostly out of scope of the IRC ISMS. Testing the IRC BCP IT configuration(s) are in scope and must be completed by IT to ensure the plans are working effectively

A.17.0 Information Security Aspects of Business Continuity Management

The purpose of this policy is to provide sufficient information to enable the IRC to restore full operational status, as quickly as possible, following any business interruption, regardless of its scale or impact.

The primary objective in the event of an interruption is to restore the availability and integrity of core services to a level which is satisfactory to our researchers and our clients.

A.17.1.1 Planning Information Security Continuity

A.17.1.1.1 Definition of a Critical Incident Requiring Business Continuity

A critical incident may be defined as any event which threatens to severely disrupt (in whole or in part) the functioning of a faculty, service or the University as a whole, and/or which carries the risk of significant adverse publicity.

An incident would normally have the following features:

1. There are substantial threats to the safety or well-being of individuals or to the fabric or reputation of the institution and
2. The incident is likely, or has the potential, to lead to the suspension of normal operations.

A critical incident might require:

1. The calling out of the emergency services.

2. Special communications mechanisms.
3. Awareness that media interest could be high.

Examples of critical incidents include:

1. A major fire or explosion.
2. An occurrence or outbreak of a contagious disease, such as meningitis.

A.17.1.1.1 University-wide Plan

The Secretariat maintains the University's Critical Incident Management Plan (CIMP) and is responsible for assisting the University Secretary with the coordination of the institution's response to any critical, or potentially critical event.

A.17.1.1.2 Leeds Institute for Data Analytics (LIDA) Specific plans

LIDA maintains its own list of key contacts. The cascade is reviewed annually.

A.17.1.1.3 IRC Specific Plans

The following plans are in place:

1. Projects can request high availability protection and have multiple nodes clustered in different Data Centre's (section A.17.2.1). Systems can automatically failover to one of the other nodes.
2. Data snapshots of all servers are configured and systems can be recovered from key points in time. Refer to the Back up of Data policy (A.12.3.1).
3. In some cases, project data can be entirely sourced from third parties and may be re-extracted in the case of data loss.
4. Remote access to IRC confidential projects is available, should the building be inaccessible.

A.17.1.2 Implementing Information Security Continuity

The University BCP process, or the University IT incident management process are both out of scope for the ISMS. However on receiving an instruction from the appropriate IT response team, The Data Services Team (DST), will initiate any necessary IRC BCP actions.

A.17.1.3 Verify, Review and Evaluate Information Security Continuity

The DST, with support from the wider IT service will manage the following annual checks to review that business continuity systems are active and working correctly (Table A.17.1.3.1).

Table A.17.1.3.1. BCP tests carried out

Task	Description	Frequency
UPS Battery Checks	Remove power and ensure UPS continues to provide power to end devices.	Annually
Server Failover Checks	Fail over some servers to the secondary data centre.	Annually
Disaster Tape/Snapshot Recovery	Test the process of recovering a server from tape / snapshot.	Annually
Check the Telephone Cascade List	Ensure the list is up to date and accurate (e.g. captures absence).	Annually
Test Remote Access	Ensure that working from home is an option for critical staff and researchers.	Annually

A 17.2 Redundancies

A.17.2.1 Availability of Information Processing Facilities

Resilience has been built into the IRC data storage service. The configuration can allow a single copy, two copies synchronously replicated between on-site data centres. If requested, a third copy can be configured to asynchronously replicate off-site to York University.

Resilience is an option provided in the costing model, but it is the responsibility of Principal Investigators to decide the level of risk that they will accept versus the resilience they are prepared to pay for.