1. **Scope**

All cryptographic keys used by Retirement Capital and as listed in the schedule [ISMS-C REC 10.1.1](ISMS-C_REC_10.1.1.docx).

1. **Responsibilities**

The Director (CISO) is responsible for maintaining the schedule of required keys in line with the risk assessment, this procedure and evolving security environment.

Individual asset owners are responsible for ensuring that the required cryptographic control is applied.

1. **Procedure** [ISO27002 Clauses 10.1.2 and 18.1.5]
   1. Retirement Capital uses the highest quality cryptographic standard that can be utilised by both the originating and receiving systems that is operational practical. The company utilises three different categories of cryptographic key:

* Self-generated, unsigned keys for use with permanent internal VPNs.
* Self-generated, digitally signed keys.
* Third-party keys provided to Retirement Capital by other organisations.

The keys used adhere to the following standards:

* AES-256 based encryption
* SHA-512 and Diffi-hellman-2048 hashing algorithms
* PSK 32-bit password strings
  1. The keys are generated automatically from a Retirement Capital generated PSK key. This is generated randomly by the key generator application. The link for this is:

[https://www.dashlane.com/features/password-generator](https://www.google.com/url?q=https://www.dashlane.com/features/password-generator&sa=D&source=hangouts&ust=1562943630193000&usg=AFQjCNGd4kH1Uv0Axj77K8RO5EtKgjrxFA)

* 1. Retirement Capital has an SSL certificate that encompasses the entire Retirement Capital.co.uk domain. Cryptographic keys are generated and signed by GoDaddy and are requested on the administration page of GoDaddy’s dashboard.
  2. Retirement Capital’s policy is to not distribute cryptographic keys unless absolutely necessary. Where we need to distribute keys, this is always done of a secure email solution provided by Google G-Mail.
  3. Keys are stored in a secure key folder held on the server and replicated with Google Drive, accessible only to system administration. Keys are retained in line with [ISMS-C DOC 18.1.3a](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A18\ISMS-C_DOC_18.1.3A.docm).

***Document Owner and Approval***

The Director (CISO) 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 |
|  |  |  |  |
|  |  |  |  |