Technical Guideline on Reporting Incidents

August 2013

Ref: MCA/O/13-1603 v1.1

Malta Communications Authority
Valletta Waterfront, Pinto Wharf, Floriana, FRN1913
Tel: 00356 21 336 840 Fax: 00356 21 336 846
Email: info@mca.org.mt Web: www.mca.org.mt

DOCUMENT REVISION HISTORY			
Date	Revision	Comments	Authors/ Contributors
June 2013	1.0	First Version	MCA
August 2013	1.1	Inserted a table of contents Inserted page numbers Inserted an email address for the submission of reports	MCA

Table of Contents

1. Introduction

The 2009 reform of the electronic communications EU legislative framework[1] introduced Article 13a into the Framework directive[2], this Article relates to security and integrity of electronic communication networks.

Paragraph 1 of the first part of Article 13a states that Member States should ensure that providers of public communication networks *"take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services"*, and to take measures *"to prevent and minimise the impact of security incidents on users and interconnected networks"*. Paragraph 2 requires providers to *"take all the appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services"*.[3]

Paragraph 3 of the second part of Article 13a requires undertakings providing public communications networks or publicly available electronic communications services to notify the Malta Communications Authority (MCA) of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

At a national level, these requirements have been transposed in Subsidiary Legislation 399.28, with articles 54 and 55 specifically mandating the guaranteeing of network security, integrity and continuity of services, whilst article 56 specifically sets out the obligation to notify the MCA in case of loss of integrity or failure of these networks.

[1] EU Directive 2009/140/EC

[2] Directive 2002/21/EC as amended by Directive 2009/140/EC

[3] (2013) Technical Guideline on Security Measures - ENISA

2. Aim and Objectives

The aim of this document is to provide a standard format of incident reporting that meets the requirements of Article 13a. The objective of reporting is to gather information from network operators about security breaches or major outages that have had significant impact on end users and to obtain information about the root cause of such incidents. This information will serve to conduct trend analyses of major outages or security breaches.

This document is based on the technical guidelines published by the European Network & Information Security Agency (ENISA) and contains excerpts from the ENISA publication – Technical Guideline on Incident Reporting.[4] The document establishes thresholds which will serve as the basis upon which the severity of outages is established and provides technical guidelines to network operators on incident reporting.

On an annual basis the MCA will submit to ENISA and the European Commission (EC) an account of all security breaches and loss of integrity as reported to MCA in line with this guidelines. The objectives of this information gathering is:

- to provide policy makers, the public and the industry with aggregate analyses of incidents which explain the overall frequency and impact of security incidents across the EU
- to facilitate the exchange of experiences and lessons learned among National Regulatory Authorities (NRA's), to allow them to better understand and better address specific types of security incidents or vulnerabilities
- to evaluate the effectiveness of security measures in place , and to issue recommendations and guidance for NRA's, the private sector and policy makers, about security measures.

Initially, the scope of annual reporting to ENISA and the EC is restricted to losses of integrity, that is the incidents with an impact on the continuity of supply of electronic communication services.

[4] (2011 and 2013) Technical Guideline on Reporting Incidents - ENISA

3. Target Audience

This document is addressed to Maltese electronic communications network operators and service providers.

4. Network Outage Reporting Considerations and Guidelines

ENISA, the agency entrusted by the European Commission to contribute towards the security of electronic communications and to the harmonisation of technical and organizational security measures taken by the Member States, defines a Network Incident as "*an event which can cause a breach of security or a loss of integrity of electronic communication networks or services*". It goes further to define a Reportable Incident as *"A breach of security or a loss of integrity that has a significant impact on the operation of electronic telecommunications networks and services"*.

This document shall provide guidance on the thresholds which should trigger a reportable incident or outage whilst ensuring the necessary balance between the risk of significant incidents going unreported and the risk of unduly burdening the operators with voluminous reporting. These thresholds might be revised in light of the experience which shall be gained from operating the outage reporting process.

5. Thresholds for reporting

A security incident can have an impact on the continuity of supply of services or an impact on the security of users and interconnected networks. In case of an impact on the continuity of supply of services over the network the incident is often referred to as an outage or disruption of a service and can be complete or partial.

The threshold for reporting an incident is based on the number of users of a service affected as a percentage of the service provider's user base of the service and the duration of the incident.

The network operators or service providers must send an incident report to the MCA if the incident:

- lasts more than an hour, and the percentage of users affected is more than 15%;

- lasts more than 2 hours, and the percentage of users affected is more than 10%;
- lasts more than 4 hours, and the percentage of users affected is more than 5%;
- lasts more than 6 hours, and the percentage of users affected is more than 2%; or if it
- lasts more than 8 hours, and the percentage of users affected is more than 1%.

	1h - 2h	2h - 4h	4h - 6h	6h - 8h	>8h
1% - 2%	🟩	🟩	🟩	🟩	🟥
2% - 5%	🟩	🟩	🟩	🟥	🟥
5% - 10%	🟩	🟩	🟥	🟥	🟥
10 - 15%	🟩	🟥	🟥	🟥	🟥
>15% of users	🟥	🟥	🟥	🟥	🟥

Figure 1: ENISA Thresholds for NRA reporting based on a combination of duration and the percentage of the user base.

6. Incident Reporting Template

Incident Reporting Form	
Date and time:	**Date and time of notification to MCA:**
Incident Impact	
Impacted services (select one or more):	
Fixed Telephony □	PSTN □ DSL □ Fibre □ Cable □ Other □
Fixed Internet Access □	DSL □ Fibre □ Cable □ Other □
Mobile Telephony □	GSM □ UMTS □ LTE □ Other □
Mobile Internet Access □	GPRS / EDGE □ UMTS □ LTE □ Other □
Other □	

Impact parameters (fill in as appropriate):

Number of users affected per service: ____________

Incident Duration: ____________________________

Geographic spread: ___________________________

Impact on emergency calls □

Impact on Interconnections □

Root Cause

Root Cause Category:

Human Errors □

System Failures □

Malicious Actions □

Natural Phenomena □

Third Party Failure □

Initial Cause:

Cable Cut □

Cable Theft □

Flood □

Storm □

Power Cut □

Power Surges □

Physical Attack □

Cyber Attack □

Bad Change □

Bad Maintenance □

Overload □

Fuel Exhaustion □

Hardware Failure □

Software Bug □

Policy / Procedure Flaw □

None □

No Information □

Other □ ___________________

Subsequent Cause:

Cable Cut □

Cable Theft □

Flood □

Storm □

Power Cut □

Power Surges □

Physical Attack □

Cyber Attack □

Bad Change □

Bad Maintenance □

Overload □

Fuel Exhaustion □

Hardware Failure □

Software Bug □

Policy / Procedure Flaw □

None □

No Information □

Other □ ___________________

Assets Affected by Initial Cause:

Base stations and controllers □ Mobile Switching □ Switches □ Transmission Nodes □

Core Network □ Interconnections □ Backup Power supply □ Power supply system □

No Information □ User and location registers □

Other □ ____

Description
Incident description:
Incident response and recovery actions:
Post-incident actions:
Lessons learnt:
Further remarks (if any):

7. Description of Report Template Fields

This section describes the incident report fields which should be completed by the operators when submitting incident reports to the MCA.

7.1 Date and Time

Details of the date and time when the incident occurred, and the date and time of the MCA was notified.

7.2 Impacted Services

In this field the network operator should provide information about the electronic communication services that were affected by the incident, by indicating a selection of one or more from:

- Fixed telephony
- Mobile telephony
- Fixed internet access
- Mobile internet access

Alternatively, the operator may indicate that another type of service was affected. If possible the operator should also provide further information about the ***technology*** or ***platform*** that was affected.

7.3 Number of Users

In the ***Number of users affected per service*** field the operators should indicate the total number of users affected. For fixed telephony and fixed internet, operators should report the number of subscribers or access lines impacted while for mobile services, the operators should report an estimate, taking into account the normal usage of the affected facilities.

In some occasions more than one service is affected by an incident and the number of users affected per service can be different. In such cases the operators should provide separate numbers per service. In the rare case were operators may not know the exact number of users affected by an incident, the operators should report estimates.

7.4 Incident Duration

In this field operators should indicate the length of time (in hours) there was significant impact on the operation of the services.

7.5 Geographic Spread

In this field operators should provide details about the region or town/s impacted by the incident

7.6 Impact on Emergency Calls

In this field operators should indicate if the incident had an impact on the possibility to call the 112 Emergency services.

7.7 Impact in Interconnections

In this field operators should indicate if there was an impact on the national or international interconnections between providers.

7.8 Root Cause Category

The root cause of an incident is the initial cause of an incident, in other words, the event or factor that triggered the incident. In the field root cause category operators should indicate the root cause of the incident. There are 5 categories which ENISA derived from the secondary legislation issued by FICORA and CESG, the UK National Technical Authority for Information Assurance.

- **Human Errors**

  This category should be used for incidents caused by human errors during the operation of equipment or facilities, the use of tools, the execution of procedures, et cetera.

- **System Failures**

  Operators should use this field for incidents caused by failures of a system, for example hardware failures, software failures or flaws in manuals, procedures or policies.

- **Natural Phenomena**

  This field should be used for incidents caused by severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife and so on.

- **Malicious Actions**

  Operators should tick this field for incidents caused by a deliberate act by someone or some organization.

- **Third Party Failure**

  This category should be used for incidents where the root cause is outside the direct control of the provider, for example, when the route cause occurred at a contractor used for outsourcing, or at an organization somewhere along the supply chain. This category maybe used standalone when the root cause of the incident is unknown. In all other cases, this category should be used in conjunction with one of the other root cause categories.

7.9 Initial Cause

In this field operators may indicate the initial cause of the incident, that is the event or factor that triggered the incident. It must be noted that these detailed causes may fit different root cause categories, depending on the specifics of the setting. For example, a cable cut may be caused by a Human error or by a flaw in a procedure.

7.10 Subsequent Cause

Often incidents involve a chain of event or factors. In this field operators may indicate a cause that subsequently played a role in the incident.

7.11 Assets Affected

Operators should indicate that assets which were first affected in the incident.

7.12 Incident description

In this field the operator should provide a description of the incident and how it initially developed.

7.13 Incident response actions

In this field the operators should provide a description of the actions taken to mitigate the impact of the incident.

7.14 Post-incident actions taken

Operators should provide in this field a description of actions taken to reduce the likelihood or impact of similar incidents.

7.15 Lessons learnt

In this field the operators may provide a description of lessons learnt from the incident or measures which will be implemented on the long-term.

8. Reporting Channel

The MCA should be immediately informed of major incidents and must be frequently updated with the actions being taken to recover the service. Incident reports must be submitted via email address incidentreporting@mca.org within 3 weeks of recovery of the service.

The reports will be collated into one report at the end of the year and the information sent to ENISA. The information provided to ENISA will be generic and will NOT include names of network operators or service providers.