SUPPLY CHAIN

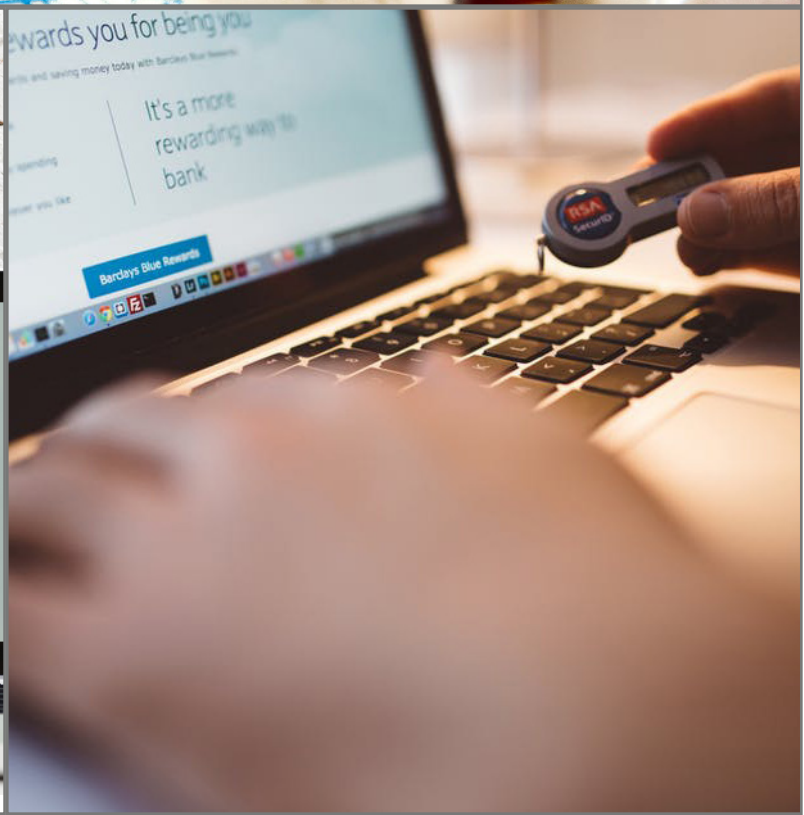

Table of Contents

Version Control

Document Reference: IL7 Security Security – Supply Chain 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 manage the supply chain. 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 Supply Chain Security Policy is to ensure there are standards for:

- Supplier Relationships.
- Supply Chain Management.
- Delivery Management.

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 Supplier Relationships and Delivery Management.

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 Supply Chain Management 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. Supply Chain Relationships

Reference ISO 27001 A15.1

Information security policy for supplier relationships

Reference ISO 27001 A15.1.1

Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.

The organisation should identify and mandate information security controls to specifically address supplier access to the organisation's information in a policy. These controls should address processes and procedures to be implemented by the organisation, as well as those processes and procedures that the organisation should require the supplier to implement, including:

- identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organisation will allow to access its information.
- a standardised process and lifecycle for managing supplier relationships.
- defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access.
- minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organisation's business needs and requirements and its risk profile.
- processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation.
- accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party.
- types of obligations applicable to suppliers to protect the organisation's information.
- handling incidents and contingencies associated with supplier access including responsibilities of both the organisation and suppliers.
- resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party.
- awareness training for the organisation's personnel involved in acquisitions regarding applicable policies, processes and procedures.
- awareness training for the organisation's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organisation's systems and information.
- conditions under which information security requirements and controls will be documented in an agreement signed by both parties.
- managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organisation needs to be aware that the legal or contractual responsibility for protecting information remains with the organisation.

Addressing security within supplier agreements

Reference ISO 27001 A15.1.2

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organisation and the supplier regarding both parties' obligations to fulfil relevant information security requirements. The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

- description of the information to be provided or accessed and methods of providing or accessing the information.
- classification of information according to the organisation's classification scheme. if necessary also mapping between the organisation's own classification scheme and the classification scheme of the supplier.
- legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met.
- obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing.
- rules of acceptable use of information, including unacceptable use if necessary.
- either explicit list of supplier personnel authorized to access or receive the organisation's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organisation's information by supplier personnel.
- information security policies relevant to the specific contract.
- incident management requirements and procedures (especially notification and collaboration during incident remediation).
- training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures.
- relevant regulations for sub-contracting, including the controls that need to be implemented.
- relevant agreement partners, including a contact person for information security issues.
- screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern.

- right to audit the supplier processes and controls related to the agreement.
- defect resolution and conflict resolution processes.
- supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report.
- supplier's obligations to comply with the organisation's security requirements.

The agreements can vary considerably for different organisations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers). The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

ICT supply chain

Reference ISO 27001 A15.1.3

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

- defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships.
- for information and communication technology services, requiring that suppliers propagate the organisation's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organisation.
- for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers.
- implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements.
- implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organisation especially if the top tier supplier outsources aspects of product or service components to other suppliers.
- obtaining assurance that critical components and their origin can be traced throughout the supply chain.
- obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features.
- defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organisation and suppliers.

- implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements. The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organisations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. organisations can influence information and communication technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain.

Information and communication technology supply chain as addressed here includes cloud computing services.

6. Supplier service delivery management

Reference ISO 27001 A15.2

Monitoring and review of supplier services

Reference ISO 27001 A15.2.1

Organisations shall regularly monitor, review and audit supplier service delivery.

Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organisation and the supplier to:

- monitor service performance levels to verify adherence to the agreements.
- review service reports produced by the supplier and arrange regular progress meetings as required by the agreements.
- conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified.
- provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures.
- review supplier audit trails and records of information security events, operational problems,
- failures, tracing of faults and disruptions related to the service delivered.
- resolve and manage any identified problems.
- review information security aspects of the supplier's relationships with its own suppliers.

- ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organisation should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organisation should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organisation should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

Managing changes to supplier services

Reference ISO 27001 A15.2.2

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

The following aspects should be taken into consideration:

- changes to supplier agreements.
- changes made by the organisation to implement:
    - enhancements to the current services offered.
    - development of any new applications and systems.
    - modifications or updates of the organisation's policies and procedures.
    - new or changed controls to resolve information security incidents and to improve security.
- changes in supplier services to implement:
    - changes and enhancement to networks.
    - use of new technologies.
    - adoption of new products or newer versions/releases.
    - new development tools and environments.
    - changes to physical location of service facilities.
    - change of suppliers.
    - sub-contracting to another supplier.