Code SI-nerGIE :		**Operations** **Security**	
Révision :	PAGE 1/7		
Autre référence :			
Classification PIGA : **DIFFUSION PUBLIQUE**			

RFC 2350
CERT FRAMATOME

Date d'application: **01/01/2027**		
Nom	Dpt.	Visa
Issuer : **Eric BUCHET**	SI-nerGIE	
For Vérification : **Florian KALADZE**	SI-nerGIE	☐ Validé en comité de pilotage en date du JJ/MM/AAAA
ISSM Approbation :	SI-nerGIE	
For Issuance : **Julien DREANO**	SI-nerGIE	
	SI-nerGIE	

Révision No.	Révision Date d'application	Change N°.	Périmètre de la révision	Raisons du changement
1	10/11/2026	0	Process création	

Référence documentaire

TABLE DES MATIERES

1 DOCUMENT INFORMATION 4
1.1 Date of Last update 4
1.2 Distribution list for notifications 4
1.3 Distribution list for notifications 4
1.4 Location where this Document May be Found. 4
1.5 Authenticating this Document 4
1.6 Document identification 4
2 INFORMATIONS SUR LE CERT FRAMATOME 4
2.1 Name of the team 4
2.2 Address 4
2.3 Time zone 5
2.4 Phone Number 5
2.5 Facsimile Number 5
2.6 Other Telecommunication 5
2.7 Email address 5
2.8 Team Member 5
3 CHARTER 5
3.1 Mission Statement 5
3.2 Constituency 5
3.3 Support / relations 6
3.4 Autority 6
4 POLICIES 6
4.1 Types of incidents and level of support 6
4.2 Cooperation, interaction and disclosure of information 6
4.3 Communication and authentication 6
5 SERVICES 7
5.1 Reactive activities 7
5 7
5.2 Triage 7
5.3 Coordination 7
5.4 Resolution 7
5.5 Proactive activities 7

6 INCIDENT REPORTING FORMS 7
7 DISCLAIMER 7

1 DOCUMENT INFORMATION

This document contains a description of the incident response cell named Csirt Framatome as recommended by RFC 2350. It provides essential information about the unit, its responsibilities and the services provided.

1.1 Date of Last update

This is the initial version 1.0 published on November 10th, 2026.

1.2 Distribution list for notifications

Notification of document changes is not distributed by a Mailing List or any other mechanisms.

1.3 Distribution list for notifications

There is no distribution list for notifications.

1.4 Location where this Document May be Found.

The current and latest version of this document are available on the following web sites:
https://www.framatome.com/fr/csirt

1.5 Authenticating this Document

The PGP public key, ID and fingerprint are available on the Framatome web site at
https://www.framatome.com/fr/csirt

1.6 Document identification

Title:	Csirt-FRAM-RFC2350_EN
Version:	V1.0
Document date:	25/09/2026
Expiration:	This document will be valid until it is replaced by a later version.

2 INFORMATIONS SUR LE CSIRT FRAMATOME

2.1 Name of the team

Csirt Framatome

2.2 Address

CSIRT Framatome

1 place Coupole Jean Millier
92400 Courbevoie
Cedex

2.3 Time zone

CET/CEST (UTC +1/UTC +2) Central European Time / Central European Summer Time

2.4 Phone Number

Main number (duty office): +33 1 82 80 01 01

2.5 Facsimile Number

None

2.6 Other Telecommunication

None

2.7 Email address

If you need to notify us of a security incident or malicious cyber activity, please contact us at csirt@framatome.com

Public key and encryption information

User ID :	csirt@framatome.com
Fingerprint :	53B2 9FB8 E203 364A 0889 FD99 AA98 5C14 AE3E E164
Key ID :	AA985C14AE3EE164

2.8 Team Member

The list of team members is not published. It is composed of experts in security information systems: vulnerability analysis, forensics, reverse engineering. The identity of a Csirt Framatome member can be disclosed on a case-by-case basis according to the need-to-know principle

3 CHARTER

3.1 Mission Statement

The Csirt Framatome team contributes to the defensive cyber warfare by providing security services, such as:

Implementation of proactive measures

Crisis management

Security incident response

3.2 Constituency

The skills of the Csirt Framatome are carried out on the elements of the FRAMATOME information system: its users, its systems, its applications and its networks.

3.3 Support / relations

Csirt Framatome exchanges and collaborates with various CERTs and institutions.

3.4 Autority

The Csirt team is responsible for anticipating, detecting, responding to, and coordinating remediation across the enterprise for all perimeters.

4 POLICIES

4.1 Types of incidents and level of support

The Csirt Framatome is the central point of contact for Framatome's security incidents

The services offered by Csirt Framatome are:

- Presence 24/7 (on call)
- Security information and alerts
- Incident response support
- Monitoring and newsletters
- Security Consulting

4.2 Cooperation, interaction and disclosure of information

Csirt Framatome may be required to communicate with the ANSSI or various certs.

4.3 Communication and authentication

The preferred means of communication is e-mail, using the PGP protocol.

5 SERVICES

5.1 Reactive activities

The incident response service is available 24/7. Non-working hours and days are provided by an on-call team.

5.2 Triage

The actions carried out are as follows:

- Analyze and qualify security incidents
- Escalate with CISOs in the event of a major security incident
- To exchange with the ANSSI, and the various CERTs in the event of an incident that may impact other sectors.

5.3 Coordination

Csirt Framatome may be required to coordinate and support the structure(s) concerned in the handling of security incidents.

5.4 Resolution

Csirt Framatome monitors incident resolution processes, analyzes artifacts and proposes action plans on a case-by-case basis.

5.5 Proactive activities

The team offers the following services:

- Proactive threat hunting
- Threat Intelligence
- Vulnerability management and scanning
- Security audits

6 INCIDENT REPORTING FORMS

All security incidents are tracked via a ticketing tool dedicated to the cyber community. All the mandatory information entered allows traceability as well as the possibility of building a timeline.

7 DISCLAIMER

Although every care has been taken in the preparation of the security bulletins, Csirt Framatome cannot be held responsible for errors or omissions, or damage that may result from the use of the information provided in the context of supporting the handling of an incident.