SOC-CORPUS RFC 2350 Profile

Corpus Solutions a.s.
Štětkova 1638/18
140 00 Praha 4

Tel.: +420 241 020 333
E-mail: sales@corpus.cz
Internet: www.corpus.cz

IČ: 25764616
DIČ: CZ25764616
Společnost Corpus Solutions a.s je vedená u rejstříkového soudu
v Praze pod spisovou značkou B5936

1 Document Information

This document complies with RFC 2350.

1.1. Date of Last Update

This is version 1.0 as of August 10, 2018.

1.2. Distribution List for Notifications

Email notification of updates is sent to SOC-Corpus **soc@corpus.cz**.

1.3. Locations where this Document May Be Found

The current version of this profile is available at https://corpus.cz/en/csirt_en.html

2. Contact Information

2.1 Name of the Team

Full name: SOC-Corpus Solutions a.s.

Short name: SOC-Corpus

2.2. Address

SOC-Corpus

Corpus Solutions a.s.
Štětkova 1638/18
140 00 Praha 4
Czech Republic

2.3. Time Zone

Time-zone (relative to GMT): Central European Summer Time = GMT+2

2.4. Telephone Number

SOC-Corpus emergency telephone number: +420 241 020 701

SOC-Corpus regular telephone number: +420 241 020 333

2.5. Facsimile Number

Not applicable.

2.6. Other Telecommunication

Not applicable.

2.7. Electronic Mail Address

All incidents reports should be sent to **soc@corpus.cz**

2.8. Public Keys and Encryption Information

Please encrypt sensitive email with the SOC-Corpus Team PGP Key ID: 0x93AA4E24

2.9. Team Members

No public information is provided about SOC-Corpus members.

2.10. Other Information

For additional information about SOC-Corpus, see https://corpus.cz/en/csirt_en.html .

SOC-Corpus is listed by the Trusted Introducer (TI) for CERTs in Europe:

https://www.trusted-introducer.org/directory/teams/soc-corpus.html

2.11. Points of Customer Contact

The preferred method for contacting SOC-Corpus is email.

- For general inquiries, please send email to **soc@corpus.cz**
- In an emergency, contact SOC-Corpus at **+420 241 020 701.**

2.12 Business Hours

The SOC-Corpus hours of emergency are 24*7

Standard hours of operations:

8h00 – 17h00 from Monday to Friday

3. Charter

3.1. Mission Statement

The purpose of the SOC-Corpus is:

1) to assist its customer community in implementing proactive measures to reduce the risks of computer security incidents,
2) to assist its customer community in responding to such incidents when they occur.

3.2. Constituency

SOC-Corpus constituency is composed of all the customer of the Corpus Solutions a.s. who subscribed a Service Level Agreement support contract.

3.3. Sponsorship and/or Affiliation

SOC-Corpus is a part of Corpus Solutions a.s..

SOC-Corpus maintains relationships with various CSIRTs throughout the world, on all continents, on an as-needed basis.

3.4. Authority

As SOC-Corpus is aimed to handle incident response on customers' perimeter, SOC-Corpus has an advisor role with local security teams and has no specific authority to require any specific action. The recommendations, which SOC-Corpus will provide to a customer, will be implemented under the direction of the concerned customer. The main purpose of SOC-Corpus in incident handling is the coordination of incident response with their customer, business partners, and employees. As such, we can only advise our constituency and have no authority to demand certain actions.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled EMERGENCY.

4.2. Co-operation, Interaction, and Disclosure of Information

All incoming information is handled confidentially by SOC-Corpus, regardless of its priority.

Information that is evidently very sensitive in nature is only communicated in an encrypted fashion.

When reporting a sensitive incident, please state so explicitly (for example, by using the label SENSITIVE in the subject field of email) and, if possible, use encryption as well.

4.3. Communication and Authentication

See section 2.8; In cases that involve sensitive information, use of PGP/GnuPG is highly recommended.

5. Services

5.1. Incident Response (Triage, Coordination, and Resolution)

SOC-Corpus a customers in handling the technical and organizational aspects of computer security incidents.

5.2. Proactive Activities

SOC-Corpus performs the following proactive activities:

- Technology watch
- Intrusion detection
- Development of security tools
- Information about major security threats or vulnerabilities to its customers
- Training on security topics

6. Incident Reporting Forms

https://corpus.cz/en/kontakt-csirt-en.html

7. Disclaimers

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