***INFORMATION SECURITY CONTINUITY PLAN***

***ISMS-C-DOC 17.1.1a***

***Contents***

[1 Introduction 3](#_Toc12275847)

[2 Information Security Processes 5](#_Toc12275848)

[3 Emergency Response 6](#_Toc12275849)

[4 Scope 6](#_Toc12275850)

[5 Personnel 7](#_Toc12275851)

[6 Information Systems and Communications 10](#_Toc12275852)

[7 Financial and Legal 12](#_Toc12275853)

[8 Document Owner and Approval 13](#_Toc12275854)

# Introduction

* 1. The purpose of this plan is to set out the steps Retirement Capital will take to ensure information security during and after a **disaster,** whether minor, moderate or major, i.e. the loss of a significant part of the function of the ISMS for more than a few hours. Causes are typically in line with business continuity threats. The Emergency Response Teams will follow this plan, and the management team are committed to it.
  2. Following a disaster, the typical response **lifecycle** would be:
* Emergency response to assess level of damage, decide whether to invoke the plan and at what level, to notify employees/staff, etc.
* Provision of an emergency level of service
* Restoration of key controls
* Recovery to business as normal.
  1. Target times have been established for the above stages:
* to be completed within two business hours of the disaster
* within six business hours of the disaster
* within two days of the disaster
* within five days of the disaster.
  1. The key resourcesof Retirement Capital are:
* Employees/staff - provision of services is dependent on the knowledge and skills of existing employees/staff.
* Premises – all UK and Ireland Offices.
* Reception team - handling visitors, post and incoming calls.
* Telephony - the telephone lines, digital phone system, mobile phones.
* Information Technology - the data, software, hardware - file servers, PCs, printers etc., structured cabling for data and telephony, LAN equipment, WAN equipment.
* Paper records and filing systems.
* Services - Power, heating, lighting, water, etc.
  1. The strategic issues affecting the development of this plan are:
     1. Alternative sites; business continuity sites; use of a disaster recovery service.
     2. The key need immediately following disaster is what, and how will it be handled? (i.e. what services have to be restored first, and how quickly does it have to happen?)
     3. What additional risk issues might there be around telecommunications and data links?
     4. How long can be allowed to restore operations completely, what limiting factors are there, and what other issues have to be taken into account?
     5. How will employees/staff continue working, what will they do, what records will they maintain? Use of wireless laptops, PDAs, cellphones could be paramount here – with security implications.
     6. Storage of records and backup procedures (fireproof safes, offsite storage, how to access?)
     7. What are the repercussions of a disaster – press, customers, suppliers, others?
  2. This plan will be maintained in accordance [ISMS-C DOC 17.1.3](ISMS-C_DOC_17.1.3.docx)*.*
  3. This plan will be available in paper (in the main office) and electronic format

# Information Security Processes

* 1. Perimeter controls

Theperimeter controlsof Retirement Capital and the persons responsible for them are**:**

All information assets are stored on a local office server that is physically locked, encrypted and has secure access controls, which is used to backup the primary data repository on Google Cloud services. All paper information must be scanned and uploaded to Google and the original destroyed or kept in a locked environment according to classification.

The Company Administrator is responsible for ensuring that all paper information is stored according to classification.

In the event of an office failure resulting in forced evacuation, portable devices can be used to access all IT Systems from employees’ homes, with appropriate security.

* + 1. Alternates are identified in Section 4.3.
  1. Internal controls.

The internal controls of Retirement Capital (the ones that secure information within Retirement Capital), the persons responsible for them are department heads, IT Manager, CISO (DIRECTOR) and Managing Director.

* Retirement Capital servers, whether under direct control, hosted or cloud based are encrypted.
* Internal servers are replicated in real-time on the Google G-Suite Platform.
* Hosted data centres used by Retirement Capital includes disaster recovery provision.

In the event of a failure of a hosted server, the hosting partner’s disaster recovery procedure will be invoked.

In the event of an internal server failure, the company operation will switch the G-Suite version.

All servers must be resynchronised following resolution of the incident.

* 1. Priorities

Following a disaster, the immediate information security priorities are (in descending order):

* Affected staff: all staff will have an assigned “buddy” who is aware or critical work at all times.
* Alternative working space in the event of building or services failure: all key staff can return home and work from there.
* Telephone lines should be set up to be diverted to mobiles if cloud phone system fails.
* Information technology is a cloud-based service provided by Google and should be fully resilient, if this fails however a local copy of all company information will be backed-up onto the local server.
* All paper records must be scanned and stored electronically.

# Emergency Response

* 1. Emergency responses are conducted in line with information security incident management policies and processes (ISMS-C DOC 16.1.2-3, 16.1.5, 16.1.7).
  2. *Emergency Response Teams (ERT)*

The team comprises those employees/staff listed on the Emergency Team Contact Card so that, in the event of an emergency, they have someone to contact.

Contact details are on the intranet and all staff are issued with a card containing Emergency Response Teams contact details, to be used in the event of a disaster.

The responsibilities of the Emergency Response Teams are to:

* respond immediately to a potential information security continuity threat, assess the extent of the threat and its impact on information security,
* decide which elements of the Information Security Continuity Plan should be invoked,
* establish and manage an Information Security Recovery Team to return to normal operation,
* ensure employees/staff are notified and allocate responsibilities and activities as required.

# Scope

This procedure applies at all Retirement Capital’s sites. The Chief Information Security Officer is responsible for invoking the BCP in respect of any of the disasters identified in this plan as well as in the event of any other occurrence that affects Retirement Capital’s capability to perform normally.

# Personnel

* 1. Alternates

Key employees/staff have an alternate nominated who has the knowledge and ability to be able to deputise, at least on a temporary basis, should that member of staff be unavailable

**Role Holder Alternate**

MD Gavin McCloskey

CISO (DIRECTOR) Gavin McCloskey

IT Manager Gavin McCloskey

* 1. Calling Tree

A calling tree mechanism has been devised to share the work of ensuring that all staff are notified of the information security continuity event, rippling down from the Emergency Response Teams to the senior managers and then to the rest of the employees/staff. The person discovering the information security continuity event calls a member of the Emergency Response Teams, trying in the order listed on their disaster card; if no Emergency Response Teams member is available then alternates are tried.

The calling tree and contact numbers for key employees/staff are shown at Appendix 5 of this section.

ERT Leader (or first member of ERT notified)

MD

IT Manager

CISO (DIRECTOR)

Board Members

Exec Assistant

IT Manager

MD

**Staff contact numbers**

**Site 1 Main line**

| **Name** | **Role** | **Home number** | **Mobile number** |
| --- | --- | --- | --- |
| Gavin McCloskey | CISO (DIRECTOR) |  |  |
|  |  |  |  |
|  |  |  |  |

# Information Systems and Communications

* 1. Paper Records

Some important information exists solely in paper form; this includes:

* personnel records
* some financial records
* signed partner and supplier contracts
* some client information.

Key personnel, financial and legal documents are kept in a fire-proof cabinet in the London office, however all documents are scanned and held on the server.

* 1. Computer system
     1. Backup arrangements: all systems are mirrored – the hosted servers are mirrored with other hosted servers at the DR site, internal servers are a mirror of the Google G-Suite.
     2. All key staff have laptop computers which remain with them when they leave the office, allowing DR access to all available systems from any location.
     3. The relative priorities for restoration of the computer applications will be determined by the Emergency Response Teams but is likely to be:
* Customer facing servers and applications
* Access to cloud services
* Office telephony
* Office access
* Office based servers
  + 1. The planned approach is:

If hosted servers have failed, then ensure failover to DR systems has occurred as per hosting contract.

If office systems have failed, then:

* Notify all staff to switch to mobile working arrangements (Mobile phone and laptop computer) using Google G-suite.

If Google systems have failed, then:

* Notify all staff to switch to office server (using VPN if off site)

There are full instructions for the restore operation in the IT Department Working Instructions ISMS-C-REC-12.4.4

* + 1. The timescale is as follows:
* Validation of hosted systems failover: 1 hour max
* Office system failure failover: 1 working hour
* Google failure failover: 1 working hour
  1. Software

An analysis of the relative importance and difficulty of securely re-installing the key software products in use at *Retirement Capital*, together with contact details is contained in the following table.

| **Software** | **Analysis – importance and options** | **Contact** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Wide Area Network/WLAN/LANs

Retirement Capital utilises a simple internet-based cloud access methodology using a secure internet connection to Google G-Suite and VPN access to the office. Office systems use a local area network (wireless and wired), which is provided by the landlord and supplied as a LASER link to the building. There us a firewall and router that protect and segregate the LAN.

* + 1. The network comprises the following elements:
* Wireless Router
* Firewall
* Server
* Network Attached Storage

* 1. Telephony

Retirement Capital uses a cloud-based telephony system with IP handsets, in the event of failure the IT Manager will contact the IP telephony provider to resolve the problem and the company staff/employees will revert to using mobile phones – voice messages are relayed as emails.

* + 1. **In the event of an electrical power failure:**

In the event of an electrical power failure at the office site, staff will revert to using laptops and mobile phones, connected to G-Suite. These can be used at home or hotel locations – a hotel conference room will be hired in the event of prolonged outage.

# Financial and Legal

* 1. An assessment shall be made by the emergency response team of the impact on the financial affairs of Retirement Capital. The assessment should include:
* Loss of confidentiality, integrity or availability of information
* loss of financial documents
* loss of revenue
* theft of cheque books etc.
* loss of cash.
  1. Company or personal credit cards could be used to pay for supplies and services required following an information security event.
  2. The Emergency Response Teams will decide whether there may be legal actions resulting from the disaster; in particular, the possibility of claims by or against Retirement Capital.
  3. If legal actions are possible, then the Board of Directors should be advised.

# Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Chief Information Security Officer (CISO (DIRECTOR)) on 24th June 2019 and is issued on a version-controlled basis under his/her signature.

Signature:

Date: 24/06/2019

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 24/06/2019 |
|  |  |  |  |
|  |  |  |  |