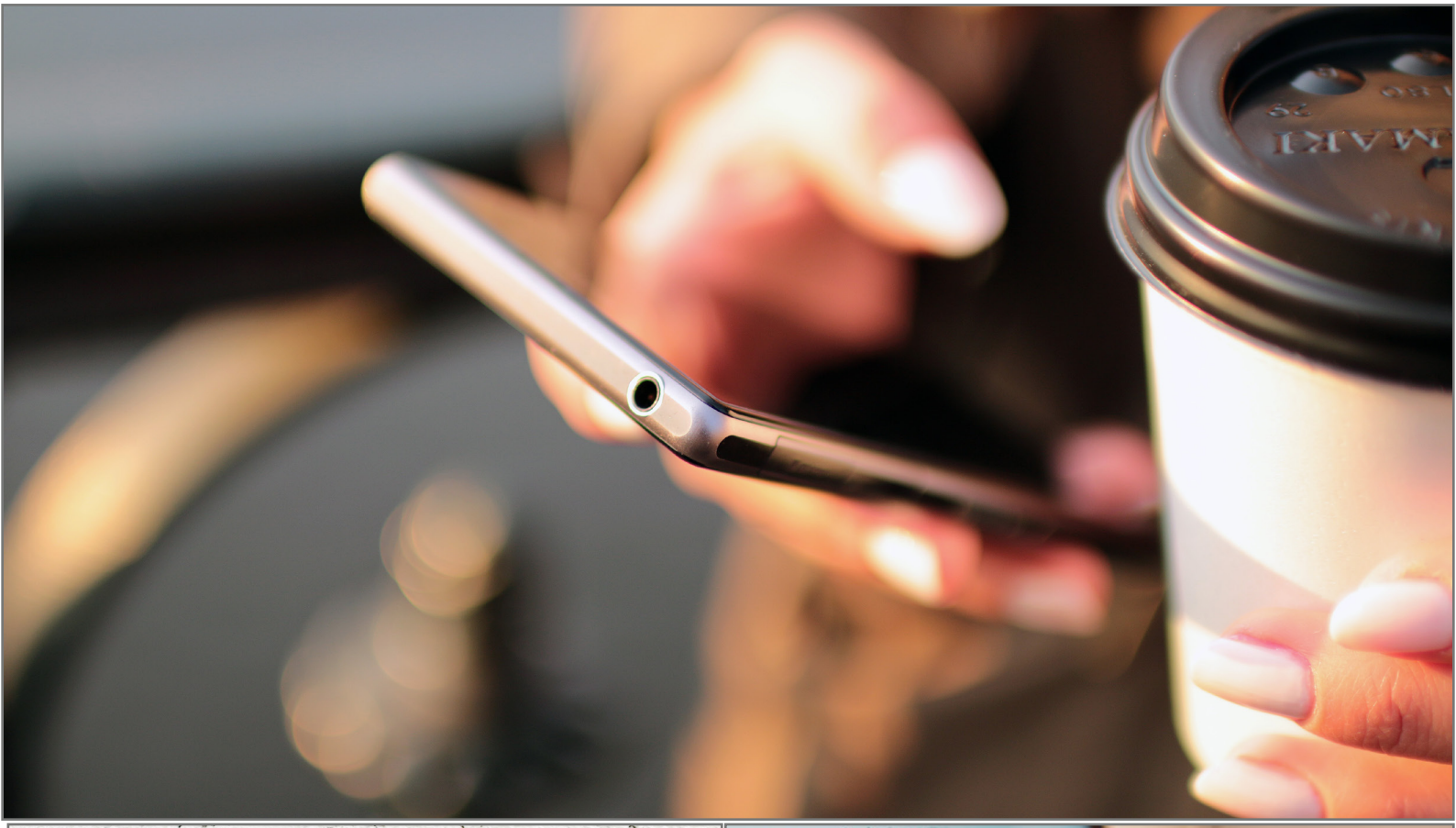
MOBILE & TELEWORKING



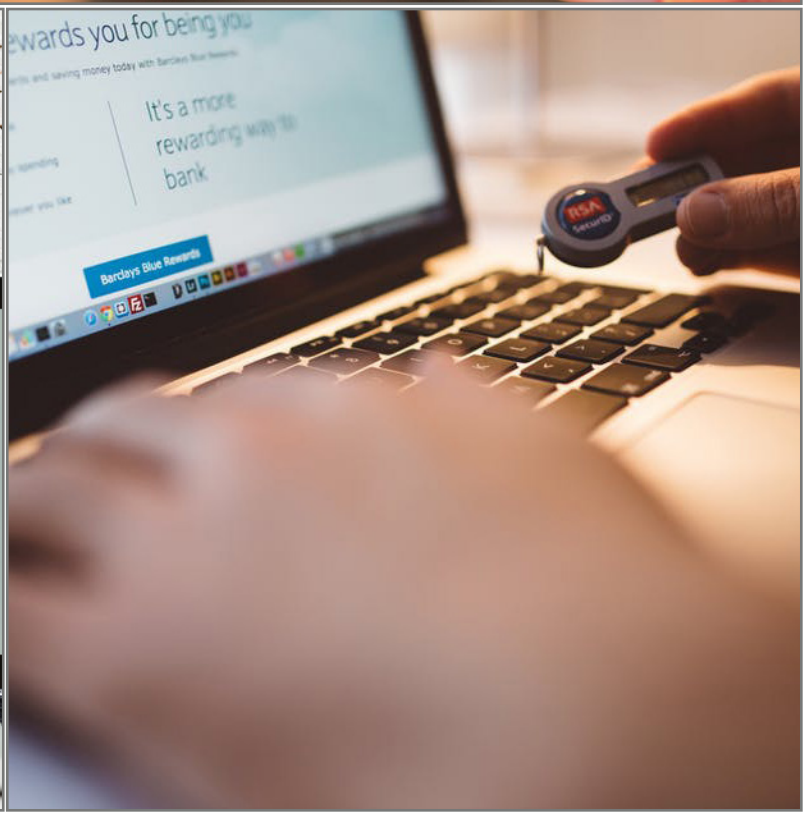


Table of Contents

Version Control

Document Reference: Il7 Security Mobile & Teleworking 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 control access to 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 Mobile & Teleworking Policy is to ensure there are mechanisms to:

- Allow the secure administration of the Mobile access to and from Il7 information assets.
- To allow secure use of mobile assets and teleworking facilities for Il7 personnel to carry out their required business functions through access to applications, productivity tools and communications facilities.
- To prevent unauthorised access to systems and facilities in order to safeguard the Confidentiality Integrity and Availability of Il7's information Assets.

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 Mobile and Teleworking.

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

5. Mobile Device Policy

Reference ISO 27001 A6.2.1

All Operating Companies shall follow this policy and supporting security measures shall be adopted to manage risks introduced by using mobile devices.

When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments. The mobile device policy should consider:

- registration of mobile devices.
- requirements for physical protection.
- restriction of software installation.
- requirements for mobile device software versions and for applying patches.
- restriction of connection to information services.
- access controls.
- cryptographic techniques.
- malware protection.
- remote disabling, erasure or lockout.
- backups.
- usage of web services and web apps.

Care should be taken when using mobile devices in public places, meeting rooms and other unprotected areas. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these devices, e.g. using cryptographic techniques (see Clause 10) and enforcing use of secret authentication information.

Mobile devices should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organisation should be established for cases of theft or loss of mobile devices. Devices carrying important, sensitive or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices.

Training should be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented. Where the mobile device policy allows the use of privately owned mobile devices, the policy and related security measures should also consider:

- separation of private and business use of the devices, including using software to support such separation and protect business data on a private device.
- providing access to business information only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organisation in case of theft or loss of the device or when no longer authorized to use the service. This policy needs to take account of privacy legislation.

- Mobile device wireless connections are similar to other types of network connection but have important differences that should be considered when identifying controls. Typical differences are:
    - some wireless security protocols are immature and have known weaknesses.
    - information stored on mobile devices may not be backed-up because of limited network bandwidth or because mobile devices may not be connected at the times when backups are scheduled.
- Mobile devices generally share common functions, e.g. networking, internet access, e-mail and file handling, with fixed use devices. Information security controls for the mobile devices generally consist of those adopted in the fixed use devices and those to address threats raised by their usage outside the organisation's premises.

6. Teleworking Policy

Reference ISO 27001 A6.2.2

All Operating Companies shall follow this policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as "telecommuting", "flexible workplace", "remote work" and "virtual work" environments.

Procedures are to be in place to define the conditions and restrictions for using teleworking. Where deemed applicable and allowed by law, the following matters should be considered:

- the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment.
- the proposed physical teleworking environment.
- the communications security requirements, taking into account the need for remote access to the organisation's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system.
- the provision of virtual desktop access that prevents processing and storage of information on privately owned equipment.
- the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends.
- the use of home networks and requirements or restrictions on the configuration of wireless network services.
- policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment.
- access to privately owned equipment (to verify the security of the machine or during an investigation), which may be prevented by legislation.
- software licensing agreements that are such that organisations may become liable for licensing for client software on workstations owned privately by employees or external party users.
- malware protection and firewall requirements.

The following guidelines and arrangements to be considered should include:

- the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organisation is not allowed.
- a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access.
- the provision of suitable communication equipment, including methods for securing remote access.
- physical security.
- rules and guidance on family and visitor access to equipment and information.
- the provision of hardware and software support and maintenance.
- the provision of insurance.
- the procedures for backup and business continuity.
- audit and security monitoring.
- revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

7. Responsibility for Mobile and Teleworking Assets

Ownership of assets

Operating Companies should identify assets relevant and document their importance. Assets associated with mobile and teleworking shall be identified, and an inventory of these assets shall be drawn up and maintained. The inventory shall include authorisation, relevant dates and responsibilities. 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 where relevant the classification should be identified.

Acceptable use of assets

Rules for the acceptable use of mobile and teleworking assets 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

All employees and external party users shall return the 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.