1. **Scope** [ISO27002 Clause 12.3]

All Retirement Capital’s information assets are subject to backup requirements, including PDAs, mobile phones, notebook computers.

1. **Responsibilities**
2. All users have individual responsibilities for backup identified in their User Agreements (see control section 9.1 of the [Manual](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\InfoSecManual.docm)).
3. All owners of information assets are required to ensure that backup arrangements and Work Instructions that conform to the requirements of this procedure exist for each of the assets for which they are the identified owner.
4. The Director (CISO) is responsible for ensuring that the IT Department execute the identified backup WIs for central systems and devices as required and for identifying and reporting any faults, failures or errors.
5. The Operations Director is responsible for documenting, testing and maintaining the restoration process in line with business needs.
6. **Procedure – Office Systems**
7. The Retirement Capital in-houseserver hardware configuration includes RAID 10 based Network Attached Storage.
8. The Retirement Capital server runs an application called Drive File Stream that replicates all information held on the G-Suite Store with the local server network attached storage. In the event of loss of connectivity to G-Suite, the local server information can be used and resynchronized when connectivity is restored. If the local server fails, connectivity to G-Suite is maintained through cloud connectivity.
9. The phone system is similarly cloud based and can operate through a Smartphone Ap in the event that the IP handsets become inoperative.
10. On a monthly basis a full image of all Retirement Capital information held on the Google G-Suite will be taken and downloaded onto the Retirement Capital in-house server.
11. **Procedure – Hosted Systems**
    1. All hosted servers and storage are procured with a disaster recovery option that includes full backup/restore and replication to a DR server at a different site. Disaster recovery will be invoked in the event of a failure of the primary hosted system.

***Document Owner and Approval***

The Operations Director 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 Director (CISO) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature:

Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |