Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

003 – Physical and Environmental 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.

The ECSM Working Group Convened on the 19th 20th and 21st of May 2020 to discuss matters concerning physical and environmental security. The group heard from experts in the field of physical and environmental security and held focussed discussions on the risks, challenges and best practices associated with physical and environmental security as it pertains to telecommunications networks. ECSM 003 – Physical and Environmental Security has been developed by the NCSC informed by those meetings.

3 Scope

The ECSMs are applicable to all undertakings providing public Electronic Communications Networks and Electronic Communications Services. It is acknowledged that there may be significant challenges associated with implementing all of the security measures of this ECSM in older buildings and sites. Undertakings are expected to comply with the security measures set out in this ECSM in a manner appropriate and proportionate to criticality and sensitivity of the asset, to improve physical security and mitigate the potential for environmental impacts.

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

4 References

Document	Title
Department of the Environment, Climate and Communications	National 5G Risk Assessment
ENISA	Technical Guideline on Security Measures under the

	EECC
ENISA	Supplement to the technical guideline on Security Measures under the EECC
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	Security and Privacy Controls for Federal Information Systems and Organizations

35

36 # 5 Definitions, Symbols and Abbreviations

37 ## 5.1 Definitions

Term	Meaning
Contractor	A person who is not an employee of an organisation but is an employee of another organisation or company engaged to perform specific tasks.
Critical or Sensitive Location	A network site that is critical to the integrity and security of a significant proportion or the complete network or hosts sensitive data. Such sites may be identified by a site or site category risk assessment.
Critical Remote Installations	Important sites that need to be protected - transmission nodes (mobile), exchange (fixed). Such sites may be identified by a site or site category risk

	assessment
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
Framework Regulations	S.I. No. 333/2011 - European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011
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
Operator of Essential Services	A person designated as an operator of essential services under Regulation 12 of European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018
Visitor	A person not employed by an organisation or one of its contracting companies

38

39

40

5.2 Symbols

Nil

5.3 Abbreviations

Abbreviation	Meaning
2FA	Two Factor Authentication
BTS	Base Transceiver Station
ComReg	The Commission for Communications Regulation
DECC	The Department of Environment, Climate and Communications
ECSM	Telecommunications Security Requirements
ENISA	European Union Agency for Cybersecurity
MNO	Mobile Network Operator
NCSC	National Cyber Security Centre

6 Overview of Risk

Physical and environmental risks are long standing considerations for the security of Electronic Communications Networks and Electronic Communications Services and form a key part of a layered approach to the overall protection of a networks' assets and functions.

Electronic communications facilities require robust physical and other security measures which are effective against:

- Theft;
- Arson;
- Vandalism;
- Other criminal damage;
- Unauthorised access to data or systems;
- Security Infringements;
- Trespass:
- Interference as regards both network hardware and software.

6.1 Physical Risks

For example, if an attacker gains physical access to critical or sensitive network assets, they have the ability to completely override most of the digital controls an operator has put in place. Also, an attacker who gains access to a core data centre could install a rogue device to capture confidential data, or damage critical network equipment compromising network availability.

In addition, attacks which cause criminal damage to property such as masts, cell towers, power boxes, infrastructure and equipment can result in serious disruptions of essential connectivity for the emergency services and other users. For example, in December 2020 a physical attack on communications infrastructure in Nashville, USA caused a severe outage in multiple neighbouring states causing disruption to communications including emergency services[1].

Physical security risks pose an increased threat in future networks as outlined in the National Risk Assessment including mobile edge computing sites because of their decentralised locations:

[1] https://www.theverge.com/2020/12/28/22202822/att-outage-nashville-christmas-bombing

> ***"The virtualised nature of 5G infrastructure presents new threats and challenges as much of the sensitive functions currently performed in the physically and logically separated core will move closer to the edge of the network… The decentralised nature of Mobile Edge Computing (MEC) makes protecting these critical nodes more challenging both physically and remotely.... Such decentralised locations are attractive targets for a threat actor who wishes to disrupt the network".***

The risk of a compromised insider, exploiting their physical access, is also highlighted:

> "***Vendors or their employees subject to third country legislation who are provided with physical access to sensitive areas of the 5G infrastructure could misuse this access to compromise the confidentiality, integrity or availability of data on the network on the instructions of a third country."***

Recognising the importance of mitigating these risks, the report recommends that having "layers" of protection:

> ***"Adequate physical security measures are required to protect these sensitive areas. Effective physical security of an asset is achieved by multi-layering the different measures, what is commonly referred to as 'defence-in-depth'. The concept is based on the principle that the security of an asset is not significantly reduced with the loss of any single layer. Physical security measures include elements such as Access Control and Locking systems, Barriers which deny or delay access, CCTV, Alarms and Detection systems, Security Personnel, Internal Segmentation."***

Equally the EU Risk Assessment highlights that

> ***"Deficiencies in physical security can lead to inadequate protection of personnel, hardware, software, networks and data from any malicious actions and events"***

Moreover, the importance of physical security was emphasised in the EU 5G Security Toolbox with Technical Measure 06 –'Reinforcing Physical Security' calling on Member States to:

> ***"Ensure that MNOs reinforce physical protection of critical components and sensitive parts of the 5G networks, taking a risk-based approach for Multi-Access Edge Computing (MEC) and base stations… In reinforcing physical access controls, it is important to ensure that access is granted only to a limited number of security-vetted, trained and qualified personnel. Access by third-parties, contractors, and employees of suppliers/vendors, should be limited and monitored, particularly where it concerns critical components and sensitive parts of the 5G networks."***

6.2 Environmental Risks

Meanwhile, environmental hazards remain a constant challenge for operators, in ensuring that telecommunications networks remain resilient. Environmental hazards include natural phenomena such as:

- Temperature and humidity extremes,
- Fires,
- Severe weather events such as storms, flooding and lightning, and,
- Electromagnetic phenomena.

It is acknowledged that undertakings have some existing sites that are prone to flooding and that these sites exist to serve the local areas in which they are situated.

ENISA reported that 'Natural Phenomena' accounted for 63% of all user hours lost (1789 m) in the electronic communications outage reports.[2]

This document sets out a series of physical and environmental security measures that operators must implement, in order to reduce the associated risks.

[2] https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

7 Security Measures

The operator should implement the Risk Management Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
PS.01	The operator shall identify and reduce the risks relating to physical threats, environmental hazards and opportunities for unauthorized access to systems or data.
PS.02	The operator shall categorise their assets based on their criticality/sensitivity and shall implement appropriate controls to secure them.
PS.03	The operator shall enforce appropriate processes to provide physical access authorisation to personnel.
PS.04	The operator shall ensure that physical security policies and procedures are sufficiently detailed and cover all sites appropriately.
PS.05	The operator shall protect critical/sensitive areas with appropriate entry controls to ensure that only authorised personnel are allowed access.
PS.06	The operator shall monitor the physical security status of their critical assets based on a site or site category risk assessment in order to detect and respond to incidents.
PS.07	The operator shall ensure that critical remote installations have a level of security appropriate to their criticality.
PS.08	The operator shall design and apply effective procedures for working in critical or sensitive areas.
PS.09	The operator shall ensure that network equipment is housed in a temperature and humidity controlled environment, within the operating specifications of the equipment.
PS.10	The operator shall ensure that measures are put in place for early detection of smoke, fire and water ingress at critical sites.

8 Implementation Guidance

The following sections cover the implementation of physical and environmental security measures outlined in the physical and environmental security principles set out in section 7. It is recognised that planning restrictions and space limitations around some sites, such as base stations, may impede an operator's ability to implement optimal physical security measures. It is also noted that many third-party sites such as data centres and BTS sites are shared with other operators, security at these sites should be addressed as part of the supply chain process with the owners of these sites as covered in ECSM 009.

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

Table 1 – Security Measures to Guidance Mapping

	PS.01	PS.02	PS.03	PS.04	PS.05	PS.06	PS.07	PS.08	PS.09	PS.10
8.1	✓	✓								
8.2	✓		✓	✓						
8.3	✓		✓	✓	✓					
8.4	✓		✓	✓	✓					
8.5						✓	✓	✓		
8.6			✓	✓	✓	✓	✓			
8.7					✓	✓	✓	✓		
8.8					✓	✓	✓	✓		
8.9									✓	✓

8.1 Physical Asset Classification

Applicable Security Measures: PS.01, PS.02

Operators should categorise their physical network assets such as core network assets, base-stations, and interconnection & transport links, based on a risk assessment and according to the asset's sensitivity/criticality. This categorisation of physical network assets should be reviewed regularly, at least annually. This categorisation will determine the level of physical security required at the site.

Operators should also review their categorisation of physical network assets regularly following any security incidents, significant changes in architecture, lessons learned activities, best practice and on foot of receipt of verifiable threat intelligence.

An operator should have their physical network asset categorisations reviewed by independent third parties and experts to assess the adequacy of policies. However appropriate internal independent risk, audit and security assessments of these policies also suffice.

8.2 Physical Security Policies and Procedures

Applicable Security Measures: PS.01, PS.03, PS.04

Operators should have documented physical security policies and procedures, which are approved by senior management, communicated to staff where appropriate and reviewed regularly. These physical security policies and procedures should be sufficiently detailed and cover all physical network assets, such as core data centre locations, aggregation sites, interconnection points, etc.

Operators should review and update their physical security policy and procedures documentation, based upon lessons learned from security incidents, security exercises or drills, best practice and on foot of receipt of verifiable threat intelligence.

An operator should have their physical security policies and procedures reviewed by accredited third parties and experts to assess the adequacy of policies, however appropriate internal independent risk, audit and security assessments also suffice.

8.3 Physical Security Authorisations

Applicable Security Measures: PS.01, PS.03, PS.04, PS.05

The operator should develop, approve and maintain a list of personnel authorised to access its non-public facilities. The operator should verify personnel's identity using an appropriate form of government issued identification document such as passport, driving licence, etc. or operator maintained photographic identity, prior to granting any physical access authorisations.

The operator should issue appropriate credentials – such as ID cards, badges or smart cards, to permanent employees and contractors, as well as temporary access cards for visitors to network sites. External visitors with no previous authorised access to critical/sensitive locations should have an employee with appropriate security clearance assigned to them at all times.

Prior to issuing physical access authorisation the operator should, within the confines of legislation, conduct internal security screening, such as security questionnaires and risk assessments on personnel granted physical access to any critical or otherwise sensitive areas. Further detail on security screening can be found in ECSM 004 and ISO 27002 §7.

The operator should implement multi-factor authorisations for access to critical/sensitive areas: such as PIN access, smart cards, biometrics, etc.

The operator could conduct background checks and screening of key personnel and contractors prior to authorisation for physical access to critical/sensitive functions. Consideration should be given to relevant legislation when conducting such background checks. Further detail on background checks and screening can be found in ECSM 004 – Training, Awareness and Personnel Security.

8.4 Physical Security Access Control

Applicable Security Measures: PS.01, PS.03, PS.04, PS.05

Physical access authorisations should be enforced to a level appropriate to the criticality and sensitivity of a site. Individuals, with authorisation as specified in section 8.3 above, need to be verified and their access controlled. Such access controls should use a combination of professional security or administrative personnel and effective physical access devices such as keys, locks, combinations, card and PIN readers, biometric scanners etc to best practice standards. Separate physical security controls should be present at the entrance and exit to any critical or sensitive locations.

Physical access to any critical or sensitive locations should be continuously monitored by security staff and/or alarms. Intruder detection equipment should be designed and

maintained to industry standard, based on a site or site type risk assessment, ensuring that it can effectively detect unauthorised access.

Visitors and contractors to any critical or sensitive locations without specific authorisation should be escorted or monitored by an employee with appropriate security clearance. Staff should be made aware of the risk posed by 'tailgating' especially at critical or sensitive sites through training etc. At least two factors of authentication (2FA) is recommended for authorised personnel to access the most critical or sensitive locations based on a site or site type risk assessment. While 2FA may be disproportionately expensive to deploy in existing sites, it should be used in new greenfield sites.

Physical access for visitors and temporary contractors should be recorded and logged at the entry and exit points of any critical or sensitive sites. The record should include the name of the visitor, form of ID, the company/organisation of the visitor, the purpose of visit or person they are visiting. Records should be retained for at least 6 months.

Security checks should be carried out on personnel entering or exiting the most critical or sensitive locations, such as core data centres, to mitigate against the risk of data exfiltration or use of unauthorised equipment.

8.5 Physical Security Monitoring

Applicable Security Measures: PS.06, PS.07, PS.08

The operator should monitor physical access to all critical or sensitive locations to detect and respond to physical security incidents. The operator should have effective surveillance equipment covering these critical or sensitive locations, such as intruder alarms and video surveillance. Alarms logs and video surveillance data should be retained for at least 30 days, subject to Data Protection Act 2018. The operator should review physical access logs at all critical or sensitive locations on at least on a monthly basis, and in the event of any suspicious physical access activities [3].

Operators should implement automated recording and logging of physical access at all critical or sensitive locations. Physical security access logs should be reviewed on a regular basis, at least monthly, by the security function or by a member of staff of suitable seniority based on a site or site type risk assessment. The operator should have an automated

[3] (i) Accesses outside of normal work hours that are not planned or in response to network fault; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses

system which detects suspicious physical access activities and notifies the security function based on a site or site type risk assessment.

The operator should have a dedicated Network/Security Operations Centre (NOC/SOC) which monitors physical access to sensitive or critical sites and investigates suspicious or malicious physical security activities. The NOC/SOC should have an ability to coordinate a response to physical security incidents.

As an additional measure, operators could employ an independent physical security penetration testing process, including unannounced attempts to bypass and circumvent security controls associated with physical access to its facilities and critical or sensitive locations, other appropriate internal independent risk audit and security assessments also suffice.

8.6 Physical Security of Remote Installations

Applicable Security Measures: PS.03, PS.04, PS.05, PS.06, PS.07

The operator should ensure that critical remote installations are not accessible to the general public where feasible, and are protected from burglary or vandalism, by installing effective physical security defences[4]. The operator should regularly monitor and/or inspect the physical security status of these critical remote installations. A record of all persons accessing any critical remote installations should be maintained, it should include at least the date/time, purpose of their visit and any works carried out.

Remote installations should be sited and constructed to ensure that they are appropriately resilient, insofar as possible, to natural phenomena and severe weather events – such as storms, hurricanes, flooding, and fires, based on a site or site type risk assessment. It is acknowledged that network site estates have evolved over time, it is expected that for older legacy sites where retro-fitting would be difficult to implement and cost prohibitive, exceptions will apply.

The operator should have an ability to continuously detect physical security activity at remote installations[5] based on a site or site type risk assessment. In order to keep the volume of recordings as manageable as possible, deployment of CCTV should only be considered

[4] This can include, but not limited to, gates, locks, locked cabinets, perimeter fences, security walls, bollards, etc.

[5] CCTV, Intrusion detection systems, motion detection,

appropriate where a demonstrable benefit can be gained but should be kept under review having regard to changes in security threats.

The operator should have an ability to respond to physical security incidents at remote installations in a timely basis based on a site or site type risk assessment. Illegal activity should be reported to the relevant authorities.

Where an external party's equipment is co-located within the same remote installation, where possible it should be securely separated for example in secured equipment cages.

8.7 Working in Critical or Sensitive Areas

Applicable Security Measures: PS.05, PS.06, PS.07, PS.08

The operator should physically segment facilities under its control and ensure only personnel with appropriate authorised security clearance have access to any critical or sensitive areas[6] Any critical or sensitive areas should be positioned to reduce the chance of material being viewed by unauthorised persons, exemptions may be allowed for legacy collocated sites where space does not permit this and for long standing services and service nodes.

Personnel should only be aware of activities on a need to know basis.

Vacant secure areas should be physically locked and periodically reviewed.

Photographic or recording devices should not be allowed in critical or sensitive areas unless otherwise authorised.

8.8 Delivery and Loading areas

Applicable Security Measures: PS.05, PS.06, PS.07, PS.08

The operator should have procedures to control and isolate access points, such as delivery areas, from any critical or sensitive areas to avoid unauthorised access. Access should be restricted to identified or authorised personnel. Delivery persons should not be able to access other parts of the building.

External doors of the delivery area should be secured when internal doors are open. Incoming deliveries should be inspected, registered and segregated from outgoing material where possible, according to asset management procedures. Exemptions may be allowed for older legacy sites where retro-fitting would be difficult to implement and cost prohibitive.

[6] Critical/Sensitive areas to be determined based on a risk assessment. Critical/sensitive areas include but are not limited to: Network Operations Centre (NOC), Security Operations Centre (SOC), Data Centres & Server rooms, Mobile Edge Computing Sites etc.

8.9 Environmental Security

Applicable Security Measures: PS.09, PS.10

Electronic communications network equipment has a specified range of operation in terms of temperature and relative humidity; therefore, it should be ensured that these parameters are maintained within the operating limits of the network equipment at the network sites. The temperature and humidity level of sites which house any critical or sensitive assets should be continuously monitored.

All critical or sensitive assets should be protected from the risk of fire – for example, the use of smoke detection systems, fire detection systems and automatic fire suppression systems based, on a site or site type risk assessment. All critical or sensitive physical assets should be protected from damage due to water ingress or flooding based on a site or site type risk assessment.

Any new build critical or sensitive assets should be sited and constructed to ensure that they are appropriately resilient to natural phenomena and weather events – such as storms, hurricanes, lightning, flooding, and fire. Any critical or sensitive assets should be protected from other environmental hazards, such as smoke, dust, vibrations, electrical interference, electromagnetic radiation and emanation.

An automatic alert should be generated when environmental monitoring systems detect levels outside of an acceptable norm. The operator could obtain specialist advice on how to avoid damage from environmental threats

9 Relevant References

The following standards and publications provide detail on implementation of physical and environmental security measures.

9.1 NIST Framework for Improving Critical Infrastructure Cybersecurity

This document is published by the US National Institute of Standards and Technology, it is a framework that is intended to compliment and support but not replace organisations' risk management processes. It provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organisations or it can be focused on the delivery of critical services within an organisation.

This publication is available free of charge at

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

9.2 NIST SP 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations.

This document is published by the US National Institute of Standards and Technology, it provides a comprehensive catalogue of security and privacy controls for information systems and organisations to protect organisational operations and assets, individuals, other organisations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

The family of controls entitled "Physical and Environmental Protection" covers the specific applicable requirements.

This document is available free of charge at

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

9.3 ISO 27001 Information Technology-Security Techniques – Information Security Management Systems - Requirements

ISO 27001 is part of the ISO 27000 series of specifications that focus on information security management systems including all elements or components that support information security. The requirements in it are generic and applicable to all types of organisations regardless of size or nature. It is a high level document with references to more detailed requirements contained in other documents in the series in particular ISO 27002. Annex A of this document is a normative annex that lists a range of measures that are aligned with the detailed measures in ISO 27002.

Clause 11 entitled “Physical and Environmental Security” covers the specific applicable requirements.

This document may be purchased form the ISO, national standards bodies or through other sources.

9.4 ISO 27002 Information Technology – Code of Practice

This document is for use by organisations as a reference for applying the information Security Management System controls based on ISO 27001. It may also be used as a guidance document for organisations implementing commonly accepted information security measures. It provided detail on the measures outlines in Annex A of ISO 27001.

Clause 11 entitled “Physical and Environmental Security” covers the specific applicable requirements.

This document may be purchased form the ISO, national standards bodies or through other sources.

9.5 ENISA Technical Guidelines on Security Measures under the EECC

This document provides technical guidance to the national regulatory authorities tasked with supervising the security of electronic communication networks and services and in particular the security measures mentioned in Article 40 the European Electronic Communications Code. It provides guidance on classifying assets, a list of security measures and security objectives, it also provides a mapping of the measures in this document to relevant ISO standards.

Security objective 9 entitled “Physical and Environmental Security” covers the specific applicable requirements.v