



## CSIRT DESCRIPTION FOR CERT-XLM RFC2350

### CERT-XLM

Reference	CERT-XLM-RFC2350
Originator	CERT-XLM
Audience	EXCELLIUM   EXTERNAL
Sharing level	TLP:WHITE
Classification	PUBLIC



## Document Versioning

### Approval

	Name	Date
Prepared By:	Dorian Retter	15/04/2022
Verified By:	Paul Jung	15/04/2022
Approved By:	Christophe Bianco	15/04/2022



## History

Version	Date	Author	Description
1.20	15/04/2022	Dorian Retter	Users update and review
1.19	22/12/2021	Paul Jung	Users modification
1.18	17/09/2021	Razvan Ursu	Users modification
1.17	17/08/2021	Paul Jung	Users modification
1.16	26/05/2021	Paul Jung	User modification
1.15	13/11/2020	Paul Jung	User modification
1.14	15/10/2020	Paul Jung	User modification
1.13	09/06/2020	Mathieu Baeumler	User modification
1.12	16/03/2020	Paul Jung	User modification.
1.11	28/11/2019	Paul Jung	Update services and reporting forms
1.10	21/11/2019	Céline Massompierre	Update Mission Statement
1.9	24/07/2019	Céline Massompierre	Link Modification
1.8	01/03/2019	Yoann Chevalier	User and contact email address modification
1.7	05/11/2018	Yoann Chevalier	User modification.
1.6	21/02/2018	Paul Jung	User modification.
1.5	21/01/2018	Paul Jung	User modification.
1.4	20/11/2017	Paul Jung	User modification, form notification, disclose process.
1.3	02/11/2016	Paul Jung	User modifications, working time, location, emails.
1.2	25/03/2016	Paul Jung	User addition.
1.1	03/04/2015	Paul Jung	User addition – Address changes.
1.0	11/09/2014	Paul Jung	Initial version.



## Distribution List

Version	Company	Name
1.20	N/A	Public document

### COPYRIGHT NOTICE AND CONFIDENTIALITY STATEMENT

Copyright © 2013-2022 by Excellium Services or its affiliates and/or licensors. All rights reserved.

This document may contains confidential information about Excellium Services, its affiliates and/or licensors and their respective businesses, business partners and/or customers, all of which is provided in confidence and may be used by the intended recipient only for the sole purpose of the adjudication of the proposal.

It must not be used for any other purpose. Copies of this document may only be provided, and disclosure of the information contained in it may only be made to employees of the intended recipient connected with the negotiations and its named professional advisors who acknowledge its confidential status.

Any recipient must not to disclose this information, either wholly or in part, to any other party without prior permission in writing being granted by Excellium Services or any entity controlled by, controlling, or under common control with Excellium Services.



<b>ABOUT THIS DOCUMENT</b> .....	<b>6</b>
DATE OF LAST UPDATE .....	6
DISTRIBUTION LIST FOR NOTIFICATIONS.....	6
LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND.....	6
AUTHENTICATING THIS DOCUMENT .....	6
<b>CONTACT INFORMATION</b> .....	<b>7</b>
NAME OF THE TEAM .....	7
ADDRESSES.....	7
TIMEZONE .....	7
TELEPHONE NUMBER.....	7
FACSIMILE NUMBER .....	7
OTHER TELECOMMUNICATION .....	7
ELECTRONIC MAIL ADDRESS .....	7
PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION .....	8
TEAM MEMBERS .....	9
OTHER INFORMATION.....	11
POINTS OF CUSTOMER CONTACT .....	11
<b>CHARTER</b> .....	<b>13</b>
MISSION STATEMENT .....	13
CONSTITUENCY.....	13
SPONSORSHIP AND/OR AFFILIATION.....	14
<b>POLICIES</b> .....	<b>15</b>
TYPES OF INCIDENTS AND LEVEL OF SUPPORT.....	15
CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION.....	15
COMMUNICATION AND AUTHENTICATION .....	15
<b>SERVICES</b> .....	<b>16</b>
INCIDENT RESPONSE.....	16
INCIDENT TRIAGE .....	16
INCIDENT COORDINATION .....	16
INCIDENT RESOLUTION .....	16
PROACTIVE ACTIVITIES .....	17
<b>INCIDENT REPORTING FORMS</b> .....	<b>17</b>
<b>DISCLAIMERS</b> .....	<b>17</b>



## About this document.

### Date of last update

This is the 1.20 version released on April 11<sup>th</sup>, 2022.

### Distribution List for notifications

Changes to this document are not distributed by a mailing list, RSS or any other mechanism. Please address any specific questions or remarks to CERT-XLM e-mail address (see chapter *Electronic mail address* )

### Locations where this document may be found

The current version of this CSIRT description document is available in pdf format in the document section on the CERT-XLM WWW site. At the following URL:

<https://excellium-services.com/assets/csirt-rfc2350.pdf>

Please make sure you are using the latest version.

### Authenticating this document

These documents have been signed with the CERT-XLM's PGP key. The main signature is available on our website, under:

<https://excellium-services.com/assets/csirt-rfc2350.pdf.sig>



## Contact Information

### Name of the team

“CERT-XLM”: Excellium CSIRT of Excellium Services S.A.

### Addresses

The primary correspondence address is the Luxembourgish one.

CERT-XLM  
Excellium Services S.A.  
5 rue de Goell  
L-5326 Contern  
Luxembourg

CERT-XLM  
Excellium Services Belgium N.V.  
Orion Bldg, Belgicastraat 13  
B-1930 Zaventem  
Belgium

### Timezone

CET / CEST

- GMT+01:00 in wintertime (from last Sunday in November to last Sunday in March).
- GMT+02:00 during summertime (from last Sunday in April to last Sunday in October).

### Telephone number

- +352 262 039 64 708 Cert-XLM direct number (Business hours).
- +352 661 348 273 Excellium Services CSOC (24/7).

### Facsimile number

Nonavailable.

### Other Telecommunication

Nonavailable.

### Electronic mail address

All incident report should be submitted to <[emergency\(at\)excellium-services.com](mailto:emergency@excellium-services.com)>.

The team may be contacted to <[cert\(at\)excellium-services.com](mailto:cert(at)excellium-services.com)>. This email alias relays emails to the human(s) on duty for the CERT-XLM.



## Public keys and other encryption information

The CERT-XLM <[cert\(at\)excellium-services.com](mailto:cert@excellium-services.com)> has a PGP key, with the KeyID **0xD74E5AC0** the related fingerprint is **8D78D1A67F2BAFDE41B74DBA67B311E5D74E5AC0**.

The Incident mailbox <[emergency\(at\)excellium-services.com](mailto:emergency@excellium-services.com)> has the key PGP, with the KeyID **0x42662EFE**, the related fingerprint is **F27E7CE46E424205A68F2B9F4F753C7942662EFE**.

The public key and its signatures can be found at the usual large public key servers, or on CERT-XLM web site:

- for <[cert\(at\)excellium-services.com](mailto:cert@excellium-services.com)>, under:
  - o [https://excellium-services.com/assets/CERT-XLM\\_PKEY.asc](https://excellium-services.com/assets/CERT-XLM_PKEY.asc)
- for <[emergency\(at\)excellium-services.com](mailto:emergency@excellium-services.com)>, under:
  - o [https://excellium-services.com/assets/EMERGENCY\\_PKEY.asc](https://excellium-services.com/assets/EMERGENCY_PKEY.asc)

Each CERT-XLM team member also has a nominative OpenPGP public key.





## Team members

CERT coordination will be performed by **Paul Jung**. All team members, along with their areas of expertise and contact information, are listed below:

### Luxembourgish Core Team

Name	Email	KeyID	Role
Paul Jung	pjung(at)excellium-services.lu	0x2BD01DE5	Coordinator
	<b>Fingerprint</b>	B851F185CBE40165388E840FFDC487D42BD01DE5	
Arnaud Garrigue	agarrigue(at)excellium-services.lu	0xB321CA08	Incident handler
	<b>Fingerprint</b>	76CDB8B53DF109301290FE7A12B5A9EAB321CA08	
Guenaëlle De Julis	gdejulis(at)excellium-services.lu	0xC38E1350	Incident handler
	<b>Fingerprint</b>	F43D8ECDB157C59767CA9F8EE5D441D0C38E1350	
Jonathan Scoupreman	jscoupreman(at)excellium-services.lu	0xAD971C07	Incident handler
	<b>Fingerprint</b>	4BCFE22D29E30436EDF48E5A6802C48EAD971C07	
Alexandre Reynaud	areynaud(at)excellium-services.lu	0xEF1E4CA3	Incident handler
	<b>Fingerprint</b>	1988A426E51EB36E8E66719AF004CC2DEF1E4CA3	
Mathieu Baeumler	mbaeumler(at)excellium-services.lu	0xE1E6CEDC	Incident handler
	<b>Fingerprint</b>	010788739CC014DCFE0B1322D2B8AE08E1E6CEDC	
Jean Luc Davenne	jdavenne(at)excellium-services.lu	0xC699 6D99	Incident handler
	<b>Fingerprint</b>	A07D A014 0404 6BFB 972A E674 F10F C6DF C699 6D99	
Adrien Gerome	agerome(at)excellium-services.lu	0x7683DCFE	Incident handler
	<b>Fingerprint</b>	736D 0C3B C24A 993B 5EC4 1C81 5CD8 5299 7683 DCFE	



## Belgium Core Team.

Name	Email	KeyID	Role
Dorian Retter	dretter(at)excellium-services.be	0xC43BF8E4	Incident handler
	<b>Fingerprint</b>	B368290A6D2AEE7877454DE3B7E01D58C43BF8E4	
Guillaume Granjon de Lépiney	ggranjon(at)excellium-services.be	0xE2FD5ED1	Incident handler
	<b>Fingerprint</b>	3F741CB302B72FA192845A9B1928ADBCE2FD5ED1	

## Senegal L1 Incident handling.

Name	Email	KeyID	Role
Sokhna Fall	sfall(at)suricatesolutions.com	0x6BA7867D	Incident handler
	<b>Fingerprint</b>	333E64E8518D2A133B99BEDA3F1A492C6BA7867D	
Mamadou Mansor Fall	mmfall(at)suricatesolutions.com	0xA9696DD4	Incident handler
	<b>Fingerprint</b>	C70029E6AD4D0DAADA111DFB322FCDDDA9696DD4	
Cherif Abdoul Mazid	cmazid(at) suricatesolutions.com	0xAA0294A3	Incident handler
	<b>Fingerprint</b>	E35E2F1F08AED336114E998BF0899C5CAA0294A3	

Software and system support may be performed by the following team.

Name	Email	KeyID	Role
Benjamin Fuhro	bfuhro(at)excellium-services.be	0x343131B7	Support
	<b>Fingerprint</b>	BC091234C3176DAF0A5FFD8237C6A6F6343131B7	



**Additional L1 Incident handling** may be performed by the following team.

Name	Email	KeyID	Role
Sebastien Kaiser	skaiser(at)excellium-services.com	0x7135874A	Incident handler
	<b>Fingerprint</b>	325EC97B5EB358DEABBE143556ADCD9E7135874A	

**Business and legal support** team members are:

Name	Email	KeyID	Role
Christophe Bianco	cbianco(at)excellium-services.com	0xE684F47E	Business support
	<b>Fingerprint</b>	46554E3FCOD37028FE0965AD8C096982E684F47E	
Xavier Vincens	xvincens(at)excellium-services.com	0x30D41DA1	Business support
	<b>Fingerprint</b>	837F21DAAB6B2A4FC58D7584FD20EBE230D41DA1	

## Other Information

General information about the CERT-XLM, as well as links to various recommended security resources, can be found at <https://www.excellium-services.com/CERT-XLM>

## Points of Customer Contact

The preferred method for contacting the CERT-XLM is via e-mail at <[cert\(at\)excellium-services.com](mailto:cert(at)excellium-services.com)>; E-mails sent to this address will be automatically forwarded to the on-call person if you require urgent assistance, put “[URGENT]” in your subject line.

Emails could be encrypted using PGP. CERT-XLM public key information are detailed in the chapter



*Public keys and other encryption information.*

If it is not possible (or not advisable for security reasons) to use e-mail, the CERT-XLM can be reached by telephone during regular office hours. (See chapter *Telephone number*) Outside these hours, incidents will be registered 24/7 through its SOC. In this case, use the emergency number referenced in chapter *Telephone number*

If possible, when submitting your report, use the form mentioned in section *Incident Reporting Forms*.



## Charter

### Mission statement

CERT-XLM is a dedicated team part of Excellium Services S.A, and acts as the Computer Security Incident Response team (CSIRT) for Excellium Group S.A.

The team's purpose is twofold: first, it implements proactive measures to reduce the risks of computer security incidents for Excellium Group S.A and its constituencies, but also any customer requiring help to do so. Secondly, CERT-XLM will provide assistance to them to respond adequately to such incidents.

CERT-XLM will address every kind of computer security incidents already ongoing or threatening to occur in the constituencies' networks. The incidents are first prioritized according to their apparent severity and extent. Then the level of support given by CERT-XLM might vary depending on the type of the incident or issue, its severity and the CSIRT's available resources, but in any case, a response will be always be provided. Additionally, CERT-XLM will release security notices based on relevancy of information.

To ensure its mission, CERT-XLM has been given the mandate to warn application owners and users of known security issues and require fix to security configurations. Additionally, CERT-XLM will report directly relevant security issues related to Excellium Group S.A. and constituencies to Excellium Group S.A. CISO and managing partners.

This team establishment dates from January 2014, and a funding model has been put in place to ensure the long-term stability of this CSIRT.

CERT-XLM will occasionally work in cooperation with various CERTs and Security Operations Centers (SOC). CERT-XLM can also act as a CSIRT bridge to *Professionnels du Secteur Financier (PSF)* entities in Luxembourg to improve reaction and coordination in case of incidents.

### Constituency

CERT-XLM is the Computer Security Incident Response Team of Excellium Services S.A.

The constituency will cover various TLD, Internet Public ASN and IP addresses located/originated and/or operating in/from his customers.

**Constituency type:** Mixed

**Constituency sector:** Commercial



## Sponsorship and/or affiliation

CERT-XLM is a private CSIRT. It is owned, and operated by Excellium services.  
It maintains relationships with various CSIRTs in Luxembourg and Belgium.

CERT-XLM is listed as team member of CERT.lu since 2015

<https://www.cert.lu/#members>

CERT-XLM is officially listed as accredited team since 23 January 2015.

<http://www.trusted-introducer.org/directory/teams/cert-xlm.html>

CERT-XLM is officially member of FIRST since 23 December 2019.

<http://www.trusted-introducer.org/directory/teams/cert-xlm.html>

CERT-XLM is member of Cyber Security Coalition (Belgium) since 8 January 2021.

<https://www.cybersecuritycoalition.be/members/>



## Policies

### Types of Incidents and Level of Support

CERT-XLM addresses all types of computer security incidents which occur, or threaten to occur, in the constituency networks. The level of support given by CERT-XLM will vary depending on the type and severity of the incident or issue and CERT's available resources. However, in all cases, some responses will be made.

Incidents will be prioritized according to their apparent severity and extent.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. The CERT-XLM will support the latter people.

### Co-operation, Interaction and Disclosure of Information

CERT-XLM will exchange all necessary information with other CSIRTs as well as with affected parties' administrators.

CERT-XLM will protect sensitive information in accordance with relevant regulations and policies, in particular regarding the rules requested by the CSSF (*Commission de Surveillance du Secteur Financier*) and the constraints of a support PSF entity.

CERT-XLM will append Light Traffic Protocol when sharing information with teams that support it and will honor such protocol if present.

For Vulnerabilities, CERT-XLM will follow his own responsible disclosure process. This process is available on demand.

### Communication and Authentication

In view of the types of information that CERT-XLM deals with, telephones will be considered sufficiently secure to be used even unencrypted.

Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data.

If it is necessary to send highly sensitive data (i.e. information classified as Confidential) by e-mail, encryption (preferably PGP) will be used.

All e-mail or data communication originating from CERT-XLM will be digitally signed, using the generic PGP key mentioned above or the CERT team members own signature keys.



## Services

### Incident Response

CERT-XLM will assist system owner in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incidents management.

### Incident Triage

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

### Incident Coordination

- Determining the initial cause of the incident.
- Facilitating contact with other sites which may be involved.
- Facilitating contact with the constituency and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable .

### Incident Resolution

Note: This set of service includes also incident response on-site.

- Technical analysis.
- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- Collecting evidence where criminal prosecution, or University disciplinary action, is contemplated.

In addition, CERT-XLM will collect statistics concerning incidents and threats which occur within his customers and will notify the community as necessary to assist it in protecting against known attacks.

For requesting CERT-XLM services please refer to section *Incident Reporting Forms* and *Contact Information* for points of contact.

Please remember that amount of assistance will vary as described in section *Mission statement*.





## Proactive Activities

Regarding his resources CERT-XLM will coordinates and maintains the following services:

- List of vulnerabilities.
- Threat notification.
- Training and educational services.

## Incident Reporting Forms

CERT-XLM does not use any Incident Reporting Forms, we strongly encourage anyone reporting a security incident to use communication by email as described in chapter “Electronic Mail Address”.

## Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT-XLM assumes no responsibility for errors or omissions, or for damages.

**[End of document]**