THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
High Commission for National Protection

Governmental CERT

Incident Reporting Guidelines for Constituents (Public)

Version 7.0 - 2024-09-19 (Final)

Procedure (PRO 301)

TLP: **TLP:CLEAR**

Contents

1 Introduction

1.1 Overview

The response to an incident is dependent on the quality of the information reported by the constituent, on the reporting time frame and on the capacity of the organisation in charge of the incident to solve the problem. This procedure defines a reporting method to help the constituent to report an incident to GOVCERT.LU within the required time frame and a common set of terms between GOVCERT.LU and its constituency.

1.2 Purpose

The aim of this procedure is to define guidelines for reporting an incident.

1.3 Scope

This procedure concerns GOVCERT.LU members and its constituency.

1.4 References

1. *POL204 - Information Disclosure Policy*
2. *PRO303 - Incident Categories*

1.5 Abbreviations

Abbreviation	Definition
IDS	Intrusion Detection System
PGP	Pretty Good Privacy

Table 1: Abbreviations

2 Definition

2.1 Event

An event is an occurrence or change of a particular set of circumstances:

NOTE 1: An event can be one or more occurrences, and can have several causes.

NOTE 2: An event can consist of something not happening.

NOTE 3: An event can sometimes be referred to as an ’incident’ or ’accident’.

2.2 Information security incident (or incident)

An information security incident (or incident) is a single or a series of unwanted or unexpected information security events (section 2.3) that have a significant probability of compromising business operations and threatening information security[1].

2.3 Information security event

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

2.4 Critical system

A critical system is a system, an application, data or other resource that is essential to the survival of an organisation. When a critical system fails or is interrupted, core operations are significantly impacted.

2.5 Non critical system

A non critical system is a system, an application, data or other resource which does not have strong impacts to the good operation of a constituent if compromised.

[1] where *information security* means preservation of confidentiality, integrity and availability of information

3 Incident reporting guidelines

Incident reports should include a description of the incident or event, using the appropriate taxonomy, and as much of the following information as possible; however, **reporting should not be delayed in order to gain additional information**:

- Constituent name
- Point of contact information including name, telephone, and email address
- Incident category
- Incident date and time, including time zone
- Location and name of all systems involved in the incident
- Method used to identify the incident (e.g. Intrusion Detection System (IDS), audit log analysis, system administrator)
- Actions[2] done (date, time, result)
- Impact
- Resolution
- Criticality of the system (e.g. national or local system, classified system, etc.)

Constituents should use this model when reporting incidents to GOVCERT.LU. Depending on the criticality of the incident, it is not always feasible to gather all the information prior to reporting. In that case, a constituent should continue to report information as it is collected.

There are several options to report an incident:

- The recommended way is to send an email to `soc@govcert.etat.lu`. This allows to protect incident reports containing sensitive information using Pretty Good Privacy (PGP) encryption.
- Incidents can also be reported by calling the GOVCERT.LU hotline ((+352) 247-88960).
- The last way to report incidents is via the form provided on the website (https://www.govcert.lu). If this reporting method is chosen, it is important to provide contact information (phone number or email address) in case there is a need for updates or feedback. On the other hand, the form allows to file anonymous incident submissions.

An incident report can also use a combination of several methods. A common scenario is for a constituent to report an incident by mail and provide all known information and then follow up with a phone call to clarify any missing information that needs to be added or to discuss any urgent actions that need to be taken.
For general questions except for reporting incidents, you can also write directly to the email address info@govcert.etat.lu or call the secretariat ((+352) 247-88966).

[2] **In order to preserve the evidence and keep investigation capacity for GOVCERT.LU, actions done for containing the incident shall be limited to the strict minimum (no re-installation of the operating system or of any software).**

4 Incident reporting time frame

Information on incident reporting time frames can be found in *PRO303 - Incident Categories*.

5 Incident categories

The incident categories can be found in *PRO303 - Incident Categories*.

6 Disclosure policy

All information addressed to GOVCERT.LU is processed in accordance with the *POL204 - Information Disclosure Policy* available on https://www.govcert.lu.