Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

008 – Network Monitoring & Incident Response 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 02nd, 3rd and 04th of June 2020 to discuss matters concerning secure network design, deployment, and operation. The group heard from experts in the field of electronic communications operations, security and incident response and held focussed discussions on the risks, challenges and best practices associated with network monitoring and incident response as it pertains to electronic communications networks and services. ECSM 008 –Network Monitoring and Incident Response 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 publicly available Electronic Communications Services.

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

4 References

Document	Title
ENISA	Supplement to the technical guideline on Security Measures under the EECC
ENISA	Technical Guideline on Security Measures under the EECC
ENISA	Good Practice Guide for Incident Management
ENISA	How to set up CSIRT and SOC
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
ISO/IEC 27037:2012	Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27037:2016	Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management
NIST	Framework for Improving Critical Infrastructure Cybersecurity v1.1
NIST SP 800-100	Information Security Handbook: A Guide for Managers
NIST SP 800-53 R4	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-61 R2	Computer Security Incident Handling Guide

5 Definitions, Symbols and Abbreviations

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
Incident Handling	Actions of detecting, reporting, assessing, responding

	to, dealing with, and learning from security incidents
Incident Response	Actions taken to mitigate or resolve a security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.
Incident Response Function	A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Security Incident Response Team (CSIRT), a Computer Emergency Response Team (CERT) or Computer Incident Response Capability (CIRC)
Indicator of Compromise	An artefact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.
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;
Playbook	A documented planned course of action in response to anticipated events.
Security Event	Any observable occurrence in a network or system that poses a risk to the security of networks and services.
Security Incident	An event having an actual adverse effect on the security of electronic communications networks or

	services.
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
Threat Intelligence	Data that is collected, processed, and analysed to understand threat actors' motives, targets and attack behaviours.

34 ## 5.2 Symbols

35 Nil

36 ## 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
IDS	Intrusion Detection Systems
IOC	Indicator of Compromise
ISAC	Information Sharing and Analysis Centre
MNO	Mobile Network Operator

MSP	Managed Service Providers
NCSC	National Cyber Security Centre
NOC	Network Operations Centre
SIEM	Security Information and Event Management
SOC	Security Operations Centre
TI	Threat Intelligence

37

38

6 Overview of Risk

Security incidents, including cyber-attacks, have become a part of operating in a connected world. The potential for a successful cyber-attack of an operator's network is not a case of if, but when. In order to best prepare for this eventuality, it is important that operators have an ability to monitor their networks, to detect anomalous or malicious activity, and respond effectively to security incidents. Preventive actions and controls based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented entirely. An incident response capability is therefore necessary for detecting incidents, minimising data loss and destruction and restoring normal network operations.

When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the operator to successfully understand, manage, and recover from an incident. Without an incident response plan, an operator may not discover an attack in the first place, or, if the attack is detected, the operator may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. As a result, the incident could have a greater impact, causing more damage, infecting more systems, and possibly exfiltrate more sensitive data than would otherwise be possible were an effective incident response plan in place.

The importance of effective Network Monitoring and Incident Response was highlighted in EU 5G Security Toolbox, particularly in technical measure 05 - *Ensuring secure 5G network management, operation and monitoring* which states:

> *"Ensure that MNOs run their Network Operation Centres (NOC) and/or Security Operation Centres (SOC) on premise, inside the country and/or inside the EU.*
>
> *The NOC and SOC are a vital component of the MNO's infrastructure in implementing and monitoring the measures for secure network management and operation. They should provide clear visibility and implement effective network monitoring of at least all the critical components and sensitive part of 5G networks, to detect anomalies and to identify and avoid threats, such as, for example, threats to the core network coming from compromised user devices and (IoT).*

Also ensure that MNOs appropriately protect the management traffic of the communications network or service to avoid unauthorised changes to the communications network or service components."

One of the key vulnerabilities identified in the National Risk Assessment, and the coordinated EU Risk Assessment, is the lack of specialised and trained personnel to secure, monitor and maintain networks, therefore it is essential that operators adequately resource their network monitoring and incident response function. ECSM 004 covers training and personnel security matters in greater detail.

7 Security Measures

The operator should implement the Network Monitoring and Incident Response Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
IR.01	The operator shall have adequate resources available to monitor, understand and analyse security-related network activity.
IR.02	The operator shall host[1] their NOC/SOC on premises or located within the EU, EEA or shall operate it in a manner compliant with European electronic communications, security and data protection legislation.
IR.03	Baseline network behaviour shall be understood, through the gathering of logging data from priority areas such as critical network nodes, allowing system abnormalities and malicious activity to be detected.
IR.04	Security events shall be identified and shall trigger appropriate alerts to the NOC/SOC.
IR.05	Security events for priority areas, such as critical network nodes shall be promptly investigated and triaged, and where necessary remediated or escalated appropriately.
IR.06	The operator shall have documented security incident management procedures, including roles and responsibilities, lines of reporting/escalation, contact information and playbooks on how to respond to common security incident types.
IR.07	The operator shall have a standard way of categorising and prioritising incidents, such as by incident type and severity/impact.
IR.08	The incident management process shall be tested through periodic incident response exercises and scenarios.

[1] f using a third party for the provision of NOC/SOC services, the third party must either be an EU/EEA registered company or operate in a manner that is compliant with European electronic communications, security, and data protection legislation.

IR.09	The operator shall have a post-incident/exercise review process, including lessons learned, to improve their resilience and minimize the likelihood or impact of similar incidents occurring.
IR.10	The operator should seek out sources of threat intelligence (TI), including indicators of compromise (IOCs) and should proactively detect, contain, and eradicate malicious activity.
IR.11	Operators shall share the details of significant security incidents with ComReg and appropriate government authorities, as required by legislation, to enhance understanding of the threats, risks and exploitation of Electronic Communications Networks and Services.
IR.12	The operator should participate in sectoral information sharing arrangements, where such arrangements exist.

86

8 Implementation Guidance

The implementation guidance in the following subsections is applicable to the security measures in section 7 as shown in **Error! Reference source not found.** below.

Table 1 - Correlation of implementation Guidance to Security Measures

	IR. 01	IR. 02	IR. 03	IR. 04	IR. 05	IR. 06	IR. 07	IR. 08	IR. 09	IR. 10	IR. 11	IR. 12
8.1	✓		✓	✓	✓	✓	✓	✓	✓	✓		
8.2	✓		✓	✓	✓							
8.3	✓	✓										
8.4	✓		✓	✓								
8.5											✓	✓

8.1 Incident Response Plan

Applicable Security Measures: IR.01, IR.03, IR.04, IR.05, IR.06, IR.07, IR.08, IR.09, IR.10

The Incident response process can be broken down into a number of phases. NIST SP 800-61 outlines four main phases of an incident response process – *Preparation, Detection & Analysis, Containment, Eradication & Recovery* and *Post-Incident Activity*

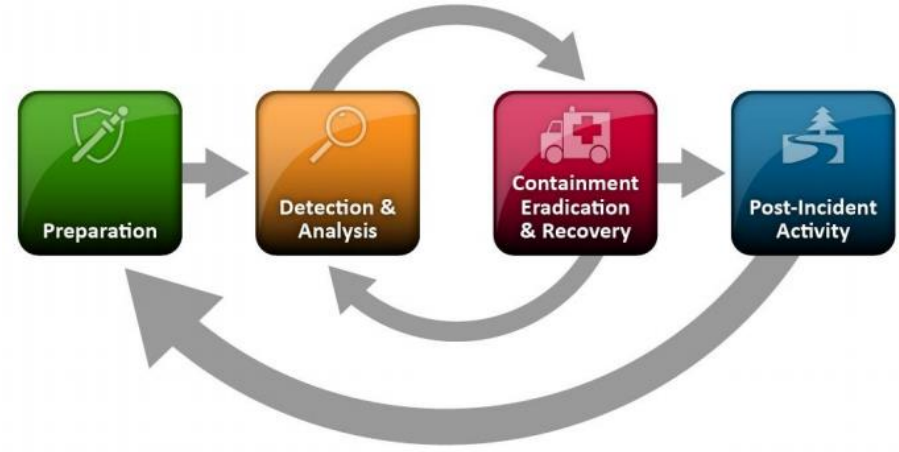

Figure 1 - Incident Response Process

8.1.1 Preparation

The preparation phase of the Incident Response process is essential in not only ensuring operators can respond to security incidents but also preventing incidents by ensuring systems, network and applications are sufficiently secure.

A comprehensive Incident Response Policy and detailed incident response playbooks for common incidents are essential to ensure a smooth response to serious security incidents. As a minimum the policy should include:

- a statement of senior management commitment,
- structure and definition of Incident Response Function,
- roles, responsibilities, and levels of authority,
- the requirements and guidelines for external communications and information sharing
- the escalation process during incident management,
- prioritisation or severity ratings of incidents.

As a minimum Incident Response Functions should have appropriate facilities and tools prepared and available, such as:

- detailed contact information,
- incident reporting and tracking mechanisms,
- hardware and software required to monitor and investigate security events,
- detailed network documentation and data flow charts,
- network baseline information.

Incident prevention is an important aspect of the preparation phase. Further detail on developing a comprehensive security training and awareness programme can be found in ECSM 004.

8.1.2 Detection and Analysis

Security incidents by their very nature are unpredictable, and it is impossible to precisely outline step by step instruction on how to deal with each incident, however, operators should be prepared to deal with the most common attacks. Frameworks such as MITRE ATT&CK[2]

[2] https://attack.mitre.org/

outline the main adversary tactics and techniques and offer a useful and consistent framework which can be used to define, analyse, and respond to cyber security incidents.

During the detection phase the incident response function should focus on identifying any potential IOCs indicating malicious activity. IOCs can include, inter alia, anomalous traffic entering or exiting the network, unknown files, applications, or processes running, suspicious user activity, particularly involving privileged users, unusual log in attempts or spikes in requests.

Data for detecting indicators of compromise can come from numerous sources including, but not limited to:

- alerts from intrusion detection systems (IDS), security information and event management systems (SIEM) or anti-virus (AV)
- analysis from log files or anomalous data flows
- alerts and advisories on vulnerabilities e.g. via system vendors.
- reports from staff within the organisation
- reports from third parties.

Once indicators of a security incident have been detected, the incident response functions should promptly investigate and triage the incident to determine the validity and severity of the alert. Prioritisation is a key aspect of this phase of the incident response process. Incidents should be classified using clearly defined metrics of the incidents likely impact and severity.

The analysis of incidents should follow a predefined process and all actions during the response should be documented. It is also important to gather evidence throughout the incident, primarily in order to resolve the incident, but it may also be required in subsequent legal proceedings. Consider obtaining expert security and legal advice as regards preserving the evidence and adopting chain of custody procedures.

8.1.3 Containment, Eradication and Recovery

Containment is important before an incident overwhelms resources or increases damage. Containment will likely require decisions to be made on shutting down systems or disconnecting from networks and disabling functions. These decisions can be made easier by having pre-determined plans for incident containment.

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user

accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. Eradication and recovery should be done in a phased approach so that remediation steps are prioritized.

Recovery from an incident can take anywhere from minutes to months and may require an entire rebuild of a system that has been fully compromised.

8.1.4 Post Incident Activity

Operators should ensure they fully investigate all major incidents and draft a final incident report including actions taken and recommendations to mitigate future occurrence of this type of incident. In order to better prepare for future incidents as well as to improve the overall incident response process, a lessons learned process is an integral part of incident response. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. The lessons learned process also provides opportunities to train new and future members of staff.

Key metrics on incidents should also be gathered which can aid reporting and tracking the effectiveness of the incident response function.

8.2 Automation

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

Introducing automation to an operator's incident response function to tackle security incidents when they arise assists in achieving timely restoration of services and reduces the opportunities for human errors. Automation is a key enabler for an operator to best use the scarce human security resources reducing the amount of time spent on manual log and alarm reviews, which can reduce the overall time to detect and respond to an incident. Elements of an operator's incident response can be automated, including fully automated playbook actions, semi-automated actions, or approval-based response actions that allow users to review before countermeasures are carried out. As automation technologies advance Artificial Intelligence (AI) is increasingly being used to improve the performance of automation and reducing the number of false positives.

8.3 Appropriate Model

Applicable Security Measures: IR.01, IR.02,

The appropriate model for an operator's network monitoring and incident response function will depend on the risk profile and operational context of the operator. Given the sensitive

nature of the work being carried out, this work should not be conducted outside of the EU/EEA or jurisdictions with legal frameworks consistent with European electronic communications, security, and data protection legislation.

8.3.1 Operator Hosted

Hosting the NOC/SOC on site and staffing with the operator's own staff offers the advantage of retaining complete control and oversight of the network monitoring and incident response functions. This model allows the operator to retain security expertise in-house and may be appropriate for larger operators.

8.3.2 Outsourced

Operator's may choose to outsource their network monitoring and/or incident response function to their parent group, or to a Managed Security Services Provider (MSSP). This can be done in order to save on costs, or to ensure the best use of scarce security expertise and resources. The network monitoring and incident response functions represent some of the most sensitive work that an operator engages in, and extreme care should be taken when this task is outsourced to a third party and the security measures in ECSM 009 – Supply Chain Security need to be strictly adhered to.

8.4 Logging and Monitoring

Applicable Security Measures: IR.01**,** IR.03, IR.04,

Logging is the foundation on which security monitoring and situational awareness are built. Effective logging allows an operator to understand what has happened and how great the impact of an incident was. It also assists in data-based decision making during the response to an incident. Effective logging also allows an operator to understand if their incident response process has been effective and if security controls are operating as they should.

The operator should have a policy for logging and monitoring critical systems and nodes including minimum monitoring and logging requirements, retention period, and the overall objectives of storing monitoring data and logs. They should also have appropriate tools for monitoring systems and collecting logs, as well as raising alerts to the NOC/SOC when security events occur.

8.5 Information Sharing

Applicable Security Measures: IR.11, IR.12

There is maxim that says in security you should cooperate whilst competing in all other areas of business. Security information sharing is one of the key components of effective preparation and response to cyber incidents. By sharing information with other electronic communications operators, other industries, and relevant public authorities, a shared body of knowledge can be developed in order to assist individual operators in preparing for and responding to cyber incidents. The type of information that can be shared includes:

- information relating to cyber threats,
- vulnerabilities,
- indicators of compromise,
- tactics, techniques and procedures,
- cybersecurity alerts and
- configuration tools

The purpose for sharing such information is to help prevent, detect, respond to, or mitigate cybersecurity incidents. In general sharing information helps to enhance the overall level of cybersecurity in particular through:

- raising awareness in relation to cyber threats,
- limiting or impeding the ability of a security threat to spread,
- supporting a range of defensive capabilities,
- vulnerability remediation and disclosure,
- threat detection techniques,
- mitigation strategies,
- response and recovery stages.

There are many forms that such information sharing can take such as meeting the minimum level of statutory obligations regarding incident reporting, bilateral sharing arrangements with other operators, informal information sharing forums through to formal Information Sharing and Analysis Centres (ISACs). ISACs typically have dedicated procedures, ICT platforms, content and conditions of the information sharing arrangements. Further information on ISACs can be found on the ENISA website[3] of including their "ISAC in a box" tool[4] for

[3] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing?tab=details

249 establishing and developing ISAC. It includes activities, documents and tools, everything
250 needed to set up and run an ISAC.

251 A key element in information sharing arrangements is the development of trust between
252 sharing partners, therefore, it is recommended that such arrangements are built
253 incrementally

254

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/view

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 ENISA Good Practice Guide for Incident Management

Good Practice Guide for Incident Management — ENISA (europa.eu)

This guide complements the existing set of ENISA guides that support Computer Emergency Response Teams. It describes good practices and provides practical information and guidelines for the management of network and information security incidents with an emphasis on incident handling.

9.2 ENISA CSIRT SOC Guide

How to set up CSIRT and SOC — ENISA (europa.eu)

This publication provides results-driven guidance for those who are interested in establishing a computer security incident response team (CSIRT) or security operations centre (SOC), and guidance on possible improvements for different types of CSIRTs and SOCs that exist currently. The reader will receive practical guidance on what to focus on during the individual phases of establishment and improvement.

9.3 ISO/IEC 27035-1 Principles of Incident Management

ISO - ISO/IEC 27035-1:2016 - Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management

ISO/IEC 27035-1:2016 presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt. The principles are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance according to their type, size and nature of business in relation to the information security risk situation. It is also applicable to external organizations providing information security incident management services.

9.4 ISO/IEC 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO - ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 27037:2012 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

9.5 NIST SP 800-61 Computer Security Incident Response Guide

Computer Security Incident Handling Guide (nist.gov)

This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications.