RFC2350 IGNITIS CERT v1.0

TLP:WHITE

Document information

Project Title:	IGNITIS CERT
Report Title:	RFC2350 IGNITIS CERT
Version:	v1.0 of 2022-05-11
Prepared by:	Donatas Vitkus
Reviewed by:	Živilė Tveragaitė
Contact person:	Živilė Tveragaitė

1. Document Information

1.1. Date of Last Update
This is version 1.0 of 2022-05-11.

1.2. Distribution List for Notifications
This profile is kept up-to-date on the location specified in 1.3 .
E-mail notification of updates are sent to:
The Trusted Introducer for CERTs in Europe (see https://www.trusted-introducer.org/)

Any questions about updates please address to the soc@ignitis.lt e-mail address.

1.3. Locations where this Document May Be Found
The current version of this profile is always available on https://ignitisgrupe.lt/Ignitis-cert-rfc2350.pdf

2. Contact Information

2.1. Name of the Team
Full name: Ignitis group CERT
Short name: Ignitis CERT

2.2. Address
Postal Address:
Skaitmeninė sauga
UAB “Ignitis grupės paslaugų centras”
Laisvės pr. 10, LT-04215 Vilnius
Lithuania

2.3. Time Zone
GMT+2 (GMT+3 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Telephone Number
+370 5 2782444

2.5. Facsimile Number
N/A

2.6. Other Telecommunication
N/A

2.7. Electronic Mail Address'
soc@ignitis.lt
This address can be used to report all security incidents to which relate to the CERT-SE constituency.

2.8. Public Keys and Other Encryption Information
PGP/GnuPG is supported for secure communication.
The current IGNITIS CERT team key can be found on https://ignitisgrupe.lt/soc@ignitis.lt.asc.
Please use this key when you want/need to encrypt messages that you send to IGNITIS CERT.

2.9. Team Members
Information is not provided about the IGNITIS CERT team members on the website. Please use our email (in 2.7) when you contact us.

2.10. Other Information
Preferred method for contacting IGNITIS CERT is via email at soc@ignitis.lt.

3. Charter

3.1. Mission Statement
Mission of IGNITIS CERT is:
1. To provide cybersecurity incident management-related services to the IGNITIS CERT constituency.
2. To assist in identifying, analyzing and mitigation of the impact of security threats.
3. To ensure monitoring and exchange of information, collaboration with national and international incident response and cybersecurity teams and organizations.

3.2. Constituency
IGNITIS CERT's constituents are customers of UAB "Ignitis grupės paslaugų centras" receiving managed security services according to the contracts and agreements.

3.3. Sponsorship and/or Affiliation
All activities of IGNITIS CERT is funded by UAB "Ignitis grupės paslaugų centras".

3.4. Authority
IGNITIS CERT operates under supervision of Ignitis Group's Head of Digital Security.

4. Policies

4.1. Types of Incidents and Level of Support
IGNITIS CERT is responsible for the coordination of all types of digital security incidents as specified in the contracts with the customers. Level of support is specified in the contracts as well.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information is tagged as either a Confidential, Internal Use, For Intendend Recipient Only or Public.

Confidential information can be distributed internally on need-to-know basis according to the business needs and cannot be disclosed to third party persons who are not explicitly authorized to receive the information. Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label CONFIDENTIAL in the subject field of e-mail, and if possible using encryption as well.

IGNITIS CERT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

4.3. Communication and Authentication

see 2.8 above. Usage of PGP/GnuPG, or other pre-approved cryptographical means, in all cases where sensitive information is involved is highly recommended.

5. Services

5.1. Reactive, Proactive and Quality Management Services

1. Information Security Event Management service
2. Information Security Incident Management service
3. Vulnerability Management service

5.2. Incident reporting Forms

Available only for customer. For others preferably report in plain text using e-mail.

5.3. Disclaimers

The purpose of this document is to provide a generalized overview of IGNITIS CERT services. IGNITIS CERT services description provided in client contracts might differ from services description provided in this document. Client contracts always take precedence over this document.