COMMUNICATIONS STRATEGY

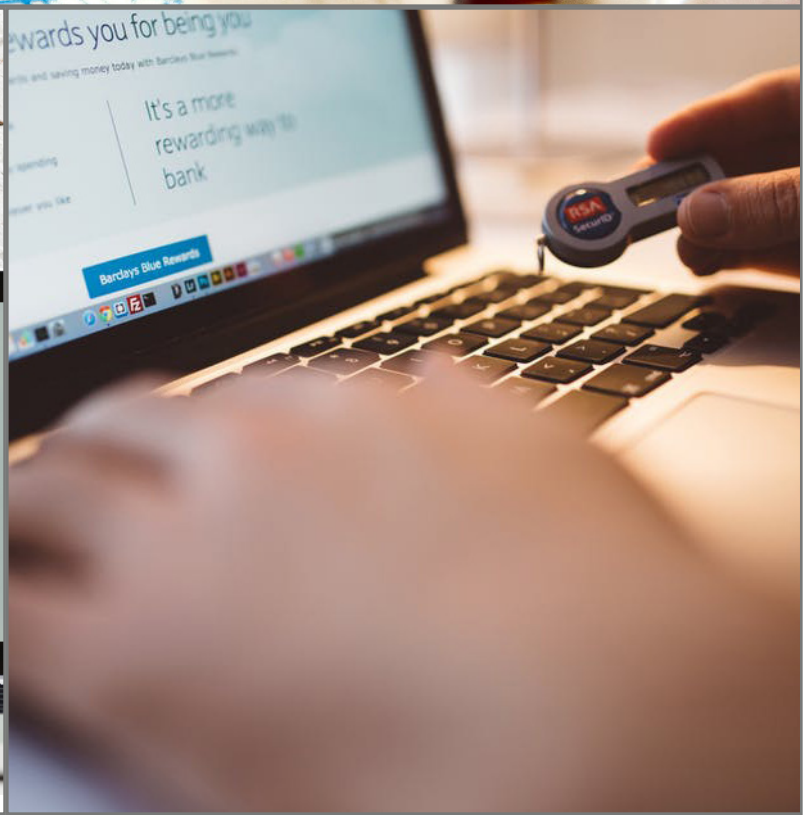

Table of Contents

Version Control

Document Reference: IL7 Security Security Communications Security Policy

Version	Description of change	Date	Author	Approver
0.1				

1. Introduction

An ever-increasing threat environment requires any organisation to implement appropriate measures to protect it from information security related threats and, in particular, to introduce communications security procedures. IL7 Security 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 Communications Security Policy is to ensure there are standards for:

- Communications Security.
- Network Management.
- Information Transfer.
- Electronic Messaging and Email.

3. Audience and Scope

This policy presents the outcomes that must be delivered through standards and procedures implemented by all IL7 Security Operating Companies including Head Office for ITC Operations – In Service Delivery

It is applicable and binding to all IL7 Security and Operating Companies employees, including Executive Management, permanent staff, contract and temporary employees.

The audience for this policy is IL7 Security and the Operating Companies.

4. Review

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

5. Network Management

Reference ISO 27001 A13.1

Network Controls

Reference ISO 27001 A13.1.1

Networks shall be managed and controlled to protect information in systems and applications.

Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. In particular, the following items should be considered:

- responsibilities and procedures for the management of networking equipment should be established.
- operational responsibility for networks should be separated from computer operations where appropriate (see ISO 27001 6.1.2).
- special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (see ISO 27001 Clause 10 and 13.2). special controls may also be required to maintain the availability of the network services and computers connected.
- appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security.
- management activities should be closely coordinated both to optimize the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure.
- systems on the network should be authenticated.
- systems connection to the network should be restricted.

Additional information on network security can be found in ISO/IEC 27033. [15][16][17][18][19].

Security of network services

Reference ISO 27001 A13.1.2

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels and management requirements, should be identified. The organisation should ensure that network service providers implement these measures.

Network services include the provision of connections, private network services and value added networks and managed network security solutions such as firewalls and intrusion detection systems.

These services can range from simple unmanaged bandwidth to complex value-added offerings. Security features of network services could be:

a) technology applied for security of network services, such as authentication, encryption and network connection controls.

b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules.

c) procedures for the network service usage to restrict access to network services or applications, where necessary.

Segregation in networks

Reference ISO 27001 A13.1.3

Groups of information services, users and information systems shall be segregated on networks.

One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organisational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organisational units). The segregation can be done using either physically different networks or by using different logical networks (e.g.virtual private networking). The perimeter of each domain should be well defined. Access between network domains is allowed, but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance

with the access control policy (see ISO 27001 9.1.1), access requirements, value and classification of information processed and also take account of the relative cost and performance impact of incorporating suitablegateway technology.

Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls policy (see ISO 27001 13.1.1) before granting access to internal systems.

The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organisation's internal network when properly implemented.

Networks often extend beyond organisational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organisation's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

6. Information Transfer

Reference ISO 27001 A13.2

Information transfer policies and procedures

Reference ISO 27001 A13.2.1

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

The procedures and controls to be followed when using communication facilities for information transfer should consider the following items:

- procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction.
- procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications.
- procedures for protecting communicated sensitive electronic information that is in the form of an attachment.
- policy or guidelines outlining acceptable use of communication facilities.
- personnel, external party and any other user's responsibilities not to compromise the organisation, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorised purchasing, etc..
- use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information.
- retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations.
- controls and restrictions associated with using communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses.
- advising personnel to take appropriate precautions not to reveal confidential information.
- not leaving messages containing confidential information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling.
- advising personnel about the problems of using facsimile machines or services, namely:
    - unauthorized access to built-in message stores to retrieve messages.
    - deliberate or accidental programming of machines to send messages to specific numbers.
    - sending documents and messages to the wrong number either by misdialling or using the wrong stored number.

In addition, personnel should be reminded that they should not have confidential conversations in public places or over insecure communication channels, open offices and meeting places. Information transfer services should comply with any relevant legal requirements.

Information transfer may occur through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile and video.

Software transfer may occur through a number of different mediums, including downloading from the Internet and acquisition from vendors selling off-the-shelf products.

The business, legal and security implications associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls should be considered.

Agreements on information transfer

Reference ISO 27001 A13.2.2

Agreements shall address the secure transfer of business information between the organisation and external parties.

Information transfer agreements should incorporate the following:

- management responsibilities for controlling and notifying transmission, dispatch and receipt.
- procedures to ensure traceability and non-repudiation.
- minimum technical standards for packaging and transmission.
- escrow agreements.
- courier identification standards.
- responsibilities and liabilities in the event of information security incidents, such as loss of data.
- use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of
- the labels is immediately understood and that the information is appropriately protected.
- technical standards for recording and reading information and software.
- any special controls that are required to protect sensitive items, such as cryptography.
- maintaining a chain of custody for information while in transit.
- acceptable levels of access control.

Policies, procedures and standards should be established and maintained to protect information and physical media in transit, and should be referenced in such transfer agreements. The information security content of any agreement should reflect the sensitivity of the business information involved.

Electronic messaging

Reference ISO 27001 A13.2.3

Information involved in electronic messaging shall be appropriately protected.

Information security considerations for electronic messaging should include the following:

- protecting messages from unauthorized access, modification or denial of service commensurate with the classification scheme adopted by the organisation.
- ensuring correct addressing and transportation of the message.
- reliability and availability of the service.
- legal considerations, for example requirements for electronic signatures.
- obtaining approval prior to using external public services such as instant messaging, social networking or file sharing.
- stronger levels of authentication controlling access from publicly accessible networks.

There are many types of electronic messaging such as email, electronic data interchange and social networking which play a role in business communications.

Confidentiality or nondisclosure agreements

Reference ISO 27001 A13.2.4

Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to external parties or employees of the organisation. Elements should be selected or added in consideration of the type of the other party and its permissible access or handling of confidential information. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

- a definition of the information to be protected (e.g. confidential information).
- expected duration of an agreement, including cases where confidentiality might need to be
- maintained indefinitely.
- required actions when an agreement is terminated.
- responsibilities and actions of signatories to avoid unauthorized information disclosure.
- ownership of information, trade secrets and intellectual property, and how this relates to the
- protection of confidential information.
- the permitted use of confidential information and rights of the signatory to use information.
- the right to audit and monitor activities that involve confidential information.
- process for notification and reporting of unauthorized disclosure or confidential information leakage.

- terms for information to be returned or destroyed at agreement cessation.
- expected actions to be taken in case of a breach of the agreement.

Based on an organisation's information security requirements, other elements may be needed in a confidentiality or non-disclosure agreement.

Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which they apply. Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements. Confidentiality and non-disclosure agreements protect organisational information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorized manner. There may be a need for an organisation to use different forms of confidentiality or non-disclosure agreements in different circumstances.