RFC 2350 description for CYMED
(CYMED SECURITY TECHNOLOGIES S.R.L.)

1. Document Information

This document contains a description of CYMED in according to RFC 2350, providing basic information about CYMED team, its channels of communication, its roles and responsibilities.

1.1 Date of Last Update

This is version 1.0, published December 2020.

1.2 Distribution List for Notifications

For the moment there is no distribution list for notifications yet

1.3 Locations where this Document May Be Found The

Current version of this document can be found at: https://www.cymed.ro/wp-content/uploads/2021/01/RFC-2350-description-for-CYMED.pdf

1.4 Authenticating this Document

This document has been signed with CYMEDs PGP key. The signatures are also on our Web site, at https://www.cymed.ro/pgp/

2. Contact Information

2.1 Name of the Team

CYMED Security Technologies S.R.L.
Short name: CYMED

2.2 Address

CYMED
37-39 Intrarea Glucozei Street, Tronson III, Room P13
0 23828 Bucharest
Romania

2.3 Time Zone

EET – Eastern European Time (UTC/GMT + 2 hours)

2.4 Telephone Number

+40 0751 116875

2.5 Facsimile Number

NOT AVAILABLE

2.6 Electronic Mail Address

Office: office@cymed.ro

Incident Reports: alerts@cymed.ro

2.7 Other Telecommunication
Call Center: (+40)751 116875

2.8 Public Keys and Other Encryption Information

CYMED has the following PGP keys, whose details are:

User ID: Alerts Cymed < alerts@cymed.ro>
Key ID: CCAFD7FE6F4B5B32
Key type: RSA
Key size: 4096
Expiration: 04.12.2023
Fingerprint: AF1F 7D04 4A06 604C EFF1 968E CCAF D7FE 6F4B 5B32
The key and its signatures can be found at the usual large public key-servers.
(http://keys.gnupg.net)

User ID: Cymed Team <office@cymed.ro>
Key ID: BA34F52DCC494730 Key type: RSA
Key size: 4096 Expiration: 08.05.2023
Fingerprint: 7052 B586 3481 7EE5 AF32 041C BA34 F52D CC49 4730
The key and its signatures can be found at the usual large public key-servers.
(http://keys.gnupg.net)

2.9 Other Information
General information about CYMED can be found at https://www.cymed.ro

2.10 Points of Customer Contact
The preferred method for contacting CYMED is via e-mail at:
- office@cymed.ro for general purposes, and
- alerts@cymed.ro for incident reports.

3. Charter
3.1 Mission Statement
CYMED is a commercial entities designated to provide cyber security services to our customers

3.2 Constituency
The team provide cyber security services to the other companies from the Medicarom Group and also for the customer (hospital, clinics, GP - private and public) part of the health system.
Any other customers from other domains than medical, could be considered.

3.3 Sponsorship and/or Affiliation
S.C. INFOWORLD SRL is the main shareholder.

3.4 Authority
CYMD was registered as Cyber Security Technologies SRL at National Trade Register, on 19.09.2020 with unique registration code 43058570.

4. Policies

4.1 Types of Incidents and Level of Support
CYMED is authorized to address all types of computer security incidents which occur, or threaten to occur, in our beneficiary networks and systems.
The level of support given by CYMED will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the CYMEDO's resources at the time, though in all cases some response will be made within 24 hours during working days and all these aspects are stipulated in the contracts we sign with our customers.
Incidents will be prioritized according to their apparent severity and extent.

4.2 Co-operation, Interaction and Disclosure of Information
CYMED highly regards the importance of operational cooperation and information sharing between Computer Emergency Response Teams, and also with other organizations which may contribute towards or make use of their services, with fully compliance of the legal aspects stipulated in the contracts we have with our customers.
All sensitive data and information (personal data, system/service configuration, vulnerabilities with their locations) are transmitted encrypted.
CYMED operates within the confines imposed by Romanian and European legislation.

4.3 Communication and Authentication
In view of the types of information that CYMED will likely be dealing with, telephones and unencrypted e-mail will be considered sufficiently secure for the transmission of low sensitivity data.
If it is necessary to send highly sensitive data by e-mail, PGP encryption will be used.
Where it is necessary to establish trust, for example before relying on information given to CYMED, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust.
Appropriate methods for trust establishment will be used, such as a search of professional associations' members, the use of WHOIS and other Internet registration information etc., along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5. Services

5.1 Incident Response
CYMED will handle the technical and organizational aspects of incidents according with a procedure convened with our beneficiaries. So, CYMED will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage
- Investigating whether indeed an incident occurred;

- Assessing and prioritizing the incident;
- Conducting investigation.

5.1.2 Incident Coordination

- Determining the involved organizations and communicate to our client;
- Contact the involved organizations directly or with our client support to investigate the incident and take the appropriate steps;
- Facilitate contact to other parties which can help resolve the incident;
- Contacting or facilitating contacting appropriate law enforcement officials, if Necessary, according with the law.

5.1.3 Incident Resolution

- Technical assistance and analysis of compromised systems.
- Support in restoring affected systems and services to their previous status.
- Collecting statistics and evidence about incidents, that could be used for protecting against future attacks.

5.2 Proactive Activities

CYMED coordinates and maintains the following activities to the extent possible depending on its resources:

- Informational and educational events;
- Records of security incidents handled will be kept;