proximus NXT
cybersecurity

# Description of PXS-LU-CSIRT

## Proximus Luxembourg
## Cybersecurity Incident Response Team

# Table of contents

# 1. About this document

This document is the description of the Cybersecurity Incident Response Team of Proximus Luxembourg also known as *PXS-LU-CSIRT*. Proximus NXT is the commercial brand of Proximus Luxembourg S.A. active on the B2B market.

This description document is performed in line with the rfc2350 document entitled Expectations for Computer Security Incident Response. It provides general information about the computer security incident response team (CSIRT) of Proximus NXT / Proximus Luxembourg S.A., its contact information, its scope of responsibilities, the procedures to contact the team, the set of services offered and how to report an incident.

## Date of last update

This is version 3.2, issued on 2026-07-21

This version is valid until superseded by a later version. Changes between two successive versions are marked with a vertical line, except for major version change. In the latter, the document shall be considered as fully revised.

| Version 1 | Version 2 | Version 3 |
|---|---|---|
| 1.0 2015-09-22<br>1.1 2015-10-16<br>1.2 2015-10-28<br>1.3 2015-12-01 | 2.0 2016-02-03<br>2.1 2016-04-11<br>2.2 2017-03-08<br>2.3 2017-06-16<br>2.4 2017-09-01<br>2.5 2017-10-09<br>2.6 2018-10-02 | 3.0 2023-12-07<br>3.1 2024-11-12<br>3.2 2026-07-21 |

## Distribution list for notifications

Currently Proximus Luxembourg S.A. does not use any distribution list to notify about changes in this document. In case of questions or remarks about this document, address them to PXS-LU-CSIRT e-mail address (refer to section 2).

# Location where this document may be found

The up-to-date current version of this CSIRT description document is available at the PXS-LU-CSIRT website at:

https://www.proximusnxt.lu/fr/csirt
or
https://www.proximusnxt.lu/en/csirt

Please make sure you are using the latest version. Printer and paper versions are not managed.

# Authenticating this document

This document has been signed with the PXS-LU-CSIRT's PGP key.

The signature is on our web site, under:

https://www.proximusnxt.lu/fr/csirt
or
https://www.proximusnxt.lu/en/csirt

# 2. Contact information

## Name of the team

Proximus Luxembourg Cyber Security Incident Response Team

Short name: PXS-LU-CSIRT

## Address

Proximus Luxembourg CSIRT
c/o Cybersecurity Services (Joany BOUTET)
Z.A. Bourmicht - 18, rue du Puits Romain
L-8070 Bertrange
Grand Duchy of Luxembourg

## Time zone

Central European Time (GMT+0100, GMT+0200 from April to October)

## Telephone number

+352 450 915 – 1

## Facsimile number

+352 450 911

## Electronic mail address

Incident reports, notification and/or any CSIRT related communications should be addressed to csirt(at)proximus(dot)lu. Operational issues should be addressed to telecomsd(at)proximus(dot)lu.

## Other telecommunication

Generic email address is contact(at)proximus(dot)lu.

The abuse contact information email address for Autonomous System Number (ASN) AS56665 is abuse(at)proximus(dot)lu.

# Public keys and other encryption information

PXS-LU-CSIRT has an OpenPGP public key, whose KeyID is 6E2EA9F8 and whose fingerprint is B6FB 4A00 5437 BA53 69D2 C379 F121 EBA2 6E2E A9F8.

Each PXS-LU-CSIRT team member has also a respective OpenPGP public key that you can also fetch from the PXS-LU-CSIRT's website and from public key servers.

# Team members

PXS-LU-CSIRT is operated by Proximus Luxembourg S.A. engineers and consultants. The Core-Team (in alphabetical order) is composed of:

| Name | Email | PGP Fingerprint |
|---|---|---|
| Joany BOUTET<br>CSIRT Leader | joany.boutet(at)proximus(dot)lu | EF08 622E 43FA EF0B 1625 539E E687 467E EDE7 D640 |
| Nicolas CARDOSO<br>Incident Manager | nicolas.cardoso(at)proximus(dot)lu | 4AFA 8B3C BBA0 231C 37E3 EEA6 D69D 56D4 693A 539E |
| Sebastien DELMOTTE | sebastien.delmotte(at)proximus(dot)lu | 308E F5F8 4030 F21C 070B 7891 84D3 D268 A37A 10D1 |
| Anthony FEY | anthony.fey(at)proximus(dot)lu | 70D4 52D2 284E 6159 168F A56B 40E2 9609 CFFA F3E7 |
| Damien GITTER | damien.gitter(at)proximus(dot)lu | E00C 7EB4 E122 2F4E 51BD 4AD6 89D6 ABF5 39D4 52D4 |
| Sebastien GRELOT | sebastien.grelot(at)proximus(dot)lu | 9D08 959A AC27 5FCB C2C4 ECCA 79C8 C5D5 8B8F A98C |
| Frederic HAUSS<br>Cybersecurity Services & CSIOC Manager | frederic.hauss(at)proximus(dot)lu | C20A 604D 86A9 B04E 202A 38C9 9C14 F308 FF59 04CE |
| Jean-François JOB<br>Security Operations Leader | jeanfrancois.job(at)proximus(dot)lu | B5AD 8ABE 4247 BFC8 93A2 CCA4 9366 3C44 0917 F7F1 |
| Moade KHLIFI | moade.khlifi(at)proximus(dot)lu | 1C23 DCE1 0AF1 9E98 549F 16CC 2E6F 374E C1C9 9C6D |
| Ilyes MAHNANE | ilyes.mahnane(at)proximus(dot)lu | 3828 B4BE 84F7 646B 4582 62DE 636F CE09 7B25 168C |
| Cédric MAUNY<br>Strategic Advisor, Cybersecurity | cedric.mauny(at)proximus(dot)lu | 6F24 CD91 0D60 B8C8 7779 E102 71A9 07DB CAB5 8406 |
| Gilles MULHEIMS | gilles.mulheims(at)proximus(dot)lu | - |
| Kevin TRIMBORN | kevin.trimborn(at)proximus(dot)lu | E557 56B0 F5CF DE3F DA5A 5675 FE80 2364 2A53 EC01 |
| Baptiste VIRY | baptiste.viry(at)proximus(dot)lu | F277 73C7 FC7E F43E B71D 4B05 63C0 220B 2C14 CBB5 |
| | | |

# Other information

Any other information about PXS-LU-CSIRT can be found at

https://www.proximusnxt.lu/fr/csirt
or
https://www.proximusnxt.lu/en/csirt

General information about Proximus NXT, the commercial brand of Proximus Luxembourg S.A. active on the B2B market can be found at https://www.proximusnxt.lu.

General information about Proximus Luxembourg S.A. can be found at https://www.proximus.lu.

# Points of customer contact

The preferred method for contacting PXS-LU-CSIRT is via e-mail at csirt(at)proximus(dot)lu. We encourage our constituency (customers) to use PGP encryption when sending any sensitive information to PXS-LU-CSIRT.

If it is not possible (or not advisable for security reasons) to use e-mail, PXS-LU-CSIRT can be reached by telephone during regular office hours. Off these hours, a voicemail message proposes a redirection to a third-party phone number, who will transmit the message to Proximus Luxembourg S.A.

PXS-LU-CSIRT hours of operation are restricted to regular business hours: 09h00-17h00 CET from Monday to Friday except during Luxembourg's public holidays.

Outside of these hours and in case of emergency, the telecomsd(at)proximus(dot)lu email address, mainly dedicated to operational problems, can be contacted.

When submitting your incident report, please use the form mentioned in section 6.

# 3. Charter

## Mission statement

PXS-LU-CSIRT is the response entity for the cybersecurity and computer security incidents related to the Autonomous System Number (ASN) AS56665.

Mission of PXS-LU-CSIRT is to provide the following set of information security incident management related services to its constituency:

- provide a response facility to ICT-incidents,
- setup of a Central-Point-of-Contact for ICT-Incidents between Proximus Luxembourg S.A., its constituency and various CSIRTs,
- support Proximus Luxembourg S.A. internal operational teams to respond from ICT-related incidents,
- coordinate communication among various incident response teams, and
- provide security expertise and advice.

## Constituency

The scope of responsibility of PXS-LU-CSIRT applies to the Autonomous System Number (ASN) AS56665 also known as AS-PROXIMUS and covers services that Proximus Luxembourg S.A. offers to its customers and to its employees (ISP customers base and Commercial organizations on the B2B market).
The full AS56665 is owned by Proximus Luxembourg S.A. however, it includes IP addresses that are statically assigned to customers for which Proximus Luxembourg S.A. will not intervene outside of the legal framework that we are bound to operate in. Consequently, the Proximus Luxembourg S.A.'s B2B customers using IP address(es) belonging to the Autonomous System AS56665 are all included in the constituency of PXS-LU-CSIRT wherever their physical location.

The scope of activities of PXS-LU-CSIRT covers incidents originated from or targeted the Autonomous System AS56665. However, all related incidents happening within the AS itself may not be considered in the scope of the covered incidents but PXS-LU-CSIRT can also provide incident response coordination and support to the extent possible depending on its resources.

PXS-LU-CSIRT may not have the authority to respond to every reported security events, vulnerabilities and incidents related to AS56665 and associated ranges of IP addresses. In particular, PXS-LU-CSIRT does not have the mandate to intervene for

responding[1] to information security incidents and vulnerabilities that are occurring on infrastructures, components and information systems not owned by Proximus Luxembourg S.A. In particular that means that equipment owned by our customers does not fall in the scope of PXS-LU-CSIRT's responsibilities. However, in such a case and depending on the situation and to the extent possible depending on its resources, PXS-LU-CSIRT may coordinate and/or support the incident response and vulnerability response and alerts & warning services with the interested parties in compliance with the Law.

The services proposed in section 5 can also be subscribed by any past, current or future customer of Proximus Luxembourg S.A.

## Sponsorship and/or Affiliation

PXS-LU-CSIRT is a private CSIRT, defined, owned and operated by Proximus Luxembourg S.A. from the territory of the Grand-Duchy of Luxembourg. PXS-LU-CSIRT maintains relationships and affiliations with the public and private CSIRT members of the CERT.lu initiative in Luxembourg.

PXS-LU-CSIRT was renamed in November 2024, formerly known as Telindus-CSIRT. It was established on 2015, September 22nd, Listed by Trusted-Introducer since 2015, October 15th and is currently Accredited since 2016, March 25th. The affiliation and accreditation to Trusted-Introducer is maintained up-to-date and still valid.

## Authority

PXS-LU-CSIRT operates under the auspices of, and with authority delegated by Proximus Luxembourg S.A.

[1] Collection, Detection, Assessment, Qualification, Confirmation, Containment, Eradication and Recovery

# 4. Policies

## Types of incidents and level of support

PXS-LU-CSIRT is authorized to address all types of computer and information security incidents which occur or threaten to occur, within its constituency.

The level of support given by PXS-LU-CSIRT varies depending on the type and severity of the incident or issue, the type of the impacted constituent, the size of the user community affected, and PXS-LU-CSIRT's resources at the time; though in all cases some response will be made. Incidents will be prioritized according to their apparent severity and extent.

End-users are expected to contact their security point of contact, systems administrator, network administrator or department head for assistance. PXS-LU-CSIRT aims in providing support in the frame of its services and abilities to the system administrators, network administrators or department heads within the limit of its constituency and services. No support is provided to the end-user by PXS-LU-CSIRT.

## Co-operation, interaction and disclosure of information

As operated by Proximus Luxembourg S.A., PXS-LU-CSIRT shall comply with same regulations applicable to Proximus Luxembourg S.A. Therefore, PXS-LU-CSIRT exchanges necessary information with other CSIRTs as well as with Constituents' and affected parties' security point-of-contact in accordance with regulations applicable to Proximus Luxembourg S.A.

Those applicable regulations include but not limited to:

- Luxembourgish sector-specific Regulations and Rules of CSSF (Commission de Surveillance du Secteur Financier) considering Proximus Luxembourg S.A. is acting as support FSP (Financial Sector Professional)
- ILR (Institut Luxembourgeois de Régulation) considering Proximus Luxembourg S.A. is acting as telecom operator in Luxembourg.

When co-operating, interacting and disclosing information, other Luxembourg's local rules and legislation are also taken into consideration by PXS-LU-CSIRT, including but not limited to:

- Data protection and privacy of personal information
  - European General Data Protection Regulation (EU) 2016/679 (the "GDPR")
- Electronic communications services and networks
  - Laws of 27 February 2011 (the Paquet Telecom) designed to provide set of rules for the entire electronic communication services and networks.
- Any other specific laws and regulations applying to our customer's activities.

PXS-LU-CSIRT recognizes and supports Information Sharing Traffic Light Protocol[2] and appends it when sharing information with teams that support it, and will honor such information if present. All sensitive data (such as but not limited to personal data, system configurations, and known vulnerabilities with their locations) are encrypted if they have to be transmitted over unsecured environment, as stated below.

## Communication and authentication

In view of the types of information that PXS-LU-CSIRT 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 by e-mail, encryption (preferably PGP) will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

All e-mail or data communication originating from PXS-LU-CSIRT will be digitally signed, using the generic PGP key mentioned above or the PXS-LU-CSIRT agents' own signature keys.

If deemed necessary, especially when there is need to exchange high volume of information, PXS-LU-CSIRT could also use repository systems as alternative communication means. Such repositories will always be provided in line with the above-mentioned secure approach. Such repository systems will be owned, managed and hosted by Proximus Luxembourg S.A. in line with applicable Regulations applicable to Proximus Luxembourg S.A.

[2] As specified at https://www.first.org/tlp/docs/tlp-letter.pdf

# 5. Services

The set of services listed and described below are either performed by member of the core-team of PXS-LU-CSIRT or subcontracted to specialized teams at Proximus Luxembourg S.A. to the extent possible depending on its resources.

## Reactive services

PXS-LU-CSIRT proposes and provides the set of following reactive services:

- Alerts and Warnings
- Incident handling
  - Incident analysis
  - Incident response support
  - Incident response coordination
- Forensic analysis
- Malware analysis
- Vulnerability handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination

## Proactive services

PXS-LU-CSIRT proposes and provides the set of following proactive services to the extent possible depending on its resources:

- Announcements
- Threat Intelligence
- Threat Hunting
- Security audits or assessments
  - Infrastructure review
  - Best practice review
  - Scanning
  - Penetration testing
- Security and network equipment configurations audit
  - Source code review
- Configuration and maintenance of security tools, applications, and infrastructures

# Security quality management services

PXS-LU-CSIRT proposes and provides the set of following security quality management services to the extent possible depending on its resources:

- **Risk Analysis**
  - Identify and assess your risks an evaluate security posture of your assets
  - Prioritize your security investments, providing optimal security in a cost-effective manner by efficient resources management

- **Security consulting**
  - For governance
    - Align your information security program activities with organizational goals and business priorities
    - Ensure security management and activities contributes to the process of value creation

  - For compliance
    - Translate regulatory requirements into effective and practicable security policies and controls
    - Lever compliance investments to increase the effectiveness of security controls

- **Awareness building**
  - Protect your assets by raising information security awareness of your staff

- **Education/Training**
  - Increase business value by improving the knowledge and skills of your staff

- **Security infrastructure management**
  - Assistance for security architecture design.
  - Implementation of security infrastructures and security devices
  - Expertise, engineering, installation, configuration and maintenance of security solutions
  - Maintenance of security solutions
  - Security audits and review of security solutions
  - Logs analysis

- **Ethical hacking**
  - Vulnerability assessment and evaluation
  - Penetration testing
  - Adversary Simulation
  - Source code review
  - Social engineering

- **Purple Teaming**
  - Through Adversary Simulation and Adversary Emulation

According to the specificities of these services, some may be outsourced to internal security consultancy departments of Proximus Luxembourg S.A. or any other departments of Proximus Luxembourg S.A. such as the Proximus Luxembourg Training Institute relevant for the different services provided.

# 6. Incident Response Form

PXS-LU-CSIRT has created a local form designated for reporting incidents to the team. We strongly encourage anyone reporting an incident to fill it out.

The current version of the form is available at:

> https://www.proximusnxt.lu/fr/csirt
> or
> https://www.proximusnxt.lu/en/csirt

# 7. Disclaimer

While every precaution will be taken in the preparation of information, notifications and alerts, PXS-LU-CSIRT assumes no responsibility for errors, omissions or for damages resulting from the use of the information contained within.