1. Retirement Capital controls access to information on the basis of business and security requirements.
2. Access control rules and rights to applications, expressed in standard user profiles, for each user / group of users are clearly stated, together with the business requirements met by the controls, in [ISMS-C DOC 9.1.2](ISMS-C_DOC_9.1.2.docx).
3. The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.
4. The access rights to each dataset take into account:
   1. The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems and network(s).
   2. Data protection (DPA 1988) and privacy legislation and any contractual commitments regarding access to data or services.
   3. The ‘need to know’ principle (i.e. access is granted at the minimum level necessary for the role).
   4. ‘Everything is generally forbidden unless expressly permitted’.
   5. Rules that must always be enforced and those that are only guidelines: at present all Data Protection requirements are rules that will be enforced without exception. Any changes to this requirement will result in a change to this policy.
   6. Labels (see control section 8.2 of the Manual).
   7. Prohibit through system controls (access rights, permissions, etc.) the ability for a user-initiated changes to user permissions.
   8. Enforcing through system controls (access rights, permissions, etc.) rules that require specific permission before enactment.
   9. Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.
5. Retirement Capital has standard user access profiles for common roles in Retirement Capital (see ISMS-C DOC 9.1.2).
6. Management of access rights across the network(s) is performed using the systems’ security dashboards and in line with [ISMS-C DOC 9.2.3](ISMS-C_DOC_9.2.3.docx).
7. User access requests, authorisation and administration are segregated as described in ISMS-C DOC 9.1.2.
8. User access requests are subject to formal authorisation, to periodic review (see control section 9.2.5 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) and to removal (see control section 9.2.6 of the Manual).

***Document Owner and Approval***

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on the corporate intranet.

This policy was approved by the Board of Directors on 14th November 2020 and is issued on a version-controlled basis under the signature of the Managing Director.

Signature: Date: 23/05/2019

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 23/05/2019 |
|  |  |  |  |
|  |  |  |  |