SYSTEM PROTECTION SECURITY

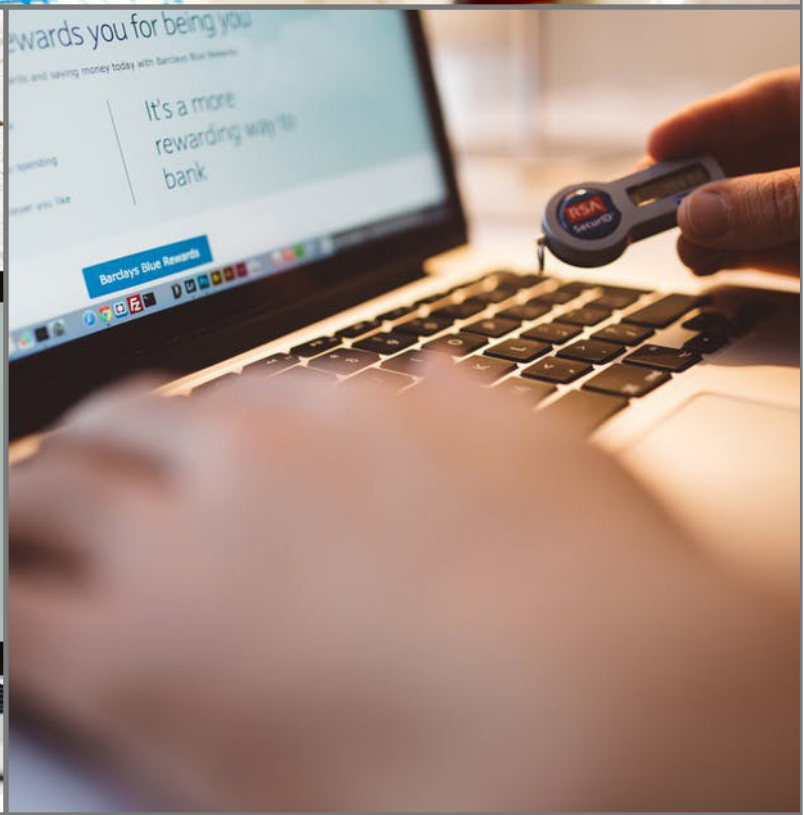

Table of Contents

Version Control

Document Reference: IL7 Security Security – System Protection 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 security procedures to protect essential systems. 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 Information System Protection Security Policy is to ensure there are standards for:

- System Acquisition.
- System Development.
- System Maintenance.

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 protecting essential systems – including all systems connected to essential systems.

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 Systems Protection 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. Security requirements of information systems

Reference ISO 27001 A14.1

Information security requirements analysis and specification

Reference ISO 27001 A14.1.1

The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

Information security requirements should be identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds. Results of the identification should be documented and reviewed by all stakeholders.

Information security requirements and controls should reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security.

Identification and management of information security requirements and associated processes should be integrated in early stages of information systems projects. Early consideration of information security requirements, e.g. at the design stage can lead to more effective and cost efficient solutions.

Information security requirements should also consider:

- the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements.
- access provisioning and authorization processes, for business users as well as for privileged or technical users.
- informing users and operators of their duties and responsibilities.
- the required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity.
- requirements derived from business processes, such as transaction logging and monitoring, nonrepudiation requirements.
- requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems.

For applications that provide services over public networks or which implement transactions, the dedicated controls should be considered.

If products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls should be reconsidered prior to purchasing the product.

Available guidance for security configuration of the product aligned with the final software / service stack of that system should be evaluated and implemented.

Criteria for accepting products should be defined e.g. in terms of their functionality, which will give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition. Additional functionality should be reviewed to ensure it does not introduce unacceptable additional risks.

Securing application services on public networks

Reference ISO 27001 A14.1.2

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.

Information security considerations for application services passing over public networks should include the following:

- the level of confidence each party requires in each other's claimed identity, e.g. through authentication.
- authorization processes associated with who may approve contents of, issue or sign key transactional documents.
- ensuring that communicating partners are fully informed of their authorizations for provision or use of the service.
- determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts, e.g. associated with tendering and contract processes.
- the level of trust required in the integrity of key documents.
- the protection requirements of any confidential information.
- the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts.
- the degree of verification appropriate to verify payment information supplied by a customer.
- selecting the most appropriate settlement form of payment to guard against fraud.
- the level of protection required to maintain the confidentiality and integrity of order information.
- avoidance of loss or duplication of transaction information.
- liability associated with any fraudulent transactions.
- insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls (see ISO 27001 Clause 10), taking into account compliance with legal requirements (see ISO 27001 Clause 18, especially see ISO 27001 18.1.5 for cryptography legislation).Application service arrangements between partners should be supported by a documented agreement which commits both parties to the agreed terms of services, including details of authorization (see ISO 27001 b) above).

Resilience requirements against attacks should be considered, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service.

Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public. Therefore, detailed risk assessments and proper selection of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer. Application services can make use of secure authentication methods, e.g. using public key cryptography and digital signatures (see ISO 27001 Clause 10) to reduce the risks. Also, trusted third parties can be used, where such services are needed.

Protecting application services transactions

Reference ISO 27001 A14.1.3

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

Information security considerations for application service transactions should include the following:

- the use of electronic signatures by each of the parties involved in the transaction.
- all aspects of the transaction, i.e. ensuring that:
    - user's secret authentication information of all parties are valid and verified.
    - the transaction remains confidential.
    - privacy associated with all parties involved is retained.
- communications path between all involved parties is encrypted.
- protocols used to communicate between all involved parties are secured.
- ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organisational intranet, and not retained and exposed on a storage medium directly accessible from the Internet.
- where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

The extent of the controls adopted needs to be commensurate with the level of the risk associated with each form of application service transaction. Transactions may need to comply with legal and regulatory requirements in the jurisdiction which the transaction is generated from, processed via, completed at or stored in.

6. Security in development and support processes

Reference ISO 27001 A14.2

Secure development policy

Reference ISO 27001 A14.2.1

Rules for the development of software and systems shall be established and applied to developments within the organisation.

Secure development is a requirement to build up a secure service, architecture, software and system. Within a secure development policy, the following aspects should be put under consideration:

- security of the development environment.
- guidance on the security in the software development lifecycle:
    - security in the software development methodology.
    - secure coding guidelines for each programming language used.
- security requirements in the design phase.
- security checkpoints within the project milestones.
- secure repositories.
- security in the version control.
- required application security knowledge.
- developers' capability of avoiding, finding and fixing vulnerabilities.

Secure programming techniques should be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or were not consistent with current best practices. Secure coding standards should be considered and where relevant mandated for use. Developers should be trained in their use and testing and code review should verify their use. If development is outsourced, the organisation should obtain assurance that the external party complies with these rules for secure development (see ISO 27001 14.2.7).

Development may also take place inside applications, such as office applications, scripting, browsers and databases.

System change control procedures

Reference ISO 27001 A14.2.2

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

Formal change control procedures should be documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts. Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control and managed implementation. This process should include a risk assessment, analysis of the impacts of changes and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work and that formal agreement and approval for any change is obtained.

Wherever practicable, application and operational change control procedures should be integrated (see ISO 27001 12.1.2). The change control procedures should include but not be limited to:

- maintaining a record of agreed authorization levels.
- ensuring changes are submitted by authorized users.

- reviewing controls and integrity procedures to ensure that they will not be compromised by the changes.
- identifying all software, information, database entities and hardware that require amendment.
- identifying and checking security critical code to minimize the likelihood of known security weaknesses.
- obtaining formal approval for detailed proposals before work commences.
- ensuring authorized users accept changes prior to implementation.
- ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of.
- maintaining a version control for all software updates.
- maintaining an audit trail of all change requests.
- ensuring that operating documentation (see ISO 27001 12.1.1) and user procedures are changed as necessary to remain appropriate.
- ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

Changing software can impact the operational environment and vice versa. Good practice includes the testing of new software in an environment segregated from both the production and development environments (see ISO 27001 12.1.4). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.

Where automatic updates are considered, the risk to the integrity and availability of the system should be weighed against the benefit of speedy deployment of updates. Automated updates should not be used on critical systems as some updates can cause critical applications to fail.

Technical review of applications after operating platform changes

Reference ISO 27001 A14.2.3

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.

This process should cover:

- review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes.
- ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation.
- ensuring that appropriate changes are made to the business continuity plans.

Operating platforms include operating systems, databases and middleware platforms. The control should also be applied for changes of applications.

Restrictions on changes to software packages

Reference ISO 27001 A14.2.4

Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

As far as possible and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified the following points should be considered:

- the risk of built-in controls and integrity processes being compromised.
- whether the consent of the vendor should be obtained.
- the possibility of obtaining the required changes from the vendor as standard program updates.
- the impact if the Organisation becomes responsible for the future maintenance of the software as a result of changes.
- compatibility with other software in use.

If changes are necessary, the original software should be retained and the changes applied to a designated copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

Secure system engineering principles

Reference ISO 27001 A14.2.5

Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

Secure information system engineering procedures based on security engineering principles should be established, documented and applied to in-house information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology should be analysed for security risks and the design should be reviewed against known attack patterns.

These principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They should also be regularly reviewed to ensure that they remain up-to-date in terms of combating any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

The established security engineering principles should be applied, where applicable, to outsourced information systems through the contracts and other binding agreements between the organisation and the supplier to whom the organisation outsources. The

organisation should confirm that the rigour of suppliers' security engineering principles is comparable with its own.

Application development procedures should apply secure engineering techniques in the development of applications that have input and output interfaces. Secure engineering techniques provide guidance on user authentication techniques, secure session control and data validation, sanitisation and elimination of debugging codes.

Secure Development Environment

Reference ISO 27001 A14.2.6

Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

A secure development environment includes people, processes and technology associated with system development and integration.

Organisations should assess risks associated with individual system development efforts and establish secure development environments for specific system development efforts, considering:

- sensitivity of data to be processed, stored and transmitted by the system.
- applicable external and internal requirements, e.g. from regulations or policies.
- security controls already implemented by the organisation that support system development.
- trustworthiness of personnel working in the environment (see ISO 27001 7.1.1).
- the degree of outsourcing associated with system development.
- the need for segregation between different development environments.
- control of access to the development environment.
- monitoring of change to the environment and code stored therein.
- backups are stored at secure offsite locations.
- control over movement of data from and to the environment.

Once the level of protection is determined for a specific development environment, organisations should document corresponding processes in secure development procedures and provide these to all individuals who need them.

Outsourced development

Reference ISO 27001 A14.2.7

The organisation shall supervise and monitor the activity of outsourced system development.

Where system development is outsourced, the following points should be considered across the organisation's entire external supply chain:

- licensing arrangements, code ownership and intellectual property rights related to the outsourced content.

- contractual requirements for secure design, coding and testing practices.
- provision of the approved threat model to the external developer.
- acceptance testing for the quality and accuracy of the deliverables.
- provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality.
- provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery.
- provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities.
- escrow arrangements, e.g. if source code is no longer available.
- contractual right to audit development processes and controls.
- effective documentation of the build environment used to create deliverables.
- the organisation remains responsible for compliance with applicable laws and control efficiency verification.

System security testing

Reference ISO 27001 A14.2.8

New and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected (see ISO 27001 14.1.1 and 14.1.9). The extent of testing should be in proportion to the importance and nature of the system.

System acceptance testing

Reference ISO 27001 A14.2.9

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

System acceptance testing should include testing of information security requirements (see ISO 27001 14.1.1 and 14.1.2) and adherence to secure system development practices (see ISO 27001 14.2.1). The testing should also be conducted on received components and integrated systems. Organisations can leverage automated tools, such as code analysis tools or vulnerability scanners, and should verify the remediation of security related defects.

7. Test data

Reference ISO 27001 A14.3

Protection of test data

Reference ISO 27001 A14.3.1

Test data shall be selected carefully, protected and controlled.

The use of operational data containing personally identifiable information or any other confidential information for testing purposes should be avoided. If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content should be protected by removal or modification (see ISO/IEC 29101[26]).

The following guidelines should be applied to protect operational data, when used for testing purposes:

- the access control procedures, which apply to operational application systems, should also apply to test application systems.
- there should be separate authorization each time operational information is copied to a test environment.
- operational information should be erased from a test environment immediately after the testing is complete.
- the copying and use of operational information should be logged to provide an audit trail.

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data.