COMPLIANCE

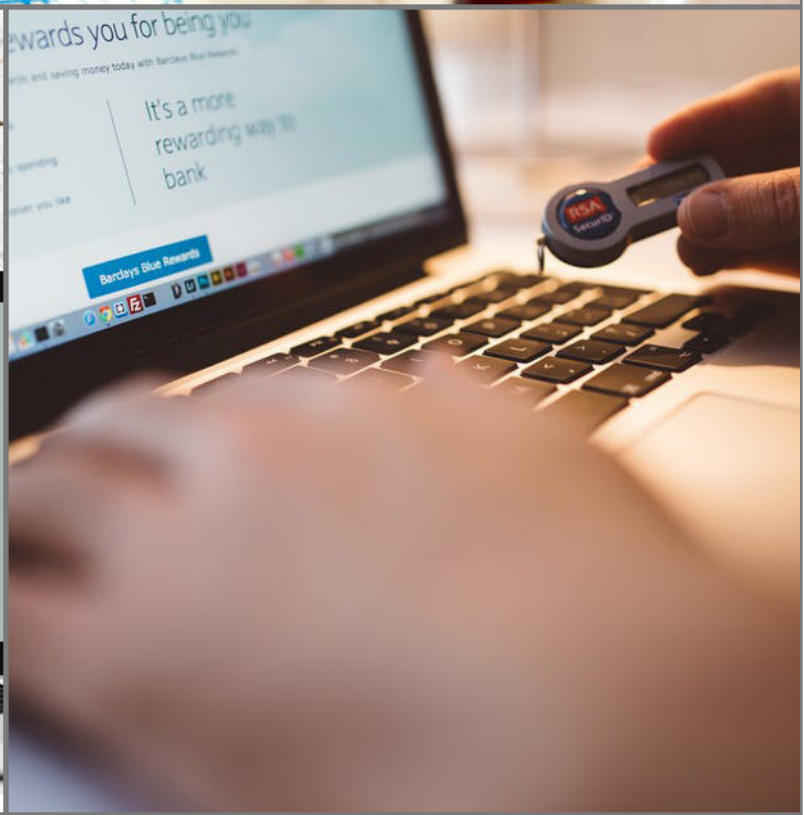

Table of Contents

Version Control

Document Reference: IL7 Security Security – Compliance 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 to introduce security procedures to ensure there is compliance with law and standards. 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 Compliance Security Policy is to ensure there are standards for:

- Legal, contractual and regulatory compliance.
- IPR and Data Protection are recognised.
- Independent review – both technical and procedural.
- Control of Cryptography.
- Protection of Records.

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 Legal and Regulatory Compliance.

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 Compliance 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. Compliance with legal and contractual requirements

Reference ISO 27001 A18.1

Identification of applicable legislation and contractual requirements

Reference ISO 27001 A18.1.1

All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organisation.

The specific controls and individual responsibilities to meet these requirements should also be defined and documented.

Managers should identify all legislation applicable to their organisation in order to meet the requirements for their type of business. If the organisation conducts business in other countries, managers should consider compliance in all relevant countries.

Intellectual property rights

Reference ISO 27001 A18.1.2

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

The following guidelines should be considered to protect any material that may be considered intellectual property:

- publishing an intellectual property rights compliance policy which defines the legal use of software and information products.
- acquiring software only through known and reputable sources, to ensure that copyright is not violated.
- maintaining awareness of policies to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them.
- maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights.
- maintaining proof and evidence of ownership of licences, master disks, manuals, etc..
- implementing controls to ensure that any maximum number of users permitted within the licence is not exceeded.
- carrying out reviews that only authorized software and licensed products are installed.
- providing a policy for maintaining appropriate licence conditions.
- providing a policy for disposing of or transferring software to others.
- complying with terms and conditions for software and information obtained from public networks.
- not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law.
- not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences. Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. The importance and awareness of intellectual property rights should be communicated to staff for software developed by the organisation.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organisation or that is licensed or provided by the developer to the organisation, can be used. Copyright infringement can lead to legal action, which may involve fines and criminal proceedings.

Protection of records

Reference ISO 27001 A18.1.3

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.

When deciding upon protection of specific organisational records, their corresponding classification based on the organisation's classification scheme, should be considered. Records should be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of allowable storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys and programs associated with encrypted

archives or digital signatures (see Clause 10), should also be stored to enable decryption of the records for the length of time the records are retained.

Consideration should be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations.

Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change.

Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.

The system of storage and handling should ensure identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organisation.

To meet these record safeguarding objectives, the following steps should be taken within an organisation:

- guidelines should be issued on the retention, storage, handling and disposal of records and information.
- a retention schedule should be drawn up identifying records and the period of time for which they should be retained.
- an inventory of sources of key information should be maintained.

Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organisation operates within statutory or regulatory rules, to ensure defence against potential civil or criminal action or to confirm the financial status of an organisation to shareholders, external parties and auditors. National law or regulation may set the time period and data content for information retention.

Privacy and protection of personally identifiable information

Reference ISO 27001 A18.1.4

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

An organisation's data policy for privacy and protection of personally identifiable information should be developed and implemented. This policy should be communicated to all persons involved in the processing of personally identifiable information.

Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organisational measures to protect personally identifiable information should be implemented.

ISO/IEC 29100[25] provides a high-level framework for the protection of personally identifiable information within information and communication technology systems. A number of countries have introduced legislation placing controls on the collection, processing and transmission of personally identifiable information (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing and disseminating personally identifiable information, and may also restrict the ability to transfer personally identifiable information to other countries.

Regulation of cryptographic controls

Reference ISO 27001 A18.1.5

Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

The following items should be considered for compliance with the relevant agreements, laws and regulations:

- restrictions on import or export of computer hardware and software for performing cryptographic functions.
- restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it.
- restrictions on the usage of encryption.
- mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with relevant legislation and regulations. Before encrypted information or cryptographic controls are moved across jurisdictional borders, legal advice should also be taken.

6. Independent review of information security

Reference ISO 27001 A18.2.1

The organisation's approach to managing information security and implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

Management should initiate the independent review. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organisation's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives. Such a review should be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or an external party organisation specializing in such reviews. Individuals carrying out these reviews should have the appropriate skills and experience. The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained. If the independent review identifies that the organisation's approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies (see 5.1.1), management should consider corrective actions.

ISO/IEC 27007[12], "Guidelines for information security management systems auditing" and ISO/IEC TR 27008[13], "Guidelines for auditors on information security controls" also provide guidance for carrying out the independent review.

Compliance with security policies and standards

Reference ISO 27001 A18.2.2

Managers shall regularly review the compliance of information processing and procedures within the area of responsibility with the appropriate security policies, standards and any other security requirements.

Managers should identify how to review that information security requirements defined in policies, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

- identify the causes of the non-compliance.
- evaluate the need for actions to achieve compliance.
- implement appropriate corrective action.
- review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews when an independent review takes place in the area of their responsibility.

Technical compliance review

Reference ISO 27001 A18.2.3

Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards.

Technical compliance should be reviewed preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed. If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable. Any technical compliance review should only be carried out by competent, authorized persons or under the supervision of such persons.

Technical compliance reviews involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance review requires specialist technical expertise.

Compliance reviews also cover, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for inspecting how effective the controls are in preventing unauthorized access due to these vulnerabilities. Penetration testing and vulnerability assessments provide a snapshot of a system in a specific

state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s). Penetration testing and vulnerability assessments are not a substitute for risk assessment. ISO/IEC TR 27008[13] provides specific guidance regarding technical compliance reviews.