OPERATIONAL SECURITY

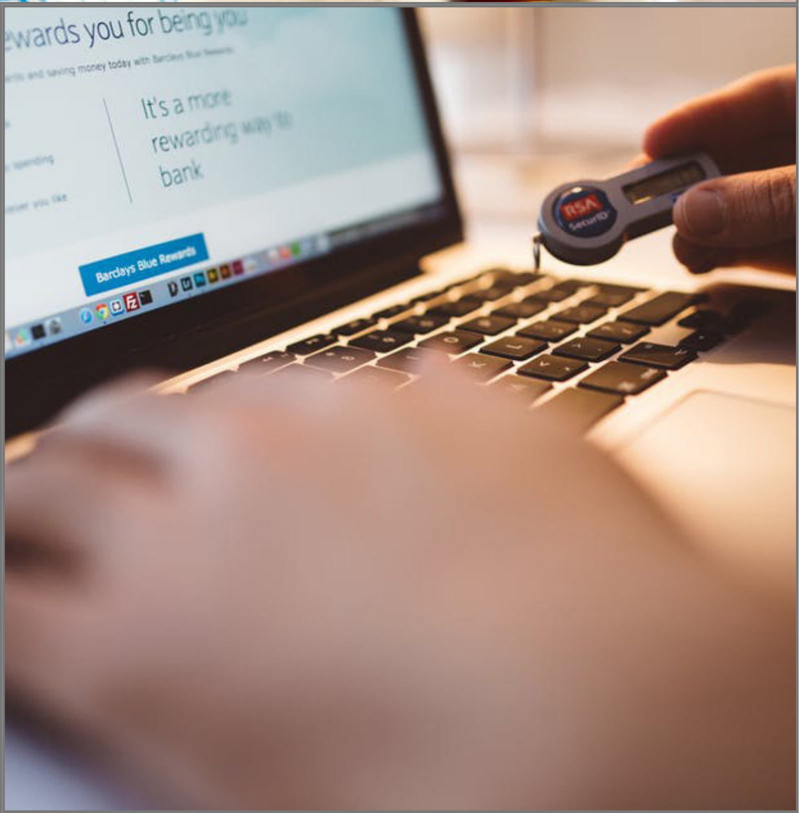

Table of Contents

Version Control

Document Reference: IL7 Security Security Operational 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 operational 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 Information Operational Security Policy is to ensure there are standards for:

- Documented Procedures.
- Change Control.
- Malware Protection.
- Protective Monitoring.
- Introducing new software.
- Vulnerability and Patch Management.
- Information Systems' Audit.

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 Operational 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. Operational Procedures and Responsibilities

Reference ISO 27001 A12.1

Documented Operational Procedures

Reference ISO 27001 A12.1.1

Operating procedures shall be documented and made available to all users who need them.

Documented procedures should be prepared for operational activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management and safety.

The operating procedures should specify the operational instructions, including:

- the installation and configuration of systems.
- processing and handling of information both automated and manual.
- backup (ISO 27001 ISO27001 12.3).
- scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times.
- instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (ISO 27001 ISO27001 9.4.4).
- support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties.
- special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs (ISO 27001 ISO27001 ISO 27001 8.3 and 11.2.7).
- system restart and recovery procedures for use in the event of system failure.
- the management of audit-trail and system log information (ISO 27001 ISO27001 ISO 27001 12.4).
- monitoring procedures.

Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

Change Management

Reference ISO 27001 A12.1.2

Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled.

In particular, the following items should be considered:

- identification and recording of significant changes.
- planning and testing of changes.

- assessment of the potential impacts, including information security impacts, of such changes.
- formal approval procedure for proposed changes.
- verification that information security requirements have been met.
- communication of change details to all relevant persons.
- fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
- provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident (ISO 27001 ISO27001 ISO 27001 16.1).

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained.

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications (ISO 27001 ISO27001 ISO 27001 14.2.2).

Capacity Management

Reference ISO 27001 A12.1.3

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

Capacity requirements should be identified, taking into account the business criticality of the concerned system. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organisation’s information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs. therefore managers should monitor the utilization of key system resources. They should identify trends in usage, particularly in relation to business applications or information systems management tools.

Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action. Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. Examples of managing capacity demand include:

- deletion of obsolete data (disk space).
- decommissioning of applications, systems, databases or environments.
- optimising batch processes and schedules.
- optimising application logic or database queries.

- denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

This control also addresses the capacity of the human resources, as well as offices and facilities.

Separation of development, testing and operational environments

Reference ISO 27001 A12.1.4

Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.

The level of separation between operational, testing, and development environments that is necessary to prevent operational problems should be identified and implemented.

The following items should be considered:

- rules for the transfer of software from development to operational status should be defined and documented.
- development and operational software should run on different systems or computer processors and in different domains or directories.
- changes to operational systems and applications should be tested in a testing or staging environment prior to being applied to operational systems.
- other than in exceptional circumstances, testing should not be done on operational systems.
- compilers, editors and other development tools or system utilities should not be accessible from operational systems when not required.
- users should use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error.
- sensitive data should not be copied into the testing system environment unless equivalent controls are provided for the testing system (ISO 27001 ISO27001 ISO 27001 14.3).

Development and testing activities can cause serious problems, e.g. unwanted modification of files or system environment or system failure. There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the operational environment.

Where development and testing personnel have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud or introduce untested or malicious code, which can cause serious operational problems.

Development and testing personnel also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, testing and operational environments is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data (ISO 27001 ISO27001 14.3 for the protection of test data).

6. Protection from Malware

Reference ISO 27001 A12.2

Controls against malware

Reference ISO 27001 A12.2.1

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls. The following guidance should be considered:

- establishing a formal policy prohibiting the use of unauthorized software (ISO 27001 ISO27001 12.6.2 and 14.2.).
- implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting).
- implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting).
- establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken.
- reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management (ISO 27001 ISO27001 12.6).
- conducting regular reviews of the software and data content of systems supporting critical business processes. the presence of any unapproved files or unauthorized amendments should be formally investigated.
- installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis. the scan carried out should include:
  - scan any files received over networks or via any form of storage medium, for malware before use.
  - scan electronic mail attachments and downloads for malware before use. this scan should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organisation.
  - scan web pages for malware.
- defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks.
- preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements (ISO 27001 ISO27001 12.3).
- implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware.

- implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative. managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware. all users should be made aware of the problem of hoaxes and what to do on receipt of them.
- isolating environments where catastrophic impacts may result.

The use of two or more software products protecting against malware across the information processing environment from different vendors and technology can improve the effectiveness of malware protection.

Care should be taken to protect against the introduction of malware during maintenance and emergency procedures, which may bypass normal malware protection controls. Under certain conditions, malware protection might cause disturbance within operations. Use of malware detection and repair software alone as a malware control is not usually adequate and commonly needs to be accompanied by operating procedures that prevent introduction of malware.

7. Logging and Monitoring

Reference ISO 27001 A12.4

Event logging

Reference ISO 27001 A12.4.1

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

Event logs should include, when relevant:

- user IDs.
- system activities.
- dates, times and details of key events, e.g. log-on and log-off.
- device identity or location if possible and system identifier.
- records of successful and rejected system access attempts.
- records of successful and rejected data and other resource access attempts.
- changes to system configuration.
- use of privileges.
- use of system utilities and applications.
- files accessed and the kind of access.
- network addresses and protocols.
- alarms raised by the access control system.
- activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.
- records of transactions executed by users in applications.
- Event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken (ISO 27001 18.1.4).

Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (ISO 27001 12.4.3).

Protection of log information

Reference ISO 27001 A12.4.2

Logging facilities and log information shall be protected against tampering and unauthorised access.

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

- alterations to the message types that are recorded.
- log files being edited or deleted.
- storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence (ISO 27001 16.1.7).

System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the copying of appropriate message types automatically to a second log, or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real-time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.

Administrator and Operator Logs

Reference ISO 27001 A12.4.3

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control, therefore it is necessary to protect and review the logs to maintain accountability for the privileged users.

An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

Clock Synchronisation

Reference ISO 27001 A12.4.4

The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source.

External and internal requirements for time representation, synchronisation and accuracy should be documented. Such requirements can be legal, regulatory, contractual requirements, standards compliance or requirements for internal monitoring. A standard reference time for use within the organisation should be defined.

The organisation's approach to obtaining a reference time from external source(s) and how to synchronise internal clocks reliably should be documented and implemented.

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol can be used to keep all of the servers in synchronisation with the master clock.

8. Control of Operational Software

Reference ISO 27001 A12.5

Installation of software on operational systems

Reference ISO 27001 A12.5.1

Procedures shall be implemented to control the installation of software on operational systems.

The following guidelines should be considered to control changes of software on operational systems:

- the updating of the operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorization (see ISO 27001 9.4.5).
- operational systems should only hold approved executable code and not development code or compilers.
- applications and operating system software should only be implemented after extensive and successful testing. the tests should cover usability, security, effects on other systems and user friendliness
- and should be carried out on separate systems (see ISO 27001 12.1.4). it should be ensured that all corresponding program source libraries have been updated.
- a configuration control system should be used to keep control of all implemented software as well as the system documentation.
- a rollback strategy should be in place before changes are implemented.
- an audit log should be maintained of all updates to operational program libraries.

- previous versions of application software should be retained as a contingency measure.
- old versions of software should be archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data are retained in archive.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organisation should consider the risks of relying on unsupported software. Any decision to upgrade to a new release should consider the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version. Software patches should be applied when they can help to remove or reduce information security weaknesses (see ISO 27001 12.6).

Physical or logical access should only be given to suppliers for support purposes when necessary and with management approval. The supplier’s activities should be monitored (see ISO 27001 15.2.1).

Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

9. Technical vulnerability management

Reference ISO 27001 A12.6

Management of Technical Vulnerabilities

Reference ISO 27001 A12.6.1

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A current and complete inventory of assets (see Clause 8) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organisation responsible for the software.

Appropriate and timely action should be taken in response to the identification of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

- the organisation should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required.

- information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list. these information resources should be updated based on changes in the inventory or when other new or useful resources are found.
- a timeline should be defined to react to notifications of potentially relevant technical vulnerabilities.
- once a potential technical vulnerability has been identified, the organisation should identify the associated risks and the actions to be taken. such action could involve patching of vulnerable systems or applying other controls.
- depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures.
- if a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch).
- patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated. if no patch is available, other controls should be considered, such as:
    - turning off services or capabilities related to the vulnerability.
    - adapting or adding access controls, e.g. firewalls, at network borders.
    - increased monitoring to detect actual attacks.
    - raising awareness of the vulnerability.
- an audit log should be kept for all procedures undertaken.
- the technical vulnerability management process should be regularly monitored and evaluated to ensure its effectiveness and efficiency.
- systems at high risk should be addressed first.
- an effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur.
- define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organisation should evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see ISO27001 12.1.2 and 14.2.2). Vendors are often under significant pressure to release patches as soon as possible. Therefore, there is a possibility that a patch does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling a patch cannot be easily achieved once the patch has been applied.

If adequate testing of the patches is not possible, e.g. because of costs or lack of resources, a delay in patching can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031[14] can be beneficial.

10. Information Systems' Audit

Reference ISO 27001 A12.7

Information systems audit controls

Reference ISO 27001 A12.7.1

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

The following guidelines should be observed:

- audit requirements for access to systems and data should be agreed with appropriate management.
- the scope of technical audit tests should be agreed and controlled.
- audit tests should be limited to read-only access to software and data.
- access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.
- requirements for special or additional processing should be identified and agreed.
- audit tests that could affect system availability should be run outside business hours.
- all access should be monitored and logged to produce a reference trail.