April 2020

Contents

1 Overview

Due to their ability to directly access and influence IT systems, people (users and administrators) represent one of the largest areas of risk to the security of IT systems and the protection of the confidentiality, integrity and availability of information.

Technical controls can only go so far in mitigating the risks from users and so the behaviour of people when using IT systems is fundamental to maintaining the security of IT systems and protecting the confidentiality, integrity and availability of IL7 information.

Therefore, a strong security culture is key to ensuring security of IL7 information and a robust training and awareness programme is necessary to embed this culture and ensure that users:

- Understand their roles and responsibilities related to the security of IL7 systems;
- Understand IL7's security principles, policy, procedures, and practice;
- Have relevant knowledge of the various management, operational, and technical security controls required and available to protect information resources for which they are responsible.

1.1 Purpose

This document provides guidelines for building and maintaining a comprehensive awareness and training program, as part of the GRA security responsibilities.

1.2 Scope

The scope of this guideline covers what IL7 should do to design, develop, implement, and maintain a security awareness and training program. The scope includes awareness and training needs of all IL7 staff from employees to supervisors and functional managers, to executive-level managers.

1.3 Applicability

This Policy applies to all personnel who work at and/or on behalf of IL7.

2 Cyber TrainingPolicy

2.1 Policy and Controls

This Policy is written to ensure that the outcomes of the following Cyber Security Principles are met:

- SP-02 Security Awareness education and Culture (Ref [1])

This Policy implements the following NIST controls, which are detailed in NIST Special Publication 800-53 (Ref [2]):

AT-1	Security awareness and training policy and procedures
AT-2	Security awareness and training
AT-3	Role-based security training
AT-4	Security training records
IR-2	Incident response training
IR-9 (2)	Training (response)
SA-16	Developer-provided training
SA-19 (1)	Anti-counterfeit training
PM-14	Testing, training, and monitoring
PM-16	Threat awareness program

3 General Requirements

IL7 seeks to administer training and oversee personnel with significant responsibilities for information security.

Management shall ensure that:

Policy ID	Policy Requirement
3.1	A security awareness and training program is constructed, documented and reviewed at regular intervals [NIST AT-1, PM-14].
3.2	All personnel are given security training for all systems they will use at IL7. Induction training is given to staff together with periodic refresher training and training on new systems any staff member may be asked to use. [NIST AT-2].
3.3	Full refresher training must be provided at least annually and 'top up' training provided throughout the year. 'Top-up' training must be provided in the event of a security incident, identification of poor security practice, changes in the operational environment and incident trends.
3.4	All staff receive briefings on pertinent security threats and threat intelligence that may affect them and the work of IL7. [NIST PM-16].
3.5	All training received by personnel is recorded in a Training Register and the staff member's HR record.
3.6	Each IL7 system has a dedicated set of Security Operating procedures, that dictate to users their responsibilities for security when using IL7 system in question. All users must read and sign these Security Operating Procedures prior to gaining access to the relevant system.
3.7	In addition to classroom/presentation based training, security awareness programmes can and should include of other media such as poster campaigns, security exercises and team meetings.

4 Training Leads shall ensure that:

Policy ID	Policy Requirement
4.1	All security training includes: • Data Classification and Handling; • Training on identifying and report insider threats [NIST AT-2 (2)]; • Training on identifying and reporting social engineering and phishing attacks [NIST AT-2 (3)]; • Training on the steps to take in a security incident, in line with the Security Incident Management Policy (Ref [3]) [NIST IR-2]; and • Training on how to prevent and mitigate data loss, particularly the loss of personal data. [NIST IR-9(2)] • Information where staff may find further information (for example IL7 Security Policy and the NCSC Website).
4.2	All security training includes practical exercises that simulate a realistic range of security incidents [NIST AT-2 (1), AT-3 (3)].

5 Project Specialisation Requirements

Team, Programme and Projects Leads shall ensure that:

Policy ID	Policy Requirement
5.1	A training needs analysis is carried out to determine which, if any, roles within the team warrant additional security training beyond IL7 baseline. This should also consider any legislative or regulatory requirements affecting the project.
5.2	All pertinent security information is distributed to all team, programme or project staff.
5.3	If a role on the team requires additional security training, then all staff in that role shall take the training. Staff must have regular refresher training and training updates as systems change. [NIST AT-3].
5.4	Where a team develops a system or service, then security training will be given to the users covering its operation and of its privacy functions. [NIST SA-16].
5.5	Where a team procures external services or goods, then training on detecting and handling insecure, counterfeit or substandard products is given to the team members. [NIST SA-19 (1)].

6 Exemptions, Exceptions and Breaches

6.1 Exemptions and Exceptions Policy

All IL7 systems and personnel must make every effort to comply with the entirety of the policy set, however, in the case that either some aspect of the policy set is not applicable, or that a system or member of staff is unable to comply with it, please refer to the exemptions and exceptions policy (Ref [4])

6.2 Breach of Policy

The IL7 reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this Policy. IL7 members of staff or contractors who breach this Policy may be subject to disciplinary action, including suspension and dismissal as provided for in IL7 Disciplinary Procedure.

Breaches of this Policy by a third-party-managed service provider may lead to the withdrawal of IL7 information technology resources to that third party service provider and/or the cancellation of any contract(s) between IL7 and the third party service provider.

The IL7 will refer any use of its IT resources for illegal activities to the Police.