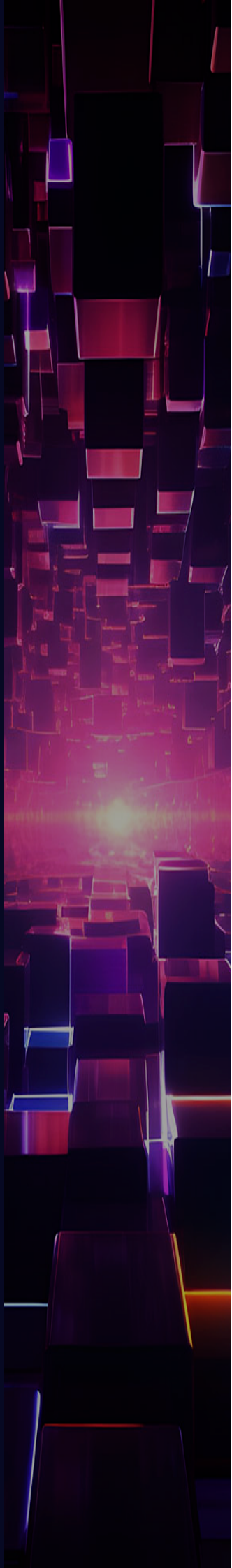
TLP:CLEAR

CSIRT LEXFO

RFC2350 Description

Réf. LEXFO-CSIRT-RFC2350-v1.2



Lexfo

VERSION 1.2
PUBLISHED ON 2024-04-22

TLP:CLEAR

Document references

Document status

Version	Date	Status
V 1.0	2020-04-05	Document validation
V 1.1	2020-04-28	Update of contact information and redesign of the layout (TLP)
V 1.2	2024-04-22	Update of LEXFO's corporate identity, URLs and contact details

Contacts

LEXFO contacts	Position	Email
Samuel DRALET	CEO	s.dralet@lexfo.fr
Sébastien CHAUDRON	CSIRT Director	s.chaudron@lexfo.fr
Wandrille KRAFFT	DFIR Manager	w.krafft@lexfo.fr
Maxime CHOUQUET	DFIR Associate Manager	m.chouquet@lexfo.fr

Reminder of the Traffic Light Protocol[1] (TLP) for information sharing:

TLP:RED For the eyes and ears of *individual* recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

TLP:AMBER Limited disclosure, recipients can only spread this on a need-to-know basis within their *organization* and its *clients*. Note that **TLP:AMBER+STRICT** restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization **only**, they must specify TLP:AMBER+STRICT.

TLP:GREEN Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

TLP:CLEAR Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

[1] Reference to FIRST document: https://www.first.org/tlp/docs/tlp-a4.pdf

Table of contents

1 Document Information

This document contains a description of CSIRT-LEXFO in accordance with RFC 2350[2] specifications. It provides basic information about CSIRT-LEXFO, describes its responsibilities and services offered.

1.1 Date of Last Update

Version 1.2 published on 2024-04-22

1.2 Distribution List for Notifications

There is no distribution list for notifications. This document is kept up to date at the location specified in section 1.3. Please send questions about updates to team email address: csirt@lexfo.fr.

1.3 Locations where this Document May Be Found

The current and latest version of this document is available on the CSIRT-LEXFO's website at:

https://lexfo.fr/LEXFO-CSIRT-RFC2530-v1.1.pdf

1.4 Authenticating this Document

This document has been signed with the PGP key of CSIRT-LEXFO (See section 2.8).

1.5 Document Identification

Title	LEXFO-CSIRT-RFC2350-v1.2
Version	1.2
Date of publication	2024-04-22
Expiration	This document is valid until the publication of a new version.

2 Contact Information

2.1 Name of the Team

- Official name: CSIRT LEXFO
- Short name: CSIRT-LEXFO

[2] http://www.ietf.org/rfc/rfc2350.txt

2.2 Address

CSIRT LEXFO
17 avenue Hoche
75008 PARIS

2.3 Time Zone

Central European [Summer] Time (CET/CEST), Europe/Paris (GMT+01, and GMT+02 on DST).

2.4 Telephone Number

Main number (duty office): 01 40 17 93 00

2.5 Facsimile Number

Not applicable.

2.6 Other telecommunication

Not applicable.

2.7 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving CSIRT-LEXFO, please contact us at: csirt@lexfo.fr.

2.8 Public Keys and Encryption Information

PGP is used for functional exchanges with CSIRT-LEXFO:

- User ID: CSIRT-LEXFO
- Key ID: C7D6A1AF7656FD94
- Fingerprint: 6F88 8EC4 2868 5CE0 7490 485C C7D6 A1AF 7656 FD94

The public PGP key is available at: https://lexfo.fr/CSIRT-LEXFO_public_key.asc

2.9 Team Members

LEXFO contacts	Position	Email
Sébastien CHAUDRON	CSIRT Director	s.chaudron@lexfo.fr
Wandrille KRAFFT	DFIR Manager	w.krafft@lexfo.fr
Maxime CHOUQUET	DFIR Associate Manager	m.chouquet@lexfo.fr

The list of CERT-LEXFO members is not publicly available.

2.10 Other Information

See our web site at https://lexfo.fr/ for additional information about CSIRT-LEXFO.

2.11 Points of Customer Contact

CSIRT-LEXFO prefers to receive incident reports via e-mail at csirt@lexfo.fr. Please use our cryptographic key to ensure integrity and confidentiality. In case of emergency, please specify the [URGENT] tag in the subject field in your e-mail.

CSIRT-LEXFO's hours of operation are 7/7 24h all year long.

3 Charter

3.1 Mission Statement

CSIRT-LEXFO is a private CSIRT team delivering Security services, mainly in France.

It has two main objectives:

- First, to assist its customers in implementing proactive measures to reduce the risks of computer security incidents.
- Second, to assist its customers in responding to such incidents against both intentional and opportunistic attacks that would hamper the integrity of their IT assets and harm their interests whenever they occur. The scope of CSIRT-LEXFO's activities covers prevention, detection & analysis, response, and recovery. CSIRT-LEXFO oversees digital forensics and incident response (DFIR) activities.

CSIRT-LEXFO will operate according to the following key values:

- CSIRT-LEXFO strives to act according to the highest standards of ethics, integrity, honesty, and professionalism.
- CSIRT-LEXFO is committed to deliver a high-quality service to its constituency.
- CSIRT-LEXFO will ensure to respond to security incidents as efficiently as possible.
- CSIRT-LEXFO will ease the exchange of good practices between constituents and with peers, on a need-to-know basis.

3.2 Constituency

As a commercial CSIRT, the CSIRT-LEXFO provides services to its customers which are located in France and other countries. CSIRT-LEXFO customers are found among:

- Private sector organizations
- Public sectors organizations
- Commercial organizations
- CSIRT-LEXFO constituency also includes all the elements of LEXFO's Information System: its users, its systems, its applications, and its networks.

More information can be found on the LEXFO's website: https://lexfo.fr/.

3.3 Affiliation

CSIRT-LEXFO is part of LEXFO (https://lexfo.fr/). CSIRT-LEXFO maintains contact with various national and international CSIRT and CERT teams (mainly in France), on an as-needed basis.

3.4 Authority

For internal matters, CSIRT-LEXFO operates under the authority of the CEO of LEXFO.

For external incidents, CSIRT-LEXFO coordinates security incidents on behalf of its constituency, and only at its constituents' request. Consequently, CSIRT-LEXFO operates under the auspices of, and with authority delegated by its constituents.

CSIRT-LEXFO primarily acts as an advisor regarding local security teams and is expected to make operational recommendations. Therefore, CSIRT-LEXFO may not have any specific authority to require specific actions. The implementation of such recommendations is not a responsibility of CSIRT-LEXFO, but solely of those to whom the recommendations were made.

Generally, CSIRT-LEXFO expects to work co-operatively with its constituents' system administrators and users.

4 Policies

4.1 Types of Incidents and Level of Support

CSIRT-LEXFO addresses all types of computer security incidents (cyber-attacks) which occur, or threaten to occur, in its constituency (see section 3.2).

The level of support given by LEXFO will vary depending on the type and severity of the incident or issue, the type of constituent, the importance of the impact on critical or essential infrastructure or services, and the CSIRT-LEXFO resources at the time. Depending on the security incident's type, CSIRT-LEXFO will gradually roll out its services which include incident response and digital forensics. In all cases, some response will be made within two working days.

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

All incidents are considered normal priority unless they are labelled EMERGENCY. CSIRT-LEXFO itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to CSIRT-LEXFO as EMERGENCY, but it is up to CSIRT-LEXFO to decide whether to uphold that status.

CSIRT-LEXFO is committed to keep its constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited. This communication will be in the form of: email alerts, or phone calls under certain circumstances.

Note that no direct support will be given to end users. They are expected to contact their Security Operation Center (SOC) for assistance. The CSIRT-LEXFO will support the latter people.

4.2 Co-operation, Interaction and Disclosure of Information

CSIRT-LEXFO considers the paramount importance of operational coordination and information sharing between CERTs, CSIRTs, SOCs and similar bodies, and with other organizations, which may aid to deliver its services, or which provide benefits to CSIRT-LEXFO's constituency.

Consequently, CSIRT-LEXFO exchanges all necessary information with affected parties, as well as with other CSIRTs, on a need-to-know basis. However, neither personal nor overhead data are exchanged unless explicitly authorized. Moreover, CSIRT-LEXFO will protect the privacy of its customers/constituents, and therefore (under normal circumstances) pass on information in an anonymized way only (unless other contractual agreements apply).

All incoming information is handled confidentially by CSIRT-LEXFO, regardless of its priority.

All sensible data (such as personal data, system configurations, known vulnerabilities with their locations) are stored in a secure environment, and are encrypted if they must be transmitted over unsecured environment as stated below.

CSIRT-LEXFO operates within the current French legal framework.

4.3 Communication and Authentication

The preferred method of communication is email. For the exchange of sensitive information and authenticated communication CSIRT-LEXFO uses several encryption solutions. By default, all sensitive communication to CSIRT-LEXFO should be encrypted with our public PGP key detailed in section 2.8.

CSIRT-LEXFO protects sensitive information in accordance with relevant regulations and policies within France and the EU.

CSIRT-LEXFO respects the sensitivity markings allocated by originators of information communicated to CSIRT-LEXFO ("originator control").

CSIRT-LEXFO supports the Traffic Light Protocol (TLP). Information that comes in with the tags TLP:WHITE, TLP:GREEN, TLP:AMBER or TLP:RED will be handled appropriately.

Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context. In particular, in CSIRT-LEXFO's context of operations, the following communication security levels may be encountered:

- → Telephones will be considered sufficiently secure to be used (even unencrypted), in view of the types of information that CSIRT-LEXFO deals with.
- → Unencrypted email 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 email, encryption (preferably PGP) will be used (see section 2.8). Network file transfers will be like email for these purposes: sensitive data should be encrypted for transmission.

5 Services

5.1 Announcements

CSIRT-LEXFO may provide information on the threat landscape, published vulnerabilities, new attack tools or artifacts and security measures needed to protect its constituency's Information System.

5.2 Alerts and Warnings

CSIRT-LEXFO disseminates information on cyberattacks, disruptions, security vulnerabilities, intrusion alerts, malware, and provides recommendations to tackle the issue within its constituency.

Alerts and warnings may be passed on to other CERTs, CSIRTs, SOCs and similar bodies if deemed necessary or useful to them on a need-to-know basis.

CSIRT-LEXFO is not responsible for the implementation of its recommendations. Incident resolution is usually left to the responsible administrators within the constituency. However, CSIRT-LEXFO will offer support and advice on request.

5.3 Pre-emptive Security Controls

CSIRT-LEXFO performs pre-emptive security controls to detect potential breaches or vulnerabilities and misconfigurations that may be leveraged in cyberattacks. The security controls also check the compliance level of various systems and applications with the security policies.

5.4 Digital Forensics and Incident Response (Triage, Coordination and Resolution)

CSIRT-LEXFO performs incident response for its constituency (as defined in 3.2).

CSIRT-LEXFO handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency. However, CSIRT-LEXFO will offer support and advice on request.

CSIRT-LEXFO will assist IT Security team in handling the technical and organizational aspects of incidents. It will provide assistance or advice with respect to the following aspects of incident management:

- Incident Triage:
  - by investigating whether indeed an incident occurred
  - by determining the extent of the incident
- Incident Coordination:
  - by determining the initial cause of the incident (vulnerability exploited)
  - by performing Digital Forensics whenever necessary (including hard drive and memory forensics)
  - by facilitating contact with Security Contacts and/or appropriate law enforcement officials, if necessary, by making reports to other CSIRTs (if applicable)
- Incident Resolution:
  - by fixing the vulnerability
  - by securing the system from the effects of the incident
  - by evaluating whether certain actions are likely to reap results in proportion to their cost and risk
  - by collecting evidence where criminal prosecution, or disciplinary action, is contemplated
  - by collecting statistics concerning incidents which occur within or involve its constituency

CSIRT-LEXFO's incident response service tries to cover at best all the '6 steps': preparation, identification, containment, eradication, recovery, and lessons to be learned.

Please remember that the amount of assistance available from CSIRT-LEXFO will vary according to the parameters described in section 4.1.

5.5 Proactive activities

CSIRT-LEXFO internally develops security tools for its own use, to improve its services and support its activities as needed.

Even though these security tools are used to provide benefits to CSIRT-LEXFO's constituency, they are not to be shared/used neither by members of its constituency or by members of the larger CERT, CSIRT and SOC communities.

6 Incident Reporting Forms

Information system security incidents can be reported using the reporting form on the LEXFO website:

https://lexfo.fr/contact-csirt/

Access to the reporting form does not require prior authentication. Reporting can also be sent by mail with at least the following information:

- Contact details and organizational information (contact name, organization name and address)
- Email address, telephone number
- IP address(es), FQDN(s), and any other relevant technical element with associated observation
- If any, scanning results or extract from the log showing the problem
- In case you wish to forward any emails, please include all email headers, body, and any attachments if possible and as permitted by the regulations, policies and legislation under which you operate

7 Disclaimers

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

End of the document