Réf : NP-SIT-DSIT-DESPA-E2S-17-00307		
Indice : 2 **-**	**COrS'R (CSIRT RTE) - RFC2350**	Date d'approbation : 01/08/2018
Prescriptif : -		Date de fin de validité :
Date d'applicabilité : 01/08/2018		Pages : 5
Destinataire(s) : Copie(s) :		Rédacteur(s) : Gwenael Heim Vérificateur(s) : Florent CARLI Approbateur(s) : Xavier CARTON Accessibilité : Libre

1. Document Information

This document contains a description of the Computer Security Incident Response Team (CSIRT) of the company RTE (Réseau de Transport de l'Electricité). This group is commonly named « COrS'R », as « Centre Opérationnel de Sécurité RTE ».
It provides basic information about the COrSR team, its channel of communication and its missions.
This document complies with RFC 2350.

1.1 Date of Last Update

This is version 2, published the 01/08/2018.

1.2 Distribution List for Notifications

There is no distribution list for notification.

1.3 Locations where this Document May Be Found

The current version of the document can always be found on the following link :
⇨ http://csirt.rte-france.com/RFC2350_COrSR.pdf

Some information may be found on public websites like https://www.trusted-introducer.org/directory/teams/corsr.html

2. Contact Information

2.1 Name of the Team

Full name: Centre Operationnel de Securite RTE
Short name: COrS'R (or COrSR)
Alternative name: CSIRT RTE

2.2 Address

RTE / DSIT / DESPA / COrS'R
41 rue Berthelot
92400 Courbevoie
France

2.3 Time Zone

Time zone: CET / CEST (UTC+1 or UTC+2)

2.4 Telephone Number

Main number: +33 178 55 50 25.

Use of the phone for reporting incidents must be used only in emergency cases.
Only French and English are supported.

2.5 Facsimile Number

Not applicable

2.6 Other Telecommunication

Not applicable

2.7 Electronic Mail Address

Mail: csirt-info@rte-france.com
This is the preferred channel of all types of communication with the CSIRT team.

2.8 Public Keys and Encryption Information

PGP can be used for operational exchanges between the COrS'R and its Partners

```
pub   rsa4096 2018-08-01 [C]
      FBDD12E77C6C3BB59A3968848190CC2E212FC72E
uid          [  ultime ] COrS'R (RTE CSIRT) <csirt-info@rte-france.com>
```

Please sign messages using a key that is verifiable using the public keyservers.

2.9 Team Members

The COrS'R team leader is Florent CARLI.
No other public information is provided about team members.

2.10 Other Information

Not applicable

2.11 Points of Customer Contact

The preferred point of contact is by mail: csirt-info@rte-france.com
Only in case of emergency, you may want to contact us by phone: +33 178 55 50 25

RTE CSIRT's hours of operation are restricted to regular business hours: 8h00 to 18h00 in local time zone from Monday to Friday, excluding bank holiday.

3. Charter

3.1 Mission Statement

The COrS'R's mission is to support RTE to protect itself against intentional and malicious attacks that would impact its business interests.

The scope is protection, prevention, detection, response and recovery.

Since RTE's business is extremely sensible and according to internal policy, the COrS'R will:

- Operate with highest standards,
- Value all types of notifications about security issues,
- Respond effectively in case of incidents and emergencies,
- Maintain a high level of service and skills.

3.2 Constituency

The COrS'R can be involved in all type of security events concerning RTE and its subsidiairies. Its perimeter is both corporate and industrial IT systems.

It concerns, but is not limited to:

- ⇨ *.rte-france.com
- ⇨ 185.30.132.0/22
- ⇨ AS60174

The team protects our employees, customers and business partners too.

3.3 Sponsorship and/or Affiliation

The COrS'R is sponsored by others CSIRT.
It is member of the TF-CSIRT as a listed team.

- ⇨ https://www.trusted-introducer.org/directory/teams/corsr.html

3.4 Authority

The CSIRT is a global team of Investigators, Engineers and Analysts that serve the IT, business and engineering organizations within RTE, under the responsibility of the Chief Information Security Officier (CISO) and the company senior management team.

4. Policies

4.1 Types of Incidents and Level Support

The COrS'R will address all types of cybersecurity incidents that occur or threat to occur.

4.2 Co-operation, Interaction and Disclosure of Information

All incoming information will be handled confidentially by the team.
For sensitive data, like vulnerabilities, login / password, architecture information, please use encryption.
The Information Sharing Traffic Light Protocol (ISTLP) is supported. The information will be handled appropriately to the tags.

4.3 Communication and Authentification

Usage of PGP is recommended.

5. Services

5.1 Incident Response

COrS'R will assist system administrators in handling the technical and organizational aspects of incidents:

- Incident triage (priority, severity, impact,…)
- Incident coordination (determining exploitable/exploited vulnerabilities, facilitating contact with third parties, reports, communication, securing the system, collect evidence, …)

In addition, the COrS'R will have its own follow-up of the incident, as part of the information security incident management process.

5.2 Proactive activities

The COrS'R coordinates and maintains the following services:

- List of security contacts in the company,
- Security solutions vendors contacts,
- Security Information Event Management,
- Training center (communication, security awareness, …),
- Auditing services.

6. Incident Reporting Forms

There is no specific forms available. To be treated appropriately, the issue should be described with as many information as possible:

- Type of issue,
- Description,
- Date and time of detection,
- Proof : printscreen, logs, code …
- Contact and identification of the sender.

7. Disclaimers

Not applicable