1 Document Information

1.1. Version

This is version 1.1 of 24th January, 2017.

1.2. Distribution List

Notification of updates are submitted to the mailing list: soc@gse.it, cert@cert-pa.it, cert@garr.it.

1.3. Location where this document may be found

A copy of this document could be requested sending an email to soc@gse.it

2 CONTACT INFORMATION

2.1 Name of the team

Full name: Security Operation Center Gestore Servizi Energetici
Short name: SOC-GSE

2.2 Address

Postal Address
SOC GSE at Gestore Servizi Energetici
Gestore Servizi Energetici
Viale Maresciallo Pilsudsky, 92
00197 - Rome
Italy

2.3 Time zone

Central Europe (GMT+0100 e GMT+0200 from the last Sunday of March to the last Sunday of October).

2.4 Telephone number

+39 06 80112450

2.5 Facsimile number

Fax number is provided for a restricted group of contacts.

2.6 Electronic mail address

SOC-GSE can be reached via soc@gse.it
All messages sent to this email address are received by all SOC-GSE members.

2.7 Other telecommunications

None.

2.8 Public Keys and encryption information

PGP/GnuPG is supported for secure communication. All members of SOC-GSE have personal PGP key that use for exchange of information classified as "Restricted" or "Secret", according to the SOC-GSE Policy on Information Classification.
SOC-GSE public PGP key for soc@gse.it is available on the public key servers.
Fingerprint is 0353 3308 2AA5 C2BE 0C2A 3394 1CE5 7487 B37D 0AC9

2.9 Team members

The list of team members is published on SOC-GSE web page in the GSE intranet portal.

2.10 Other information

None

2.11 Other information

The preferred mode for contacting SOC-GSE is via email: soc@gse.it. The mailbox is monitored during regular office hours: Monday to Friday. 09:00-18:0, except during public holiday in Italy.

If it is necessary not contact SOC-GSE via email for security reason, contact may be made by telephone during regular office hours.

Please use PGP/GPG if you would be send sensitive information.

3 CHARTER

3.1 Mission statement

SOC-GSE mission is to suggest and implement security tactical and technical countermeasures, in order to prevent and protect any violation attempt having an impact for GSE business.
SOC-GSE main targets are:

- Security Incident Response coordination.
- To provide information on potential threat impacting the information asset of GSE.
- To increase the awareness and security culture for GSE.

3.2 Constituency

SOC-GSE constituency refers to users, systems and applications and any other relevant resources of GSE. This initial constituency is planned to grow, in order to include all of the other entities belonging to the GSE Group.

3.3 Sponsorship/affiliation

SOC-GSE is managed by Security Information Unit within Gestore Servizi Energetici, under control of Information Systems Department.

3.4 Authority

SOC-GSE operates under the auspices of Gestore Servizi Energetici management.
GSE has adopted a shared model for SOC-GSE:

4 POLICIES

4.1 Types of Incidents and Level of Support

SOC-GSE is authorized to address all types of information security incidents that occur within its constituency.
SOC-GSE is also committed to keeping its constituency informed of potential vulnerabilities, possibly before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

SOC-GSE receives incident reports related to events or threats impacting GSE, evaluating classification and severity, then notify it to the appropriate management level. It also coordinates the activities needed to put in place appropriate incident resolutions (countermeasures).

SOC-GSE takes into account with regards to the handling and disclosure of information applicable laws of Italy, in order to not cause any injury. In

particular, the Legislative Decree 30 June 2003 n.196 "Code for the Protection of Personal Data" introduces a legal classification of information to be protected.

The protection of information regards their treatment, or rather any operation, carried out with or without the aid of electronic or automated means, such as collection, recording, organization, storage, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, dissemination, erasure and destruction of data.

4.3 Communication and Authentication

Unencrypted emails are considered sufficient for transmission of low-sensitivity data. In order to exchange high-sensitivity information, an encrypted email with PGP/GPG keys is mandatory required.

SOC-GSE CERT recognize and support the ISTLP (Information Sharing Traffic Light Protocol), following best practice in NISCC (UK).

The Traffic Light Protocol (LTP) is used to exchange confidential information and ensures controlled disclosure. This method is based on the use of four colors (Red, Amber, Green and White) to classify information according to how sensitive it is and address the recipient on how to process it.

- Red Information can only be used by recipient in the information exchange.
- Amber information can be shared by the parts participating in the information exchange with others within their organization, but only on a "need-to-know" reason.
- Green information can be shared by the parts participating in the information exchange with any others organization, but not using publicly accessible channels.
- White information can be shared freely in compliance with standard copyright rules.

5 SERVICES

SOC-GSE provides security services for GSE only.

5.1 Incident Response

SOC-GSE is responsible to implements the whole GSE security incident response process. It asses incoming reports about incident and follow up on these with a suggestion of a recovery solution to internal IT Department.

5.1.1 Incident Triage

SOC-GSE handles triage classifying reported incident or event observed by SIEM or reported by other unit/department. The events are analyzed verifying the reliability of the source and finding any other available information. Then they are categorized according to three factor: class of the event, event priority and asset value (critical issue).

5.1.2 Incident Coordination

SOC-GSE offer an Incident Coordination service on its constituency acting as described following:

1) Identifying GSE Unit or Team involved;

2) Establishing contacts with all the stakeholders in order to analyze the incident and identify actions to be undertaken;
3) Facilitating contacts with other GSE Unit or Team that can provide support in solving the incident;
4) Promptly informing GSE Management at the level corresponding to incident severity;
5) Writing reports and sending them to other CERTs or interested organizations.

5.1.3 Incident Resolution

SOC-GSE defines containment strategies and suggests and coordinates actions to contrast/recovery incident to ensure a return to normal operations (before the security incident) as quickly as possible. Such actions may include, for example, the reconnection of disconnected networks, the commissioning of services, systems or blocked applications, the restoring of corrupted or lost data backup. The return to normal operations is properly checked by specific tests on systems, applications and data. In case of failure new strategies are identified by SOC-GSE in according with GSE Management.

5.2 Proactive Activities

SOC-GSE provides the following proactive activities to its constituency:
- dissemination of useful information for the growth of cyber security;
- security bulletin (advisory);
- advanced training in the field of cyber security, awareness campaigns for users in order to enhance their knowledge of information security issues;
- information sharing.

6 Incident Reporting forms

SOC-GSE provides bulletins and advisories that could be matter of constituency interest.

All constituency members could send incident report or security threat via email, encrypted eventually to SOC-GSE email address.
In this case, it is necessary to provide as much more information as possible, such as:
- Date/time of event;
- Class or type of event
- Involved system (even potentially involved)
- Other.

Do not send malicious code or other attachments via email without having previously agreed the mode of transmission with a SOC-GSE team members.
Specify the level of confidentiality of information (public domain or not). In case of absence of this information SOC-GSE will assume that the information itself is in the public domain.

7 Disclaimers

SOC-GSE assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.