1. **Scope**

All Retirement Capital’s information systems are subject to this procedure.

1. **Responsibilities**

The Director (CISO) performs the risk assessment to identify the type and level of audit logging and monitoring that might be required for each individual information asset.

Owners of individual assets are responsible for identifying and agreeing with the Director (CISO) the logging and monitoring capabilities of the assets they own and for having them configured to meet the requirements of the risk assessment.

The Director (CISO) is responsible for ensuring that the required monitoring activity takes place using, where necessary, outside contractors to confirm that configuration is in line with requirements of this procedure.

The Director (CISO) is responsible for configuring the information systems to meet the requirements of this procedure.

1. **Audit logging** [ISO27002 Clause 12.4.1]
   1. The servers/systems/devices/services for which user activity audit logging is configured, and the audit logging software that is deployed together with the schedule/matrix of audit log requirements and reporting regularity are set out in [ISMS-C REC 12.6.1](ISMS-C_DOC_12.6.1.docx).
   2. System administrators are prohibited from erasing or de-activating logs of their own activities.
   3. The schedule/matrix of audit log requirements and the audit log reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.
   4. The following data protection or privacy protection restrictions also apply: Data Protection Act 2018.
   5. The Retirement Capital deals with error and fault logging as follows:
   6. The Director (CISO) will investigate the issue, attempt to resolve it and then re-run the procedure. If the issue cannot be resolved, an alternative application will be investigated and sourced under change control.
2. **Monitoring system use** [ISO27002 Clause 12.7.1]
   1. The servers/systems/devices/services for which user activity monitoring is configured, together with the schedule/matrix of monitoring requirements and reporting regularity are set out in [ISMS-C REC 12.4.1](ISMS-C_DOC_12.4.1.docx).
   2. System administrators are prohibited from erasing or de-activating logs of their own activities.
   3. The schedule/matrix of monitoring requirements and the monitoring reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.
   4. The following data protection or privacy protection restrictions also apply: Data Protection Act 2018.
   5. Monitoring reports are reviewed monthly by the Chief Director (CISO), with the Director (CISO). Any evidence of system misuse is investigated further, and the disciplinary process may be invoked. See also control section 16.1 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx).
3. **Protection of log information** [ISO27002 Clause 12.4.2]
   1. Audit logging is configured as set out above.
   2. System administrators are prohibited from disabling logging activity; disabling audit logs or tampering with audit log information is treated as a serious offence in the disciplinary policy and may result in immediate dismissal.
   3. Google G-Suite provides a mechanism for logging any changes made to the systems, which is Retirement Capital’s primary information management system, and which is backed up onto an in-house server.
   4. Hosted servers are used for production systems only and access to them is restricted and all authorised sign-ons are logged. Any activity relating to changes within production servers must follow the change control procedure ISMS-C-DOC 12.1.2.
4. **Administrator and operator logs** [ISO27002 Clause 12.4.3]
   1. The servers/systems/devices/services for which administrator/operator activities are logged together with the schedule/matrix of administrator and operator activity log requirements and reporting regularity are set out in [ISMS-C REC 12.4.3](ISMS-C_REC_12.4.3.docx).
   2. System administrators are prohibited from erasing or de-activating logs of their own activities.
   3. The schedule/matrix of activity log requirements and the log reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.
   4. The following data protection or privacy protection restrictions also apply Data Protection Act 2018
   5. All administrative changes to the IT system are logged automatically by G-Suite or are managed under change control by the Director (CISO). No access to production systems is granted without a change control mandate. Failure to adhere to this policy may result in the dismissal of the member of staff infringing the policy.
5. **Clock synchronisation** [ISO27002 Clause 12.4.4]
   1. The clocks of all information systems within Retirement Capital are synchronised with Google clocks, as the Google cloud service G-Suite provides the primary IT systems.
   2. Throughout its information systems, the date stamp format used by Retirement Capital is: dd/mm/yyyy. The timestamp format used by Retirement Capital is hh:mm, applying the 24-hour clock.
   3. The clocks on all servers and all organisational information processing devices (including laptops, PDAs) are automatically synchronised with Google. The record of completed checks and any necessary corrections is forwarded to the Director (CISO).

***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 |
|  |  |  |  |
|  |  |  |  |