

# VIRTUO GROUP SP. Z O.O. CSIRT

## RFC 2350

### 1. Information about the document

This document provides a description of the activities of CSIRT VIRTUO GROUP SP. Z O.O. in a format compliant with RFC 2350. It contains basic information about the CERT team, such as contact information, description of responsibilities and services offered.

Abbreviation expansion:

Computer Security Incident Response Team - CSIRT

Computer Emergency Response Team - CERT

Security Operation Center - SOC

Certified Information Systems Security Professional - CISSP

Certified in Risk and Information Systems Control - CRISC

Certified Ethical Hacker - CEH

Certified Information Systems Auditor - CISA

Certified Information Security Manager - CISM

Virtual Private Network - VPN

#### 1.1 Date of last update

Document version 1.1, published on 30.05.2024.

#### 1.2 Distribution of notifications of changes to the document

Currently, VIRTUO GROUP SP. Z O.O does not use any distribution lists for notification of changes to this document.

#### 1.3 Where to find the document

The current version of the document is available at:

<https://www.virtuosolution.com/rfc-2350>

## **2.Contact information**

### 2.1 Name of the team

SOC VIRTUO

### 2.2 Address

VIRTUO GROUP SP. Z O.O.

St. Tytusa Chałubińskiego 9/2

02-004 Warsaw, Poland

### 2.3 Time zone

Central European Time (CET) UTC+1

Central European Summer Time (CEST) UTC+2

### 2.4 Phone number

+48 503351483

### 2.5 Fax number

NONE

### 2.6 Other telecommunications

Not available.

### 2.7 E-mail address

Please send notifications, incident reports and operational issues to

[csirt@virtuosolution.com](mailto:csirt@virtuosolution.com)

For inquiries about our offerings, scope of services and business issues, please contact us at

[biznes@virtuosolution.com](mailto:biznes@virtuosolution.com)

### 2.8 Public keys and other encryption information

We use PGP encryption to protect sensitive information.

E-mail: [csirt@virtuosolution.com](mailto:csirt@virtuosolution.com)

PGP key used by VIRTUO GROUP SP. Z O.O.:

User ID: VIRTUO GROUP SP. Z O.O. [csirt@virtuosolution.com](mailto:csirt@virtuosolution.com)

The public key can be seen at the end of the RFC 2350 document

Key footprint: 7CC1C7B2782DD2C7A4C421DB0F9D36CC1B8C2D3C

## 2.9 Team members

SOC VIRTUO consists of an international team of practitioners and security engineers. They have many years of experience and hold such certifications as ISO 27001, CISA, CISM, CRISC, CISSP, CEH, among others. Team members work remotely using a secure VPN using IPsec protocols in conjunction with IKEv2.

## 2.10 Customer contact points

The preferred method of contact by VIRTUO GROUP SP. Z O.O. is email, using our cryptographic keys to ensure integrity and confidentiality.

Business hours are limited to regular business hours (9:00 a.m. to 5:00 p.m. Monday through Friday excluding holidays)

## 3. Statute

### 3.1 Mission

Through experience and commitment, VIRTUO GROUP SP. Z O.O creates personalized solutions, tailored to the needs of each client. Our specialties include IT solutions, consulting services, maintenance, support and cyber security.

VIRTUO GROUP SP. Z O.O. is a team of IT experts specializing in providing innovative technology solutions for business.

The mission of VIRTUO GROUP SP. Z O.O. is to help clients achieve their goals by leveraging the potential of modern technology. Building the competence and capacity of clients in preventing, identifying and minimizing ICT security threats, and supporting them in dealing with these threats.

VIRTUO GROUP SP. Z O.O. serves private, public or government entities with which the company will have contracts to provide incident management services. The company considers the entire virtuosolution.com domain as an area of its special interest.

### 3.3 Sponsorship and affiliation VIRTUO GROUP SP. Z O.O. is a private and self-funded entity.

### 3.4 Empowerment

SOC VIRTUO operates under the direction and authority of the Board of Directors of VIRTUO GROUP SP. Z O.O., based on contracts concluded with clients.

The company handles and coordinates incidents on behalf of its clients in accordance with the terms of the contracts. It also issues regular recommendations from the incident handling process to non-customer stakeholders.

## 4. Policies

### 4.1 Incident types and level of support

The default priority for all incidents is normal, unless otherwise specified in customer contracts. Priorities may be raised at the discretion of the authorities of VIRTUO GROUP SP. Z O.O

The level of support provided by SOC VIRTUO depends on the type, severity and scope of the incident. SOC VIRTUO classifies incidents in accordance with its contracts with customers.

### 4.2 Cooperation, interaction and disclosure of information

Information related to the handling of incidents is treated as confidential and is secured under contracts and confidentiality documents.

### 4.3 Communication and authentication

VIRTUO GROUP SP. Z O.O secures acquired information in accordance with relevant laws and internal regulations on information classification. Data is stored on the Microsoft Azure platform and Microsoft 365 compliant with ISO 27001

Azure platform compliance documentation is available for review at:

<https://learn.microsoft.com/pl-pl/azure/compliance/>

## 5. Services

### 5.1 Incident response

VIRTUO GROUP SP. Z O.O. will support organizations in the entire process of handling ICT security incidents, from preparation, through detection and analysis, to mitigation, decommissioning and recovery, as well as analysis of collected evidence and formulation of recommendations.

## 5.2 Proactive activities

The company will help develop SOC teams and incident management, raise awareness of threats, and participate in the CERT community through training and exercises.

## 6. Reservations

VIRTUO GROUP SP. Z O.O. makes every effort to ensure the accuracy and reliability of the information, but is not responsible for any errors or omissions, or for damages resulting from the use of the data contained in the document.

PGP public key with reference to Section 2.8.

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

```
mDMEZk+jGRYJKwYBBAHaRw8BAQdAMi9sqxXKY0ORbX9zq72Sv+QqgY9o42v/fXi6
8LyDfhi0MFZpcnR1byBHcm91cCBTcCB6IG8uby4gPGluZm9AdmlydHVvc29sdXRp
b24uY29tPoiZBBMWCgBBFiEEC1EEI4bcoKOTBJ7SEYU/C2IbPZYFAMZPoxkCGwMF
CQWjCwcFCwkIBwIClgIGFQoJCAcCBBYCAwECHgcCF4AACgkQEYU/C2IbPZZG2gD/.
Q5o9mcv7edd6HWhq/AEiGlcWurYkdxoL72sxj7OWtxsBALe3UgclWqeupjq6AtPc
WBQ2JfngAdmQf7w2g6iHE/wFuDgEZk+jGRIKKwYBBAGXVQEFAQEHBHfkWxHcZ2j
jvgGuhndGiVDEzQJLcaf5+csG+yttyE9AwEIB4h+BBgWCgAmFiEEC1EEI4bcoKOT
BJ7SEYU/C2IbPZYFAMZPoxkCGwFCQWjCwcACgkQEYU/C2IbPZbQWwEAwLfaL0Hx
YV6Q54yXtnmQWsdm/G0PmHZflazW7NctkoYBALAGVYX0omGOi9sFXT6hlq0JvKGT
i485iQBPviYN1r4B
=cPbZ
```

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