

## EXAMPLE – Procedure IS-6 Access Control and Rights Review

### 1 People and Purpose

This procedure applies to the Chief Technical Officer (CTO), ICT Manager and workers (employees and contractors) that manage Information and Communication Technology (ICT) resources. It specifies the policy and review procedure for access to our ICT resources, and complements Procedure BM-1.

This procedure covers ISO 27001, Annex A, Controls A.9.1.1 and A.9.2.5.

### 2 Access Control Policy

This section covers ISO 27001, Annex A, Control A.9.1.1.

#### 2-1 Policy Statement

We provide to each worker, only the access to our ICT resources that they require, to do their work.

#### 2-2 How we implement it

*Procedure BM-1 – Starting and Finishing a Role together with Form 11 – Induction – Logins.*

### 3 Access Rights Review Procedure

This section covers ISO 27001, Annex A, Control A.9.2.5.

- (1) An ICT Management Review Meeting reviews users' access rights to our ICT resources at least once per year.
- (2) If any of the following situations occur:
  - (a) We introduce a new ICT resource;
  - (b) We change an ICT resource, which necessitates a review of a user's access;
  - (c) We remove an ICT resource;
  - (d) The worker or worker's line manager requests a change to the worker's access;

do the following procedure:

- (i) The ICT Manager and/or line manager review(s) a worker's access to ICT resources, recorded on Form 11;
- (ii) The ICT Manager and/or other workers that administer ICT resources, make(s) any required changes.
- (iii) The ICT Manager records any changes on Form 11.

<b>NOTE</b> If a worker starts or finishes a role, refer to Procedure BM-1.
---