

Opt



RFC2350

Contents

1	Document Information	1
1.1	Date of Last Update	1
1.2	Distribution List for Notifications	1
1.3	Locations where this Document May Be Found	1
2	Contact information	1
2.1	Name of the team	1
2.2	Address	1
2.3	Time zone	1
2.4	Telephone number	1
2.5	Facsimile Number	1
2.6	Other Telecommunications	2
2.7	Electronic Mail Address	2
2.8	Public Keys and Other Encryption Information	2
2.9	Team Members	3
2.10	Other Information	3
2.11	Points of Customer Contact	3
3	Charter	3
3.1	Mission Statement	3
3.2	Constituency	3
3.3	Sponsorship and/or Affiliation	4
3.4	Authority	4
4	Policies	4
4.1	Types of Incidents and Level of Support	4
4.2	Co-operation, Interaction and Disclosure of Information	5
4.3	Communication and Authentication	5
5	Services	5
5.1	Reactive services	5
5.1.1	Event Security Management	5
5.1.2	Incident Management	6
5.2	Proactive Services	6
5.2.1	Proactive threat detection	6
5.2.2	Vulnerability analysis	6
6	Incident Reporting Forms	6
7	Disclaimers	7

Copyright 2023 © Grail Cyber Tech SL or its subsidiaris. All rights reserved. Any unauthorized copy or use of the marks is illegal and may lead to legal process. All rights, including but not limited to intellectual property rights , in the materials and information contained in this document are the exclusive property of Grail Cyber Tech SL. Any use of the materials and information contained herein, in any form or by any means, is permitted for internal or non-commercial use only. Any other use of the mentioned materials and information, in any form or by any means, without the explicit and written permission of Grail Cyber Tech SL, is strictly prohibited. Notwithstanding the above, modification of the materials and information, or deletion of author attribution, trademark, legend, or copyright, is strictly prohibited.

1 Document Information

1.1 Date of Last Update

This is version v1.0, published the 16th of May of 2023.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our constituency using established communication channels.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the Grail Cyber Tech's website; its URL is <https://grailcyber.tech/CSIRT/RFC2350.pdf>.

2 Contact information

2.1 Name of the team

Full name: Grail Cyber Tech - Computer Security Incident Response Team
Short name: GCT-CSIRT


2.2 Address


GCT-CSIRT, Grail Cyber Tech
Carrer de la Fontansa, 46
Sant Joan Despí, 08970
Barcelona, Spain (ES)

2.3 Time zone

Central European Time - CET (GMT+0100, and GMT+0200 from April to October)

2.4 Telephone number

 CSIRT emergency mobile number: +34 633 03 10 30

 CSIRT emergency telephone number: +34 934 97 31 57

2.5 Facsimile Number

Not Available

2.6 Other Telecommunications

Not Available

2.7 Electronic Mail Address

📧 General purpose enquiries: grail-csirt@grailcyber.tech

📧 Information exchange about incidents: incidents@grailcyber.tech

2.8 Public Keys and Other Encryption Information

The GCT-CSIRT **grail-csirt@grailcyber.tech** key has the KeyID 0x7F558533 and the following fingerprint: 7135 31E4 E900 221A 3C1F 7442 D33D 98C6 7F55 8533

The public key is as follows:

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mDMEYwMahYJKwYBBAHaRw8BAQdAkGtnaCHtW5korIrEMc6y7fiDHZYXXa8Z9Av1
Mm03kaGOKWdyYwlsLWNzaXJOIDxncmFpbC1jc2lydEBncmFpbGN5YmVyLnRlY2g+
iJkEEYKAEEWIQRxNTHk6QAiGjwfdELTPZjGf1WFMwUCYywMagIbAwUJA8PeNgUL
CQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRDTPZjGf1WFMxHOAP4lq/yeNOFm
FAV07V6GRY23kJ0hRyzGBMTJco5f64kf+gD/a3ZxG7gqAQNa/42nKrc+V8IeaZwA
kHWWfvcL3npOuA640ARjLaxqEgorBgEEAZdVAQUBAQdAZrOeShs05BYZb25BGJlc
1BPzt8gE/RP+sVDujsAdQXADAQgHiH4EGBYKACYWIQRxNTHk6QAiGjwfdELTPZjG
f1WFMwUCYywMagIbDAUJA8PeNgAKCRDTPZjGf1WFMzH3AP9z0kk6PD4wAM61wPdW
re07/bZyMYylsuRWFQWNUg/7kwD/S4i3Miul5+aLiPCfpSKR7uAAfhSG2HoTQ57G
DcgrsAY=
=8KgB
```

-----END PGP PUBLIC KEY BLOCK-----

The GCT-CSIRT **incidents@grailcyber.tech** key has the KeyID 0x3A132FE4 and the following fingerprint: 25FD E01D 29D0 4069 68A9 4BBB EBFE FE7B 3A13 2FE4

The public key is as follows:

-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mDMEZB3JUBYJKwYBBAHaRw8BAQdAwAzg1QzX4ud5+kJZ145ztvakQbK94YwzDwh8
+cMgw820JUluY21kZW50cyA8aw5jaWRlbnRzQGdyYwlsY3liZXIudGVjaD6ImQQT
FgoAQRyhBCX94B0p0EBpaK1Lu+v+/ns6Ey/kBQJkHclQAhsDBQkDw3HgBQsJCAcC
AiICBhUKCQgLAQWAgMBAh4HAheAAAoJE0v+/ns6Ey/kW88BAKUvGtfspyvJyb0J
uknER8Kj6QfbsjBKjwtkDhyb45xJAQD4S0wo5vaaJVcN83VNOgNERp1VggDUjvRz
C8z+GNluDrg4BGQdyVASCisGAQQB11UBBQEBOCwWvP6fjC35n1ACwTyBZH7gVcF
```

4qFfUjhZ7R+e/DvtEQMBCAeIfgQYFgoAJhYhBCX94B0p0EBpaK1Lu+v+/ns6Ey/k
BQJkHclQAhsMBQkDw3HgAAoJE0v+/ns6Ey/kJy8A/iq/PIkHWuLU/KiVyp21LLA4
RYt7oPJgEW4Sy2iqcxAP9PfMJGRbfEc0sZ5PRL2fA264jgWRHyuhw9t++C90qW
Ag==
=C2VN

-----END PGP PUBLIC KEY BLOCK-----

Please sign your messages using your own key which is verifiable using the public key servers.

2.9 Team Members

No information is publicly available about the GCT-CSIRT team members.

2.10 Other Information

Further information about Grail Cyber Tech can be found at: <https://grailcyber.tech>

GCT-CSIRT is a member of CSIRT.es; see <https://www.csirt.es/index.php/es/miembros/grail-csirt> for further details.

2.11 Points of Customer Contact

The preferred method for contacting GCT-CSIRT is via e-mail through grail-csirt@grailcyber.tech. All the e-mail sent to this address will be delivered to the on-duty staff. If urgent assistance is required, it is recommended to deliver the email to incidents@grailcyber.tech, including the keyword [URGENT] in the subject line.

If it is not possible or not advisable for security reasons to contact the GCT-CSIRT via e-mail, contact may be made by telephone during regular office hours.

The GCT-CSIRT hours of operation are generally restricted to regular business hours (08:00 - 18:00 local time, Monday through Friday).

3 Charter

3.1 Mission Statement

The main mission of GCT-CSIRT is to protect and secure the information assets and the technological infrastructures of our constituents by the prevention, detection, analysis and response to cybersecurity incidents. We are compromised to collaborate with our partners in order to share knowledge as well as to foster the security awareness culture between our employees and stakeholders.

3.2 Constituency

The constituency of **GCT-CSIRT** is:

- Ⓒ **Internal: GCT-CSIRT** focus its activity in protecting the information assets and the infrastructure of its own organization (Grail Cyber Tech).
- Ⓒ **External: GCT-CSIRT** acts as a provider of cybersecurity services to its own clients bag by offering these costumers a set of services previously defined by a mutual agreement.
- Ⓒ **Cybersecurity community: GCT-CSIRT** collaborates in the exchange of information flow with others CSIRTs, cybersecurity organizations, governmental agencies, investigation groups and any actor involved in the cybersecurity community.

3.3 Sponsorship and/or Affiliation

The GCT - CSIRT is part of Grail Cyber Tech.

3.4 Authority

GCT-CSIRT operates under the authority of the Chief Technology Officer (CTO) of Grail Cyber Tech. The CTO is ultimately responsible for the GCT-CSIRT information security policy and the company's response to security incidents.

The CTO delegates daily operational decision-making authority to the GCT-CSIRT Manager, who reports directly to the CTO. The GCT-CSIRT Manager is authorized to take any necessary actions to mitigate and respond to security incidents affecting the constituency of Grail Cyber Tech. These actions may include, but are not limited to, notifying affected clients, recommending appropriate mitigation measures, and coordinating incident response activities with the clients' internal/external IT or security teams.

GCT-CSIRT's team's role is to advise and assist its constituency in responding to security incidents, during which it has direct authority over the affected client's systems and networks.

When it comes to incidents involving multiple members of the constituency or affecting Grail Cyber Tech's own infrastructure, the GCT-CSIRT has the authority to coordinate the response across all affected parties. This includes sharing relevant information with other affected clients (subject to legal and contractual restrictions) and with relevant external entities, such as vendors, other CSIRTs, and law enforcement agencies.

Decisions made by the GCT-CSIRT Manager may be appealed to the CTO. The CTO's decisions may, in turn, be appealed to Grail Cyber Tech's executive leadership team.

4 Policies

4.1 Types of Incidents and Level of Support

All the incident reports received at the GCT-CSIRT are analyzed, classified and prioritized according to its internal incident classification policy, so an efficient and appropriate level of service is always granted.

The response type for each incident will depend on its risk level which can be critical, high, medium or low, and it can be categorized based on the taxonomy described in the internal incident handling procedure.

4.2 Co-operation, Interaction and Disclosure of Information

Information regarding an incident will always be classified as "Confidential" and therefore it cannot be communicated to a third party without a prior reclassification that grants a different level of confidentiality. Information classified as "not public" is protected by internal procedures that enforce mechanisms such as encryption.

GCT-CSIRT will only provide information to other parties with the sole purpose of facilitating the tasks of containment, eradication and recovery of incidents, under the general principle of providing the minimum information possible.

4.3 Communication and Authentication

See 2.8 above. Usage of PGP in all cases where sensitive information is involved is highly recommended.

5 Services

5.1 Reactive services



GCT-CSIRT will assist its constituency in handling the technical, organizational and legal aspects of computer security incidents and cyberthreats.

To make use of GCT-CSIRT's reactive services, please send an email as per section 2.11 above.

Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.

5.1.1 Event Security Management

This service involves the process of identifying, monitoring, and systematically addressing security events that occur within the computer networks of our constituents. It implies collecting and analyzing data from various sources to identify possible security incidents. Some of the areas covered by this service are:

-  Network and system security monitoring
-  Events and alerts analysis

5.1.2 Incident Management

This service pursues the identification, the containment, the eradication and the efficient resolution of cybersecurity incidents, while minimizing their impact and contributing to the improvement of the constituency, so those same cyberincidents do not happen ever again under the same terms. Some of the areas covered by this service are:

- 🔍 Incident reporting
- 🔍 Incident analysis and correlation
- 🔍 Evidence acquisition
- 🔍 Incident containment mitigation
- 🔍 Incident recovery
- 🔍 Incident remote response support and guidance
- 🔍 Incident response coordination with third parties
- 🔍 Forensic Analysis

5.2 Proactive Services

To make use of **GCT-CSIRT** proactive services, please send an email as per section 2.11 above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.

5.2.1 Proactive threat detection

Detection and identification of computer security incidents that have not generated any type of detection alert and have not been blocked by any of the existing security controls available in the constituency.

5.2.2 Vulnerability analysis

GCT-CSIRT evaluates the weak points of a system or a network, with the aim of identifying possible vulnerabilities. Once identified, solutions to remediate them are given, enhancing the existing security once these are applied.

6 Incident Reporting Forms

Not available. Preferably report using email or telephone:

- Incident Reporting Specific Mailbox: incidents@grailcyber.tech

- Telephone: +34 633 03 10 30

7 Disclaimers

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