PERSONNEL MANAGEMENT

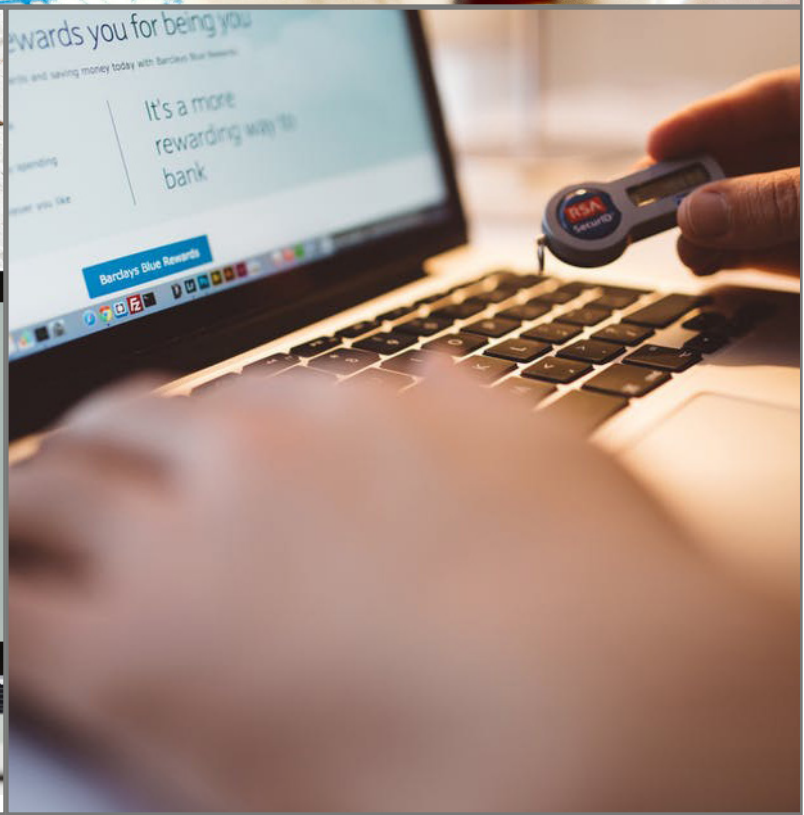

Table of Contents

Version Control

Document Reference: IL7 Security Information Security Personnel Management 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 appoint reliable responsible and informed personnel to carry out, use, operate and manage its information assets. 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 Security Personnel Management Policy is to ensure there are mechanisms to:

- Recruit reliable, responsible personnel are recruited.
- Management and Personnel remain aware of their security responsibilities towards assets.
- That IT security can rely on HR for the execution of appropriate recourse in the event of a breach of these responsibilities.
- That there is a co-ordinated approach to personnel leaving or changing employment and such does not undermine the security of information assets.

3. Audience and Scope

This policy outlines the outcomes that must be delivered by standards and procedures implemented and followed by all IL7 Security Operating Companies, including Head Office, when managing personnel, before, during and after their period of employment.

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 Personnel Management (HR) policy shall be established, documented and reviewed based on business and information security requirements. It is to be reviewed annually and updated accordingly.

5. Pre-employment Policy

Reference ISO 27001 A7.1

Screening Policy

Reference ISO 27001 A7.1.1

Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Verification should take into account all relevant privacy, protection of personally identifiable information and employment-based legislation, and should, where permitted, include the following:

- availability of satisfactory character references, e.g. one business and one personal.
- a verification (for completeness and accuracy) of the applicant's curriculum vitae.
- confirmation of claimed academic and professional qualifications.
- independent identity verification (passport or similar document).
- more detailed verification, such as credit review or review of criminal records.

When an individual is hired for a specific information security role, organisations should make sure the candidate:

- has the necessary competence to perform the security role.
- can be trusted to take on the role, especially if the role is critical for the organisation.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and particularly if these are handling confidential information, e.g. financial information, sensitive or highly confidential information, the organisation should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out.

A screening process should also be ensured for contractors. In these cases, the agreement between the organisation and the contractor should specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

Information on all candidates being considered for positions within the organisation should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

Terms and conditions of employment

Reference ISO 27001 A7.1.2

The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security.

The contractual obligations for employees or contractors should reflect the organisation's policies for information security in addition to clarifying and stating:

- that all employees and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities.
- the employee's or contractor's legal responsibilities and rights, e.g. regarding copyright laws or data
- protection legislation.
- responsibilities for the classification of information and management of organisational assets associated with information, information processing facilities and information services handled by the employee or contractor.
- responsibilities of the employee or contractor for the handling of information received from other companies or external parties.
- actions to be taken if the employee or contractor disregards the organisation's security requirements. Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

The organisation should ensure that employees and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organisation's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

A code of conduct may be used to state the employee's or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organisation's equipment and facilities, as well as reputable practices expected by the organisation. An external party, (e.g. an Employment of Contracting Agency) with which a contractor is associated, can be required to enter into contractual arrangements on behalf of the contracted individual.

6. During Employment

Reference ISO 27001 A7.2

Management responsibilities

Reference ISO 27001 A7.2.1

Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation. Management responsibilities should include ensuring that employees and contractors:

- are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems.
- are provided with guidelines to state information security expectations of their role within the organisation.
- are motivated to fulfil the information security policies of the organisation.
- achieve a level of awareness on information security relevant to their roles and responsibilities within the organisation.
- conform to the terms and conditions of employment, which includes the organisation's information security policy and appropriate methods of working.
- continue to have the appropriate skills and qualifications and are educated on a regular basis.
- are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").
- Management should demonstrate support of information security policies, procedures and controls, and act as a role model.

If employees and contractors are not made aware of their information security responsibilities, they can cause considerable damage to an organisation. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

Poor management can cause personnel to feel undervalued resulting in a negative information security impact on the organisation. For example, poor management can lead to information security being neglected or potential misuse of the organisation's assets.

Policy Awareness

Reference ISO 27001 A5.1.1

All employees shall be aware of the corporate "information security policy" which is approved by the board and which sets out the organisation's approach to managing its information security objectives. Employees should be aware of corporate responsibilities and goals including:

- business strategy.
- regulations, legislation and contracts.
- the current and projected information security threat environment.

Corporate information security policy contains statements concerning:

- definition of information security, objectives and principles to guide all activities relating to information security.
- assignment of general and specific responsibilities for information security management to defined roles.
- processes for handling deviations and exceptions.

All employees should be aware of corporate policy on:

- access control (see ISO/IEC 27001:2013 Clause 9).
- information classification (and handling) (see ISO/IEC 27001:2013 8.2).

- physical and environmental security (see ISO/IEC 27001:2013 Clause 11).
- end user topics such as:
    - acceptable use of assets (see ISO/IEC 27001:2013 8.1.3).
    - clear desk and clear screen (see ISO/IEC 27001:2013 11.2.9).
    - information transfer (see ISO/IEC 27001:2013 13.2.1).
    - mobile devices and teleworking (see ISO/IEC 27001:2013 6.2).
    - restrictions on software installations and use (see ISO/IEC 27001:2013 12.6.2).
- backup (see ISO/IEC 27001:2013 12.3).
- information transfer (see ISO/IEC 27001:2013 13.2).
- protection from malware (see ISO/IEC 27001:2013 12.2).
- management of technical vulnerabilities (see ISO/IEC 27001:2013 12.6.1).
- cryptographic controls (see ISO/IEC 27001:2013 Clause 10).j) communications security (see ISO/IEC 27001:2013 Clause 13).
- privacy and protection of personally identifiable information (see ISO/IEC 27001:2013 18.1.4). l) supplier relationships (see ISO/IEC 27001:2013 Clause 15).

These policies should be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme" (see ISO/IEC 27001:2013 7.2.2).

Information security awareness, education and training

Reference ISO 27001 A7.2.2

All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.

An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security, and the means by which those responsibilities are discharged. An information security awareness programme should be established in line with the organisation's information security policies and relevant procedures, taking into consideration the organisation's information to be protected and the controls that have been implemented to protect the information.

The awareness programme should include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters.

The awareness programme should be planned, taking into consideration the employees' roles in the organisation, and, where relevant, the organisation's expectation of the awareness of contractors. The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors. The awareness programme should also be updated regularly so it stays in line with organisational policies and procedures, and should be

built on lessons learnt from information security incidents. Awareness training should be performed as required by the organisation's information security awareness programme. Awareness training can use different delivery media including classroom-based, distance

learning, web-based, self-paced and others. Information security education and training should also cover general aspects such as:

- stating management's commitment to information security throughout the organisation.
- the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements.
- personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organisation and external parties.
- basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks).
- contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

Information security education and training should take place periodically. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.

The organisation should develop the education and training programme in order to conduct the education and training effectively. The programme should be in line with the organisation's information security policies and relevant procedures, taking into consideration the organisation's information to be protected and the controls that have been implemented to protect the information. The programme should consider different forms of education and training, e.g. lectures or self-studies.

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why'. It is important that employees understand the aim of information security and the potential impact, positive and negative, on the organisation of their own behaviour. Awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills. An assessment of the employees' understanding could be conducted at the end of an awareness, education and training course to test knowledge transfer.

Disciplinary Process - Recourse

Reference ISO 27001 A7.2.3

There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

The disciplinary process should not be commenced without prior verification that an information security breach has occurred.

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of information security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

The disciplinary process should also be used as a deterrent to prevent employees from violating the organisation's information security policies and procedures and any other information security breaches. Deliberate breaches may require immediate actions.

The disciplinary process can also become a motivation or an incentive if positive sanctions are defined for remarkable behaviour with regards to information security.

7. Termination or Change of Employment

Reference ISO 27001 A7.3

Termination or change of employment responsibilities

Reference ISO 27001 A7.3.1

The registration and de-registration of employees for the purpose of access to IT facilities shall be bound by their business needs and the policy of how this is to be managed is contained in the corporate Access Control Policy.

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.

The communication of termination responsibilities should include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment continuing for a defined period after the end of the employee's or contractor's employment.

Responsibilities and duties still valid after termination of employment should be contained in the employee's or contractor's terms and conditions of employment.

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

The human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the information security aspects of the relevant procedures. In the case of a contractor provided through an external party, this termination process is undertaken by the external party in accordance with the contract between the organisation and the external party.

It may be necessary to inform employees, customers or contractors of changes to personnel and operating arrangements.

8. Acceptable Use Standards

The following is a list of acceptable use standards that should be introduced by all operating companies (OC) to govern the behaviour of their employees:

1. All authorised users must conform to the regulations laid out in the company's policies applying to all users of the network.
2. All authorised users must conform to any all requirements laid out by the following Acts/policies:

    - Computer Misuse Act (1990).
    - Data Protection Act (1998).
    - Chest Code of conduct.
    - Regulation of Investigatory Powers Act (2000).
    - The Counter-Terrorism and Security Act 2015.

3. Only desktop computers, laptop computers, Tablets/PDAs, or Internet-capable cellular devices ("Authorised Devices") may be registered for connection to the network. No other devices, including all network equipment (switches, hubs, wireless routers etc) may be attached to the network, either directly or indirectly, unless these have first been approved for connection by the IT Department.
4. Any authorised device that will be connected to the network must be registered through the OC On-line Registration System, to the authorised user of that device.
5. Any device connected to the network must be configured solely as a client. No device may offer services on the network, including (but not limited to) email servers, web servers, ftp servers and wireless access.
6. Peer-to-peer applications may not be used on the network. The only exception to this rule is Skype which must be configured according to the guidance.
7. The use/misuse of authorised devices connected to the network is the responsibility of the individual to whom the device has been registered.
8. Authorised users are permitted to use only network and host addresses that have been issued to them by the OC.
9. Any device connected to the network must run up-to-date anti-virus protection (assuming a/v protection exists for that platform) and be up to date with the appropriate operating system security patches. Updates should be performed daily and at a minimum, must be performed weekly.
10. All authorised users must conform to the regulations laid out in the University's "Regulations and Policies applying to all users of University ICT facilities" document and the OC's Information Security Policy.
11. All authorised devices must (where possible) be running a properly-configured firewall program, such as the Windows or MacOS firewalls supplied with the operating system.