1. **Scope** [Components of ISO27002 Clauses 9.1.1; 9.2.1; 9.2.2; 9.2.3; 9.2.4]

All users/user groups that need to access organisational information have specific, pre-determined access rights to information, operating systems and applications that conform to and are restricted by the Access Control Policy ([ISMS-C DOC 9.1.1](ISMS-C_DOC_9.1.1.docx)).

1. **Responsibilities**

The IT Manager is responsible for creating, documenting and maintaining individual user/user group profiles that meet the requirements of the Access Control Policy (ISMS-C DOC 9.1.1).

User access administration is carried out in line with [ISMS-C DOC 9.2.3](ISMS-C_DOC_9.2.3.docx).

1. **Procedure**

Retirement Capital provides access to information based upon the function and seniority of the individual. In this way both the need to know and the authority levels are preserved.

The Function is a two letter abbreviation that describes the department or function to which the individual belongs and the seniority is described by a number ranging from 1 to 4, where 4 is the most senior.

An individual can be assigned multiple functions if required, but seniority will remain the same.

An individual with seniority of 4 will be automatically provided access to seniority levels 1-3.

Procedure ISMS-C DOC 9.2.3, details the administration of user rights, and work instruction [*ISMS-C DOC 12.1.1a*](../Control%20A12%20-%20operations%20security/ISMS-C_DOC_12.1.1a.docx)sets out the IT username and access rights administration.

1. **Classification of Users**

Users are also classified in terms of the level of access they need to information and systems. These classification levels, which are to be recorded in *user* agreements, are set out below:

| **Classification of data users** | | |
| --- | --- | --- |
| **Classification** | **Access Rights** | **Example** |
| 1 | Internet access and PUBLIC data | Clients |
| 2 | Internet access, PUBLIC & PRIVATE data | Junior staff |
| 3 | Internet access, PUBLIC & PRIVATE & RESTRICTED data | Senior Staff |
| 4 | Internet access, PUBLIC & PRIVATE, RESTRICTED & CONFIDNETIAL data | Directors |

1. **Privileges**

Privileges are allocated in line with the requirements of ISMS-C DOC 9.2.3.

Should a user or group of users require access to information from a different department or information that would normally above the person’s seniority, for example to assist with the creation of a customer proposal, then the following will take place:

1. The CISO (DIRECTOR) will determine if the request is valid and in the company interest.
2. The IT Department will create a PROJECT and allocate both users and information resources to that project.
3. The project members will have access to the information as required by business need regardless of classification level.
4. Access to information may be under specific conditions, for example: office-based access only.
5. When the project is completed, all users will be deleted from project access and ALL information stored under the project reference, at the security level of the most restricted document.
6. **User Authentication**

Users are authenticated at log-on by providing both their username and their password within the parameters of the log-on system (see [ISMS-C DOC 9.4.2](ISMS-C_DOC_9.4.2.docx)).

***Document Owner and Control***

The 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 14/11/2020 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 |
|  |  |  |  |
|  |  |  |  |