Saint-Gobain CSIRT
RFC 2350

1. About this document

This document contains a description of Saint-Gobain CSIRT according to RFC 2350 and provides essential information about Saint-Gobain CSIRT, its role, responsibilities and means of communication.

The version of this document is 1.0, published on January 28, 2022.

2. Contact Information

This section describes the means of communication of Saint-Gobain CSIRT.

2.1. Name of the team

The registered name is **Saint-Gobain CSIRT.**

2.2. Address

Saint-Gobain DSI Groupe – Saint-Gobain CSIRT
Tour Saint-Gobain
12 place de l'Iris,
92400 Courbevoie
France

2.3. Creation date

Saint-Gobain CSIRT was created on June 2018.

2.4. Time zone

CET/CEST: Europe/Paris

2.5. Electronic email address

Saint-Gobain CSIRT email address is **csirt@saint-gobain.com**

2.6. Public keys and other encryption information

Saint-Gobain CSIRT has a PGP public key for encrypted communications including:

- **KeyID:** 0x5BD1A72D
- **Fingerprint:** CF90FD024BD73D15C2ACEFC56075C3725BD1A72D

Download the CSIRT key by clicking here.

2.7. Team members

The team is made up of Paris-based Service Line Managers, and a Mumbai-based operational team composed of cyber security analysts and expert security incident responders. No personal information relating to members of Saint-Gobain CSIRT is published in this document.

2.8. Operating hours

Saint-Gobain CSIRT operates on a 24/7 basis.

3. Charter

3.1. Mission statement

The activities of Saint-Gobain CSIRT are non-profit and are financed by Saint-Gobain DSI Groupe. The mandate for Saint-Gobain CSIRT is as follows:

- Identifying and anticipating cyber threats through a recurring monitoring activity on cyber threats and vulnerabilities for the entire Saint-Gobain Group and its subsidiaries;
- Protecting the Group from cyber threats through the use of several security tools and the delivery of several cybersecurity services;
- Detecting, responding and coordinating cyber security incidents that may affect Saint-Gobain assets.

3.2. Constituency

Saint-Gobain CSIRT coordinates and processes the response to incidents. It also provides cybersecurity services for the entire Saint-Gobain Group.

3.3. Sponsorship / Affiliation

Saint-Gobain CSIRT is a private CSIRT in the environment sector. It is operated, financed by and owned by Saint-Gobain DSI Groupe.

Saint-Gobain CSIRT is willing to share within the CSIRT/CERT networks and to join these communities.

3.4. Authority

Saint-Gobain CSIRT acts under the authority of Saint-Gobain DSI Groupe.

3.5. Responsibility

Saint-Gobain CSIRT is responsible for anticipating, protecting and responding to cybersecurity incidents throughout the Group.

4. Policies

4.1. Types of incidents and level of support

Saint-Gobain CSIRT coordinates, analyzes and handles cybersecurity incidents that could target Saint-Gobain Group, requiring its L1, L2 and L3 expertise. As such, it also participates to the management of cybersecurity vulnerabilities by informing people who need to know about vulnerabilities in products they manage and helping them to remediate them.

The level of support offered by Saint-Gobain CSIRT may vary according to the type of incident, its criticality, and the resources available to handle it.

4.2. Cooperation, interaction and disclosure of information

At a Group level, Saint-Gobain CSIRT cooperates with local Saint-Gobain security officers to manage incidents, vulnerabilities and recoveries. Processes are formalized to set the scope and interactions of each stakeholder.

At a Groupwide level, Saint-Gobain CSIRT is willing to exchange all necessary information with other CERT/CSIRTs who may be concerned on a need-to-know basis.

No incident or vulnerability will be disclosed publicly without the agreement of all the concerned parties. Legal requests will be evaluated by our Legal Department and an appropriate response will be given if the request is acceptable, within the limits of the court order, the related investigation and the information requested.

4.3. Communication

Saint-Gobain CSIRT strongly encourages the use of a PGP key for email encryption. All emails containing confidential information must be encrypted using a PGP key.

Saint-Gobain CSIRT respects the Information Sharing Traffic Light Protocol (TLP) that comes with the tags WHITE, GREEN, AMBER or RED.

An unencrypted email can be used for non-sensitive information sharing.

5. Services

5.1. Incident response

Saint-Gobain CSIRT is in charge of detecting and responding to any cybersecurity event impacting Saint-Gobain, so as to contain their impact.

To this aim, it provides different incident response services:

- Monitoring, detecting and reporting standard IT cybersecurity events on 24/7;
- Monitoring, detecting and reporting industrial-related cybersecurity events on 12/5;
- Analyzing suspicious emails reported by end users to assess whether they are safe.

5.2. Proactive activities

Saint-Gobain CSIRT is also in charge of providing the appropriate safeguards to protect and contain the impact of any potential cybersecurity event for Saint-Gobain.

To this aim, it provides different proactive services:

- Protecting workstations and servers against local attacks;
- Protecting public web applications against vulnerabilities;
- Providing a strong authentication for end users;
- Protecting endpoints with encryption;
- Protecting end users through internally signed digital certificates;
- Preventing attacks by detecting known vulnerabilities and informing system owners for remediation.

5.3. Identification of cyber threats

Saint-Gobain CSIRT is in charge of identifying cyber threats occurring in the world in order to anticipate them before they have any impact for Saint-Gobain.

To this aim, it provides different identification services:

- Monitoring cyber threats, data leaks threats and brand abuse taking into consideration Saint-Gobain context;
- Monitoring, assessing and informing on vulnerabilities in software used within the Group;
- Analyzing suspicious files in a secure sandbox environment;
- Internal communication on cyber threats.

6. Incident Reporting

To report an incident, please report the incident by encrypted email to the address in section 2.6.
Incident reports should contain the following information:

- Date and time of the incident (including time zone);
- Description of the incident;

- Source/Destination IPs, ports and protocols or products concerned;
- Any other relevant information

7. Disclaimers

Although the information provided in this document has been verified, Saint-Gobain CSIRT declines all responsibility in the event of any error or omission or for any prejudice resulting from information contained in this document. If you notice any error in this document, please notify us by e-mail. We will try to rectify the information as soon as possible.