1. **Scope**

All cryptographic keys used by *{OrganisationName}* and as listed in the schedule [ISMS-C REC 10.1.1](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_REC_10.1.1.docm).

1. **Responsibilities**

The *{InfoSecManager}* 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**
   1. [Set out here exactly how you have decided to manage the use of cryptographic keys to support the policy requirements of the ISMS and taking account of the guidance given by Clauses 10.1.2 and 18.1.5 of ISO27002.]
   2. [*Key generation.*]
   3. [*Public key certificates*.]
   4. [*Key distribution, activation*.]
   5. [Retention of keys associated with encrypted archives or digital signatures in line with [ISMS-C DOC 18](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_18.docm).]
   6. [Etc.]

***Document Owner and Approval***

The *{InfoSecManager}* 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/specified]* members of staff on the *[corporate intranet*] and is published *[ ]*.

This procedure was approved by the *{ChiefInfoSecOfficer}* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |