Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

004 – Training, Awareness & Personnel Security v1.0

2021

Prepared by Department of the
Environment, Climate & Communications
gov.ie/decc

Table of Contents

1 Foreword

The Electronic Communications Security Measures (ECSMs) have been produced by the Electronic Communications Security Measures working group convened by the Irish National Cyber Security Centre (NCSC), which forms part of the Department of the Environment, Climate and Communications (DECC); and with the support of the Commission for Communications Regulation (ComReg). Industry participation in the WG has involved network operators, including the Mobile Network Operators (MNO) which have been awarded 5G licences, and selected fixed line operators.

This ECSM is part of a series of documents listed below:

Title	Subject
ECSM 001	General
ECSM 002	Risk Management
ECSM 003	Physical and Environmental Security
ECSM 004	Training, Awareness and Personnel Security
ECSM 005	Network Management & Access Control
ECSM 006	Signalling Plane Security
ECSM 007	Virtualisation Security
ECSM 008	Network, Monitoring and Incident Response
ECSM 009	Supply Chain Security
ECSM 010	Diversity, Resilience & Continuity
…	…

2 Introduction

Ireland's modern digitally connected society and economy is highly dependent on reliable and secure electronic communications networks and services (ECN and ECS respectively). They form the backbone of much of Ireland's critical national infrastructure providing connectivity to the essential services upon which citizens rely, such as healthcare providers, energy providers, financial institutions, emergency services and public administration. It is of paramount importance that these vital networks and services are protected from the full range of threats with an appropriate level of technical and organisation security measures.

This document focuses on aspects relating to training, awareness and personnel security of staff employed by the operator and its managed service providers / contractors.

The need for highly trained and skilled staff when designing, deploying, and operating next generation networks, such as 5G, was highlighted throughout the series of meetings of the ECSM Working Group held throughout 2020. Likewise, the need for all staff to be aware of security issues was emphasized as an important means of protecting operators and from compromises to one of the three main pillars of security - the **confidentiality**, **integrity** and **availability** of networks through robust security procedures and processes. In order to ensure proper compliance with the appropriate security measures, operators need to integrate security concepts into their decision making and culture through responsible policies, procedures and processes - including staff training and awareness.

3 Scope

The ECSMs are applicable to all undertakings providing public Electronic Communications Networks and Electronic Communications Services.

The legislative basis for the ECSMs is set out in ECSM 001- General

Security measures relating to training, awareness and personnel matters are particularly important to staff who have physical or logical access to sensitive data and operational networks. External attackers undermining electronic communications systems often target enterprise staff initially, escalating privilege to operational parts of networks and staff working in those areas. As such it is important that all new staff are screened, undergo mandatory and appropriate security awareness training and that all existing staff undergo annual training.

The legislative basis for the ECSMs is set out in ECSM 001- General

4 References

Document	Title
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27002:2013	Information technology — Security techniques — Code of practice for information security controls
NIST	Framework for Improving Critical Infrastructure Cybersecurity v1.1
NIST SP 800-53 Rev4	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program
NIST SP 800-100	Information Security Handbook: A Guide for Managers
ENISA	Technical Guideline on Security Measures under the EECC
ENISA	Supplement to the technical guideline on Security Measures under the EECC
ENISA	The new users' guide: How to raise information security awareness
ETSI TR 103 305-1 V3.1.1	Critical Security Controls for Effective Cyber Defence
SANS	Security Awareness Report 2019 - The Rising Era of Awareness Training

44 5 Definitions, Symbols and Abbreviations

45 5.1 Definitions

Term	Meaning
EU 5G Security Toolbox	Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures' document published jointly by member states on 31st of January 2020
EU Risk Assessment	EU coordinated risk assessment of the cybersecurity of 5G networks report published jointly by the EU Member States on 09th October 2019
Managed Service Provider (MSP)	A third-party that helps to run or administrate a network.
National Risk Assessment	Risk assessment carried out by the National Cyber Security Centre and forwarded to the European Commission on 15 July 2019.
Operator	An undertaking providing or authorised to provide a public electronic communications network or an associated facility;
Personnel	The people who work for an organisation.
Security Awareness Program	A set of policies the organisation implements to create a culture of security for its staff.
Security of Networks and Services	The ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services

5.2 Symbols

Nil

5.3 Abbreviations

Term	Meaning
AV	Anti Virus
ComReg	The Commission for Communications Regulation
CSIRT	Computer Security Incident Response Team
DECC	The Department of Environment, Climate and Communications
ECSM	Electronic Communications Security Measure
JML	Joiner, Mover, Leaver
MNO	Mobile Network Operator
MSP	Managed Service Providers
NCSC	National Cyber Security Centre

6 Overview of Risk

Creating an effective security awareness program is key to securing any organisation, large or small. Demystifying security and educating users about their role in protecting the organisation helps cultivate a robust first line of defence. Likewise, ensuring that appropriate personnel security policies are in place helps protect the organisation from breaches of confidentiality, integrity and availability arising from poor staff practices and poor human resources policy, or training, or the lack of implementation of such policies and training.

Cybersecurity can often be considered primarily a technical challenge; however, the actions of staff can have a huge impact in maintaining the security, confidentiality, integrity and availability of networks. A range of personnel play a crucial role throughout the design, deployment and operation of electronic communications networks. They fulfil important functions including in system development and programming, network operations engineering, security functions and in executive decision-making. All personnel face security challenges – including avoiding the introduction of vulnerabilities or compromises at any points in the network. Staff and other personnel within an organisation can be faced with any number of threats from different sources, such as:

- Phishing campaigns and other social engineering attempts,
- Ransomware and other malicious attacks,
- Cyber espionage and
- Network misconfigurations and human errors.

An organisation may be vulnerable where there are gaps or seams between policy and technology (e.g. policies that have no technical enforcement) or during times of vulnerability, for example during a window of patching or system changes. A staff member with a poor understanding of cybersecurity threats and risks make an organisation vulnerable, as attackers target weaknesses in humans in order to overcome technical security controls. Therefore, an effective security training and awareness regime is critical to protecting the confidentiality, integrity and availability of an operator's network.

In addition to external actors, an operator's own personnel can also act as a vector or target for security incidents, such as where there is staff incompetency or because of the actions from a malicious insider. The actions of insiders, be they staff or a subcontractor, working within electronic communications operators was highlighted as a serious concern in the EU-wide Risk Assessment, being rated second only to Nation States as representing the most serious threat actors:

> ***"It is also noted that insiders or subcontractors can in certain circumstances also be considered potential threat actors, especially if leveraged by States as they could be used as a channel for a State to gain access to critical target assets"***

Accordingly, in areas where operators delegate operational control -even if very temporarily- they should ensure that their partners sign-up to the organisation's key security principles and can abide by them and that there are implications where issues arise.

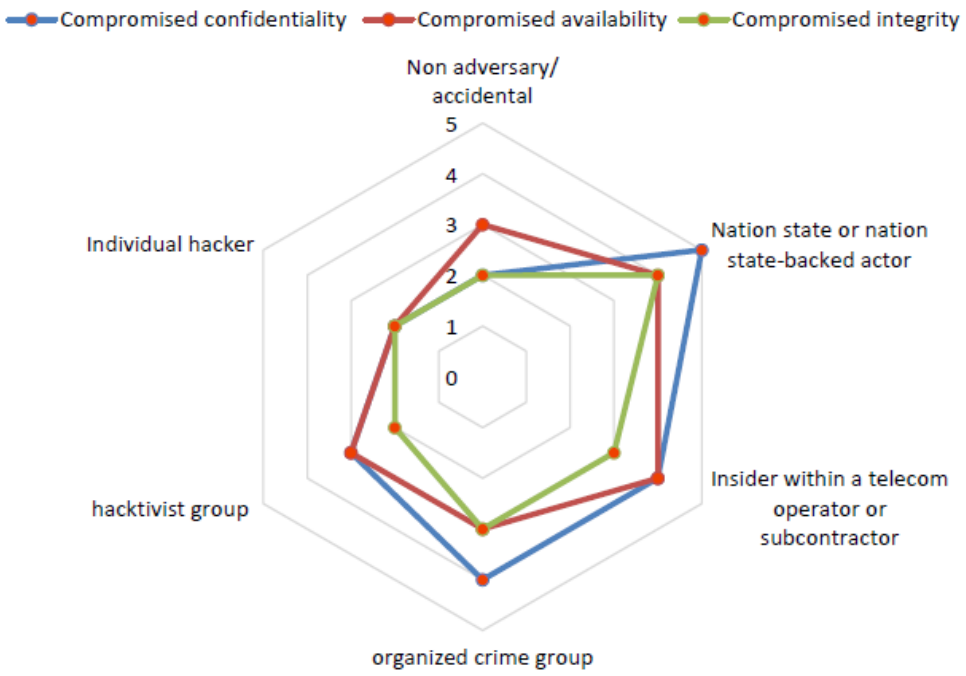

Figure 1 – Threat Actors

The increasingly complex nature of electronic communications networks and the need for highly specialised and trained personnel was also emphasised as an issue given that this expertise is difficult to source.

> ***"Lack of specialised and trained personnel to secure, monitor and maintain 5G networks: the fast-evolving threat landscape and technology and the complexity of 5G networks will lead to an increased need for IT security professionals with specialized knowledge (e.g. competence in the areas of cloud architecture)."***

In order to effectively address cybersecurity risks it is paramount that operators take actions to reduce the risks arising from the vulnerabilities that are tolerated or are caused wilfully or by human error. Empowering staff with good security training, awareness, personnel policies and procedures can significantly increase an operator's readiness in effectively responding to a security threat.

7 Security Measures

The operator should implement the Training, Awareness and Personnel Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
Personnel Security	
TP.01	Operators shall have appropriate personnel security policies, procedures and processes in place which are approved by senior management, communicated to staff and reviewed regularly.
TP.02	Roles within the organisation with access to network management systems or sensitive data shall be assessed and assigned a risk designation.
TP.03	Operators shall establish a screening process for new staff in roles considered high risk, such as those which require administrative access to operational networks or handling sensitive data.
TP.04	Employee contracts, or codes of conduct, shall include employee and operator obligations regarding security, particularly for roles assessed as high risk.
TP.05	Operators shall have an appropriate disciplinary process in place to take action against personnel who commit a serious breach of their security obligations.
TP.06	Operators shall have an appropriate joiner, mover, leaver (JML) process. The JML process shall link human resource processes with other relevant organisation processes, such as security authorisations and access control. This process should be automated wherever feasible.
Training and Awareness	
TP.07	Operators shall have appropriate training and awareness policies, procedures and processes in place which are approved by senior management, communicated to staff, and reviewed regularly.
TP.08	New employees shall receive security & awareness training as part of their on

	boarding process. This training should be repeated periodically, at least annually.
TP.09	Personnel, particularly those in high-risk roles, shall be sufficiently competent and shall have a level of skill, education, and training appropriate to their position.
TP.10	Role based training shall be provided to personnel in roles assessed as high risk. It should cover as a minimum, how to: detect and avoid common cybersecurity attacks, to recognise anomalous behaviours, handle sensitive data and to report and respond to security incidents.
TP.11	The operator shall maintain records of all security training.

108

109

8 Implementation Guidance

The implementation guidance in the following subsections is applicable to the security measures in section 7 as shown in Table 1 below.

Table 1 – Security Measures to Guidance Mapping

	TP. 01	TP. 02	TP. 03	TP. 04	TP. 05	TP. 06	TP. 07	TP. 08	TP. 09	TP. 10	TP. 11
8.1	✓	✓		✓			✓	✓	✓		
8.2					✓		✓	✓	✓	✓	✓
8.3		✓	✓					✓	✓	✓	
8.4	✓			✓	✓	✓		✓			

8.1 Security Training and Awareness Programme

Applicable Security Measures: TP.01, TP.02, TP.04, TP.07, TP.08, TP.09

The most effective approach to implementing the *Security Measures* described above is for operators to implement a comprehensive Security Training and Awareness programme which is governed by overarching security policies. Accordingly, the programme should cover security principles, vulnerabilities and threats, most common sources of attacks, how to defend against them and knowing the response required.

The operators Risk Management process, as outlined in ECSM 002 – Risk Management, is a key factor in establishing appropriate security training and awareness policies and procedures. The procedures should be established both for a general security programme and one that is for particular information systems. The security training and awareness programme should, as a minimum, identify the scope of who needs to be trained in the program. In particular, care should be taken to ensure that those personnel in roles considered high risk, such as those which require administrative access to operational networks or handling sensitive data receive an appropriate level of security and awareness training. In order for a security training and awareness programme to be successful, it should be led by a Security Training and Awareness officer and championed at the most senior level of management of the organisation.

The aim of the security training and awareness programme should, in the first instance, be to communicate the operator's security policies and requirements to ensure that the operator's personnel know, understand and can follow the set down policies, procedures and processes. The security training and awareness programme should be **risk-based**, in line with ECSM 002, and the operator's security team should help identify the main human risks to the organisation.

The focus of the security training and awareness programme is identifying which personnel behaviours require modification in order to effectively manage the main risks. The ultimate goal of a successful security training and awareness programme is to have a workforce which acts in a secure manner, resulting in a reduced risk profile for the operator.

Certain personnel, such as those in roles considered high risk, or with access to certain critical systems, may require additional specialised training in addition to a general security training and awareness programme.

It is important that security awareness training is recorded, and key metrics are measured over time in order to track the effectiveness of the security training and awareness programme. A security training and awareness programme should be focussed on the long-term goal of creating a security culture within the operator by embedding security behaviours in personnel throughout the organisation.

8.2 Security & Awareness Training

Applicable Security Measures: TP.05, TP.07, TP.08, TP.09, TP.10, TP.11

The content of security awareness training can vary depending on the level of risk presented, and on the user base at which it is aimed. The key aim of the program is to modify the behaviour of staff and create a security culture within the organisation; therefore the security awareness training should take a long-term view, and not a "*fire and forget*" approach. While a "one size fits all approach" is not possible, a typical security and awareness training should cover at least three types of roles:

- All personnel (or general),
- Specialized staff and
- Management.

As a minimum basic security awareness training should include an understanding of the need for information security and user actions to maintain security and to respond to

suspected security incidents.[1] It should also include an overview of the operator's security policies, procedures, and processes, as well as staff's shared obligations to security. The training should cover basic cyber hygiene and how to detect and avoid common cybersecurity attacks. Users should be taught how to recognise anomalous behaviours, handle sensitive data and to report and respond to security incidents. In addition, the training should provide users with an overview of the cyber threat environment.

There are various techniques that can be used to provide security awareness training including, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organisational officials, displaying logon screen messages, and conducting information security awareness events. However, a more engaging and proactive approach generally has more effective results such as running simulated phishing attack exercises, executive level tabletop exercises or simulated cyber attack exercises.

As outlined in the *Overview of Risk* section, insider threats continue to be a serious threat to operators' security. As such, in addition to personnel security policies, operators should provide training to staff on common signs to look for in detecting a malicious insider or disgruntled employee and how this should be reported to management. The UK CPNI has detailed guidance on reducing insider threats.[2]

In addition to the general security awareness training, certain persons in roles considered to be high risk, should be provided with specific role-based training. System or network administrators, or users with privileged access or who possess valuable information, should receive training which is specific to the systems which they oversee. As high value targets, senior executives should receive enhanced security training, particularly in how to detect targeted spear phishing and social engineering attacks, be aware of current information on security threats and effective countermeasures.

In order to understand whether a security training and awareness programme has been effective, it is important to record key metrics, for example improvements in staff security behaviours.

Finally, management needs to be clear in its messaging to all staff in terms of the policies and practices it pursues externally and internally. Security and privacy are a core corporate responsibility underpinned by legal obligations and norms.

[1] *All staff should be made aware of the importance of strong passwords and password controls; secure e-mail practices; secure practices for working remotely; secure browsing practices while avoiding malicious software – viruses, spyware, adware*.

[2] Reducing Insider Risk by good personnel security practices | Public Website (cpni.gov.uk)

8.3 Screening

Applicable Security Measures: TP.02, TP.03, TP.08, TP09, TP.10

Operators are required to establish a screening process for roles which are considered as high risk. The purpose of a screening process is to ensure that only competent and adequately skilled personnel have access to the operator's most critical systems and sensitive data. The level of screening should be in proportion to the risks presented. The screening process should follow a clear policy which at a minimum outlines which roles should be screened, who in the organisation is authorised to screen people and how, guidance on screening is provided in ISO 27002 § 7.

Operators should include due diligence measures to ensure that the personnel they employ are who they say they are, hold the qualifications they purport to, are of good character and competent to perform their duties. As part of the screening process, information provided by candidates should wherever possible be independently verified.

Information, particularly relating to academic performance and skills should be independently verified, including from universities. The operator should have a process to verify the identity of any prospective employees. Operators should seek character references from previous employers or trusted introducers, particularly with regard to competence to perform the duties and trusted to take on roles considered as being high risk. Consider retaining third party expert recruiters to confirm all details. Information may be obtained from searches of the public domain but must be done so in line with relevant legislation, including providing the candidate with an opportunity to comment.

The screening process must be conducted on a lawful basis, consistent with relevant privacy, equality and employment legislation, including, inter alia, the Data Protection Act 2018, the General Data Protection Regulation (GDPR), and the Employment Equality Acts 1998 – 2015. Operators must comply with the principles of data protection (Article 5 GDPR) in their collection and use of personal data.

8.4 Joiners, Movers, Leaver (JML) Process

Applicable Security Measures: TP.01, TP.04, TP.05, TP.06, TP.08

Often a key failing of security is the result of Human Resource processes not linking with other relevant organisational processes. For example, personnel may have a higher level of access than required or maintain their access to critical systems or sensitive data after they have moved positions or left the organisation entirely. It may also result in personnel not

receiving key induction or follow-up training, or not understanding their obligations while they were with the organisation or after they have left. Exit interviews should be conducted in order that staff are made aware that their obligations to maintain confidential information regarding security and privacy of sensitive information after they have left the organisation.

Operators should ensure that their HR processes include providing new employees with adequate induction training, including security training and awareness, which outlines the security obligations and responsibilities expected of new employees. The HR process should also be linked to IT and security processes which provide the appropriate level of security authorisations and access to new employees. The joiners process should also ensure that personnel have the appropriate equipment and technology available to conduct their work in a secure manner. Similarly, credentials such as ID cards and badges should be issued as part of the joiners' process.

When personnel change roles, or take on new responsibilities, there should be a specific movers' process, which provides them with any new security authorisations and access, and revokes previous credentials, security clearance and access. Employees should receive adequate training for their new roles.

Finally, as part of the leaver's process personnel should have all security authorisations, clearances and associated accesses revoked. All operator owned equipment and data should be reclaimed, and credentials such as ID cards and badges returned. Employee contractual arrangements should ensure that there are obligations on employees to maintain confidential information regarding security and privacy of sensitive information after they have left the organisation. It is best practice to conduct employee exit interviews as part of a leavers process, which may be used as an opportunity to remind personnel of their continuing security obligations.

The JML process, particularly when it comes to security authorisations and access to information systems, should be directly linked with HR processes and automated wherever possible. The JML process should also be subject to monitoring and audit to ensure that they are fit for purpose, reflect best practice and that the policies are being adhered to.

9 Relevant References

The following standards, guidelines and reports offer further detail and will assist operators in designing policies, procedures and processes that meet the *Security Measures* outlined in Section 7 of this document.

9.1 NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

NVD - Rev4 (nist.gov)

This publication provides a catalogue of security and privacy controls to protect organizational operations, assets, individuals, from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.

Relevant to this ECSM are the families of controls Awareness and Training (AT) and Personnel Security (PS) which cover in more detail, many of the recommended security measures.

9.2 NIST SP 800-50: Building an Information Technology Security Awareness and Training Program

SP 800-50, Building an Information Technology Security Awareness and Training Program | CSRC (nist.gov)

NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, provides guidance for building an effective information technology (IT) security program.

The document identifies the four critical steps in the life cycle of an IT security awareness and training program: 1) awareness and training program design; 2) awareness and training material development; 3) program implementation; and 4) post-implementation.

9.3 ENISA: The new users' guide: How to raise information security awareness

The new users' guide: How to raise information security awareness (EN) — ENISA (europa.eu)

The guide presents an analysis of the main processes to prepare and implement information security awareness programmes in public and private organisations. Each process is

analysed and time-related activities and dependencies are identified. The process modelling serves as a jumpstart for awareness programme development.

9.4 ISO/IEC 27001:2013 & ISO/IEC 27002:2013

Clause A.7 – Human Resource security covers the controls an organisation needs to implement prior, during and after employment. It covers areas such as screening, terms and conditions of employment, management responsibilities, information security awareness, education & training, disciplinary procedures, and termination of employment.

https://www.nsai.ie/certification/management-systems/iso-iec-27001-information-security-management-system/