Deloitte.

# CSIRT-DELOITTE-FR RFC 2350

TLP: WHITE

## Preamble

Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP: WHITE information may be distributed without restriction, subject to copyright controls.

This document cancels and replaces all previous versions. Please ensure that you are using the latest version and securely destroy any copies of previous versions in your possession, whether in paper or electronic format.

# Contents

# 1. Document information

This document contains a description of CSIRT Deloitte France (CSIRT-DELOITTE-FR) as implemented by RFC 2350. It provides basic information about CSIRT-DELOITTE-FR, its channels of communication, its roles, responsibilities and the services offered.

## 1.1 Date of last update

Version 1, created on 2020-03-23.

## 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 1.3.

Should you have any questions regarding updates, please contact the CSIRT-DELOITTE-FR email address.

## 1.3 Locations where this document may be found

The current and latest version of this document is available from CSIRT-DELOITTE-FR's website. Its URL is:

https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/solutions/computer-security-incident-response-team.html

Please make sure you are using the latest version.

## 1.4 Authenticating this Document

This document has been signed with the PGP key of CSIRT-DELOITTE-FR. The signature is available from CSIRT-DELOITTE-FR 's website. Its URL is:

https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/solutions/computer-security-incident-response-team.html

## 1.5 Document Identification

- Title: **CSIRT-DELOITTE-FR RFC 2350**
- Version: 1
- Document Date: 2020-03-23
- Expiration: This document is valid until superseded by a later version.

# 2. Contact Information

This section describes how to contact CSIRT Deloitte France.

## 2.1 Name of the Team

- Full Name: CSIRT-DELOITTE-FR
- Short Name: D.CSIRT

CSIRT-DELOITTE-France is Deloitte France's commercial CERT/CSIRT team (Computer Emergency Response Team / Computer Security Incident Response Team).

## 2.2 Address

CSIRT-DELOITTE
6 place de la Pyramide
92908 Paris-la-Défense Cedex
France

## 2.3 Time Zone

GMT+1 (with Daylight Saving Time or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October). Also known as CET/CEST.

## 2.4 Telephone Number

+33 1 40 88 28 29 (French Business hours).

## 2.5 Facsimile Number

None available.

## 2.6 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Deloitte France, please contact us at: **csirt@deloitte.fr**.

## 2.7 Public Keys and Encryption Information

PGP/GnuPG is supported to secure communication.

Consequently, the CSIRT-DELOITTE-FR has a PGP key:

- KeyID: 0xAEF73AF9
- Fingerprint: F54E 580D BB5D 6C29 41D0 5329 615F 5AA8 AEF7 3AF9

The key can be retrieved from one of the usual public key servers such as http://pgp.mit.edu/.

The key shall be used whenever information must be sent to CSIRT-DELOITTE-FR in a secure manner.

- Please use this key when you want/need to encrypt messages that you send to CSIRT-DELOITTE-FR.
- When due, CSIRT-DELOITTE-FR will sign messages.
- When due, sign your messages using your own key please. It helps when that key is verifiable (for instance, using the public key servers).

## 2.8 Team Members

CSIRT-DELOITTE-FR ’s acting team leader is Mathieu Hartheiser.

The team consists of IT security analysts.

## 2.9 Other Information

General information about CSIRT-DELOITTE-FR can be found at the following URL:

https://www2.deloitte.com/fr/fr/pages/risque-compliance-et-controle-interne/solutions/computer-security-incident-response-team.html

## 2.10 Points of Customer Contact

The preferred method to contact CSIRT Deloitte France is to send an email to the following address: csirt@deloitte.fr.

If necessary, urgent cases can be reported by phone (+33 1 40 88 28 29) during French business hours.

CSIRT-DELOITTE-FR ’s hours of operation are usually restricted to regular French business hours (Monday to Friday 09:00 to 18:00).

Out of office hours operations in case of emergency.

# 3. Charter

This section describes CSIRT-DELOITTE-FR's mandate.

## 3.1 Mission Statement

CSIRT-DELOITTE-FR is a private CSIRT team delivering security services, mainly in France.

Its purpose main purpose is to assist its customer community:

- First, in implementing proactive measures to reduce the risks of computer security incidents.
- And second, in responding to such incidents whenever they occur.

CSIRT-DELOITTE-FR's mission is to support its customer community to protect themselves against both intentional and opportunistic attacks that would hamper the integrity of their IT assets and harm their interests. The scope of CSIRT-DELOITTE-FR's activities cover prevention, detection, response and recovery. CSIRT-DELOITTE-FR oversees digital forensics and incident response (DFIR) activities.

CSIRT-DELOITTE-FR are driven by several key values:

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

## 3.2 Constituency

CSIRT-DELOITTE-FR's primary constituency is composed of all the elements of Deloitte Conseil Information System: its users, its systems, its applications and its networks.

However, notwithstanding the above, CSIRT-DELOITTE-FR's services are also delivered to a secondary constituency. As a commercial CSIRT, the CSIRT-DELOITTE-FR also provides services to its Customers Community, who subscribed a Service Level Agreement support contract.

Current customers which are in France and other countries are found among:

- Private sector organizations
- Public sector bodies
- Commercial bodies

## 3.3 Affiliation

CSIRT-DELOITTE-FR is affiliated to Deloitte Conseil in France. It maintains contacts with various national and international CSIRT and CERT teams according to its needs and the information exchange culture that it values.

## 3.4 Authority

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

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

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

# 4. Policies

This section describes CSIRT-DELOITTE-FR's policies.

## 4.1 Types of Incidents and Level of Support

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

The level of support given by CSIRT-DELOITTE-FR will vary depending on the type and severity of the incident or issue, its potential or assessed impact, the type of constituent, the size of the user community affected, and CSIRT-DELOITTE-FR's resources at the time. Depending on the security incident's type, CSIRT-DELOITTE-FR will gradually roll out its services which include incident response and digital forensics.

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

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

CSIRT-DELOITTE-FR 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-DELOITTE-FR's constituency.

Consequently, CSIRT-DELOITTE-FR 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-DELOITTE-FR 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-DELOITTE-FR, 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-DELOITTE-FR supports the Information Sharing Traffic Light Protocol version 1.1 (see https://www.trusted-introducer.org/ISTLPv11.pdf). Information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

CSIRT-DELOITTE-FR operates within the current French legal framework.

## 4.3 Communication and Authentication

CSIRT-DELOITTE-FR protects sensitive information in accordance with relevant French and European regulations and policies within France and the EU. CSIRT-DELOITTE-FR respects the sensitivity markings allocated by originators of information communicated to CSIRT-DELOITTE-FR ("originator control").

CSIRT-DELOITTE-FR also recognizes and supports the FIRST TLP (Traffic Light Protocol) version 1.1.

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 CSIRT-DELOITTE-FR'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-DELOITTE-FR deals with.
- Unencrypted email will not be considered particularly secure but will be enough 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 2.8). Network file transfers will be similar to email for these purposes: sensitive data should be encrypted for transmission

# 5. Services

This section describes CSIRT-DELOITTE-FR's services.

## 5.1 Announcements

CSIRT-DELOITTE-FR may provide information on the threat landscape, published vulnerabilities, new attack tools or artefacts and security measures.

## 5.2 Alerts and Warnings

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

## 5.3 Pre-emptive Security Controls

CSIRT-DELOITTE-FR 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.

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

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

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

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

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

Incident Triage:

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

Incident Coordination:

- Determining the initial cause of the incident (vulnerability exploited)
- Performing acquisition and Digital Forensics whenever necessary (including hard drive and memory forensics)
- Facilitating contact with Security Contacts and/or appropriate law enforcement officials, if necessary
- Making reports to other CSIRTs, CERTs, SOC (if applicable)

Incident Resolution:

- Providing guidance and support to fix the vulnerability
- Providing support in 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
- Collecting evidence where criminal prosecution, or disciplinary action, is contemplated

## 5.5 Development of Security Tools

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

## 5.6 Digital Forensics and Incident Response

CSIRT-DELOITTE-FR performs incident response for its constituency. The incident response service as developed by CSIRT-DELOITTE-FR covers the following steps:

1. Alert & scope;
2. Triage;
3. Collect & Preserve;
4. Contain;
5. Eradicate & Mitigate;
6. Recover
7. Report;
8. Closure.

CSIRT-DELOITTE-FR also performs digital forensics whenever necessary including hard drive and memory forensics.

# 6. Incident Reporting Forms

No local form has been developed to report incidents to CSIRT-DELOITTE-FR.

In case of emergency or crisis, please provide CSIRT-DELOITTE-FR at least the following information:

- Contact details and organizational name, including address and telephone number.
- Date and time when the incident started.
- Date and time when the incident was detected.
- Incident description.
- Affected assets, impact.
- Actions taken so far.
- Expectations or priorities.

# 7. Disclaimers

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

Deloitte.