ILT

ASSET MANAGEMENT

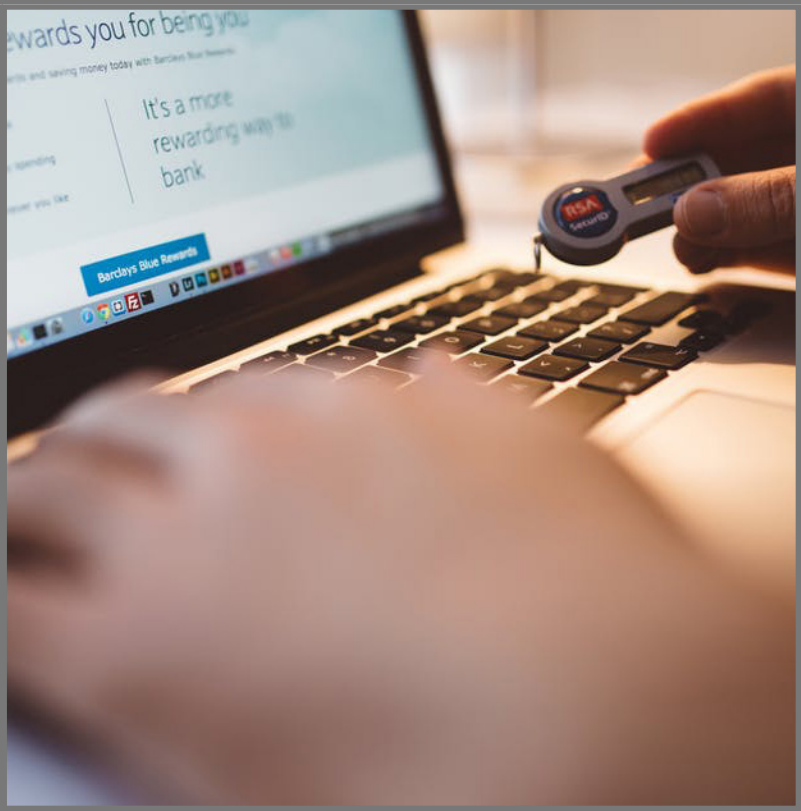

Table of Contents

Version Control

Document Reference: Il7 Security Access Control Policy

Version	Description of change	Date	Author	Approver
0.1				

1. Introduction

An ever-increasing threat environment requires any organization to implement appropriate measures to protect it from information security related threats and to manage its information assets. Il7 has updated its policy status to align itself with ISO/IEC 27001:2013 in line with the approved Information Security Management System (ISMS), October 2018.

2. Purpose

The purpose of the Information Security Asset Management Policy is to ensure there are mechanisms within each Operating Company as well as Il7 to:

- Record all assets.
- Assign ownership to assets.
- Ensure the acceptable use of information assets.
- Ensure the return of information assets when business need requires.

3. Audience and Scope

This policy presents the outcomes that must be delivered through standards and procedures implemented by all Il7 Operating Companies including Head Office for Information Asset Management

It is applicable and binding to all Il7 and Operating Companies employees, including Executive Management, permanent staff, contract and temporary employees.

The audience for this policy is Il7 and the Operating Companies.

4. Review

This asset management policy shall be established, documented and reviewed based on business and information security requirements. It is to be reviewed annually and updated accordingly.

5. Ownership – Responsibility For Assets

Reference ISO 27001 A.8

Inventory of assets

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

Reference ISO 27001 A.8.1.1

The organisation should identify assets relevant in the lifecycle of information and document their importance. The lifecycle of information should include creation, processing, storage, transmission, deletion and destruction. Documentation should be maintained in dedicated or existing inventories as appropriate.

The asset inventory should be accurate, up to date, consistent and aligned with other inventories.

For each of the identified assets, ownership of the asset should be assigned and the classification should be identified.

Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons.

ISO/IEC 27005[11] provides examples of assets that might need to be considered by the organisation when identifying assets. The process of compiling an inventory of assets is an important prerequisite of risk management (see also ISO/IEC 27000 and ISO/IEC 27005[11]).

Ownership of assets

Reference ISO 27001 A.8.1.2

Assets maintained in the inventory shall be owned. Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners.

A process to ensure timely assignment of asset ownership is usually implemented. Ownership should be assigned when assets are created or when assets are transferred to the organisation. The asset owner should be responsible for the proper management of an asset over the whole asset lifecycle.

The asset owner should:

- ensure that assets are inventoried
- ensure that assets are appropriately classified and protected
- define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies
- ensure proper handling when the asset is deleted or destroyed.

The identified owner can be either an individual or an entity who has approved management responsibility for controlling the whole lifecycle of an asset. The identified owner does not necessarily have any property rights to the asset.

Routine tasks may be delegated, e.g. to a custodian looking after the assets on a daily basis, but the responsibility remains with the owner.

In complex information systems, it may be useful to designate groups of assets which act together to provide a particular service. In this case the owner of this service is accountable for the delivery of the service, including the operation of its assets.

Acceptable use of assets

Reference ISO 27001 A.8.1.3

Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. Employees and external party users using or having access to the organisation's assets should be made aware of the information security requirements of the organisation's assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility.

Return of assets

Reference ISO 27001 A.8.1.4

All employees and external party users shall return all organisational assets in their possession upon termination of their employment, contract or agreement.

The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organisation.

In cases where an employee or external party user purchases the organisation's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organisation and securely erased from the equipment.

In cases where an employee or external party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organisation. During the notice period of termination, the organisation should control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.