1. **Scope**

All system utilities that are part of organisational operating systems or applications are subject to this procedure. A matrix, by system, showing all the system utilities and how they are configured is shown below:

1. **Responsibilities**

Retirement Capital has a standard process for managing access to classified information([ISMS-C DOC 9.2.3](ISMS-C_DOC_9.2.3.docx)) based upon function (HR, development, etc.) and organisational level (staff, manager, director). However, there are specific activities whereby an individual may be granted privileged access to information, that would not normally be within their security level. For example: a sales bid team may need access to classified information concerning earlier bids. It is the responsibility of the department manager to request that the team or individual be granted privileged access and the responsibility of the Chief Information Security Officer (CISO (DIRECTOR)) to grant access, which is implemented by the IT Manager.

1. **Procedure**
   1. Should a Departmental Manager deem it necessary that an individual or team require access to information above their normal security level for the purposes of a specific project, a request must be made by email to the Chief Information Security Officer. This request must include as a minimum:

* Name(s) of individual(s) requiring access
* The information to which access is required
* The duration of the access requirement
* Business justification for the information access.

The CISO (DIRECTOR) will evaluate the risk of information access against the organisational benefits and determine whether to allow the access.

If access is to be granted, the IT Manager will:

* Create a new directory specifically for the project in question.
* Enable access (ISMS DOC 9.1.2) for those who access is requested.
* Copy the required information into the new directory.
* Classify the directory at the level of the highest document classification to be transferred according to [ISMS-C DOC 8.2](file:///C:\Users\Sarah\Documents\ISO%209001\ISO%2027001\Section6\RiskMngmt\Control-A8\ISMS-C_DOC_8.2.docm) (classification levels).
* Ensure that the users for whom access is requested are authenticated users as per ISMS DOC 9.3 (user registration).
* When the project is over or the duration of access has expired, the IT Manager will store the project directory in the appropriate location and remove access to the privileged individuals.

***Document Owner and Approval***

The IT 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 |
|  |  |  |  |
|  |  |  |  |