1. **Scope**

Access to all Retirement Capital’s information systems is controlled to restrict access to authorised users, including by secure log-on and session time-out procedures as detailed here.

1. **Responsibilities**

The IT Manager is responsible for maintenance of the secure log-on and session time-out procedure, and the configuration of the IT systems.

[ISMS-C DOC 9.2.3](ISMS-C_DOC_9.2.3.docx) describes the requirements of the password management system; ISMS-C DOC 9.2.3 provides the work instructions for user registration on Retirement Capital’s system.

Application owners are responsible for documenting any requirements for session time-outs or sensitive system isolation.

All users have responsibilities, as detailed in their User Agreements.

1. **Secure log-on Procedure**
2. The screen displays no system or application identifiers until the logon has been successfully completed.
3. The display on the logon screen includes a standard notice “This device is intended for the sole use of the named Retirement Capital employee, unauthorised use of this device is prohibited.”
4. The screen provides no help messages during the logon procedure.
5. The system validates the logon data only on completion of input and then, if there is an error, the system requires the user to try again.
6. The logon procedure limits the number of unsuccessful attempts allowed to six (and unsuccessful attempts are automatically recorded) and automatically disconnects the data link and rejects any further attempts without specific authorisation from the IT Manager, the user having first been positively identified by the IT Manager.
7. Password characters are hidden by symbols and always encrypted using the company encryption software before being sent across the network.
8. The configuration instructions are set out in work instruction ISMS C DOC 9.2.3a
9. **Prevention of misuse of information processing facilities** [ISO27002 Clause 13.1]
10. The logon screen above is also required to display a warning message at logon that indicates that the information processing facility is owned and operated by Retirement Capital and that unauthorised access is not permitted. Any user that continues the logon process explicitly confirms that they are authorised to access it and accepts that, in all instances of abuse of organisational facilities, the disciplinary policy will be invoked.
11. **Session time-out** [ISO27002 Clause 9.4.2]
12. Users are required to log out of sessions when they are finished.
13. Inactive sessions on any computer system must lock after 5 minutes and be shut down automatically when they have been inactive for a period of 60 minutes.
14. The configuration instructions for this are set out in work instruction ISMS C DOC 9.2.3a
15. **Sensitive system isolation** [ISO27002 Clause 9.4.1 and 13.1.3]
16. The system(s) which require an isolated environment, and their physical secure areas, are servers that process customer information.
17. Isolation for these systems is achieved by installing them in a secure hosting data centre within the UK.

***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 25th May 2019 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 |
|  |  |  |  |
|  |  |  |  |