1. **Scope**

The access rights of all users/user groups (as specified in [ISMS-C DOC 9.1.2](ISMS-C_DOC_9.1.2.docx)) to any of Retirement Capital’s information assets, systems or services are managed in accordance with this procedure. Retirement Capital operates a single sign-on process using XXX

1. **Responsibilities**

The IT Manager is responsible for administration of allocated and authorised user/user group access rights in conformity with the policy.

The HR Administrator is responsible for initiation and administration of new and changed user access requests (user agreements) and user training.

Department Manager are responsible for authorising access requests as being in line with business and organisational security policy and procedure.

Asset owners are responsible for classifying their information assets as being in conformity to the security requirements of the asset.

The Information Security Manager is responsible for reviewing user access rights in line with the review requirements of the ISMS.

1. **User registration and de-registration** [ISO27002 Clause 9.2.1]

User agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access. Retirement Capital ‘s standard User Agreement template is [ISMS-C DOC 9.2.1a](ISMS-C_DOC_9.2.1a.docx).

Every user’s proposed access rights are documented in a User Agreement, which details the systems/services/applications/information assets to which access is to be granted, together with the level of access that is to granted, taking into account the Access Control Policy ([ISMS-C DOC 9.1.1](ISMS-C_DOC_9.1.1.docx)) and the standard user profiles set out in [ISMS-C DOC 9.1.2](ISMS-C_DOC_9.1.2.docx). If a user is to be granted access rights other than the standard ones set out in ISMS-C DOC 9.1.2, then the specific additional authorisation of the Information Security Manager is also required.

The Manager and the IT Manager authorise access to the system/asset.

The User Agreement is then signed by the user and passed to the IT Manager and the username/user ID is created and administered in line with work instruction [ISMS-C DOC 9.2.3A](ISMS-C_DOC_9.2.3a.docx).

The IT Department maintains a list of authorised users, administers changes in access rights and removes users in line with ISMS-C DOC 9.2.3A.

The disciplinary policy will be invoked in cases of attempted unauthorised access.

1. **Privilege management** [ISO27002 Clauses 9.2.2 and 9.2.3]

Privileges are allocated to a different username than that allocated for normal use.

The available access privileges for each of Retirement Capital’s operating systems, applications and other systems, are identified and documented in ISMS-C DOC 9.1.2.

Privileges are allocated on a need-to-use and event-by-event (project) basis; the request for allocation of a privilege is initiated in an e-mail from the departmental manager or user concerned to the Information Security Manager which sets out the reasons why the privilege is required and the length of time for which it is required.

The Information Security Manager retains a log of all privileges authorised and allocated and checks on a monthly basis that they have been de-activated as specified in the original request.

The Information Security Manager checks using Google Suite reports on a monthly basis that unauthorised privileges have not been obtained.

1. **Username/Password management** [ISO27002 Clauses 9.2.4; 9.4.3]
   1. The company used XXX to provision accounts and manage access to core systems.
   2. Two Factor authentication (mobile phone app) is enabled for access to any company information via Google G-Suite.
   3. Usernames are the user’s email address and passwords must be generated in accordance with ISMS-C DOC 9.2.3A.

User password responsibilities are documented in their signed User Agreements (ISMS-C DOC 9.2.1a).

Users are initially issued with a unique temporary password (see ISMS-C DOC 9.2.3A) which they are forced to change at first logon.

Quarterly (90 day) password changes are enforced, re-use of passwords is prohibited for 3 subsequent attempts, and at least seven-character alphanumeric passwords are required.

Users who need to be issued with a replacement do so via a link which is authorised by the IT Manager once the user identified (see ISMS-C REC 9.4.2.

The default passwords on all new equipment are changed to conform with Retirement Capital’s password requirements (see ISMS-C DOC 9.2.1a) before the equipment is brought into service.

1. **Review of user access rights** [ISO27002 Clause 9.2.5]

Access rights are reviewed semi-annually, and their adequacy is confirmed; any changes that need to take place are actioned in line with ISMS-C DOC 9.2.3A.

User access rights are reviewed when a user’s role or location within Retirement Capital changes in any way. If the access rights need to change, a new user agreement is issued, in line with this procedure, setting out those access rights.

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