COIG S.A.

ul. Mikołowska 100, 40-065 Katowice
tel. 32 757 33 50 | fax 32 757 41 98
coig@coig.pl | www.coig.pl

WASKO®
GRUPA KAPITAŁOWA

# „Information on the operation of COIG CSIRT" RFC-2350

*English language version*

NIP 634-013-42-05
KRS 00000 92497
ING Bank Śląski S.A. w Katowicach
nr konta: 97 1050 1214 1000 0007 0005 5510

Sąd Rejonowy Katowice-Wschód w Katowicach
Wydział VIII Gospodarczy Krajowego Rejestru Sądowego
Kapitał zakładowy w kwocie 5.400.000 zł
w całości wniesiony

# 1. Document information

This document contains a formal description of COIG CSIRT, based on RFC 2350. It provides information on CSIRT, its communication channels and services.

## 1.1. Date of last update

This is the first document version – 1.0, issued in November 2021.

## 1.2. Notifications distribution list

Presently COIG CSIRT does not use any distribution list for notifications on changes in this document.

## 1.3. Locations, where this document may be found

The present version of this document may be found under https://www.coig.pl/cyberbezpieczenstwo/csirt-coig

## 1.4. Authentication of this document

This document has been signed using a PGP key belonging to CSIRT COIG. Its reference number may be found under https://www.coig.pl/cyberbezpieczenstwo/csirt-coig

# 2. Contact information

## 2.1. Team name

CSIRT COIG

## 2.2. Address

CSIRT COIG

COIG S.A. (further: COIG)
ul. Mikołowska 100
40-065 Katowice, Polska

## 2.3. Time zone

GMT +0100 – Central European Time (CET)
GMT +0200 – Daylight saving time (from the last Sunday of March until the last Sunday of October)

## 2.4. Telephone number

+48 32 757-44-44, +48 32 338-27-00

## 2.5. Fax number

N/A

## 2.6. Other forms of communication

N/A

## 2.7. E-mail address

helpdesk@gk.wasko.pl

## 2.8.Public keys and additional information regarding encryption

Information and public key may be found under https://www.coig.pl/cyberbezpieczenstwo/csirt-coig

## 2.9. Team members

COIG CSIRT consists of cybersecurity experts.

## 2.10. Additional information

CSIRT COIG is a commercial unit providing cybersecurity services to entities that have signed relevant agreements for providing such services. There is no current foreseen to provide services for notifications from any individuals of entities other than those listed.

For more information on COIG CSIRT follow the https://www.coig.pl/cyberbezpieczenstwo/csirt-coig

## 2.11. Customer contact points

helpdesk@gk.wasko.pl

# 3. Statute

## 3.1. Main objectives

COIG CSIRT mission is identifying, analyzing and minimizing risks encountered by COIG and its customers.

## 3.2. Establishment

NSZW SOC ensures support of security relevant incidents for themselves and their customers.

## 3.3. Sponsoring and/or associated

Operation of COIG CSIRT is fully financed by COIG.

## 3.4. Authorities

COIG CSIRT operates under the auspices and authorization of COIG management and is bound by its internal regulations.

# 4. Principles

## 4.1. Types of incidents and level of support

COIG CSIRT is allocated to respond to all incidents occurring in infrastructure owned by COIG and entities referred to in point 2.10. The level of support in case of a security incident depends on its nature, duration time, extent and available means. Regardless of any specific case, COIG CSIRT response time does not exceed 1 working day. Incidents will be responded to according to the assigned priority. Details are specified in contracts concluded with any particular customer.

## 4.2. Cooperation, interaction and information disclosure

COIG CSIRT exchanges information with other CSIRT teams and parties involved. Information exchanged does not contain sensitive data. Sensitive data, such as personal data, configuration of operating system, information on found vulnerability, in case of necessity, is encrypted if it is sent through an unencrypted communication channels.

## 4.3. Communication and authentication

Information transferred to COIG CSIRT through the telephone is considered to be secure even if it is not encrypted. Unencrypted information sent through e-mail is considered to be safe enough for transmission of low sensitivity data. In case of transmitting sensitive data through e-mail, it will be additionally encrypted using PGP.

# 5. Services

## 5.1. Incident handling

COIG CSIRT ensures capability to respond to security incidents in areas of:

### 5.1.1. Incident evaluation

1. Assessment of incident authenticity.
2. Incidents correlation on basis of collected data.
3. Constant seeking for ways to improve team efficiency.
4. Defining the extent of the incident.

### 5.1.2. Incident coordination

1. Determining source of the incident (used vulnerability).
2. Facilitating contact with parties that may be interested as to the present incident.
3. Facilitating contact with law enforcement authorities.
4. Reporting to other CSIRT.
5. Creating user notices in case the incident is directly connected with them.

### 5.1.3.Incident analysis

The scope of support depends on type, significance, type of entity that the incident applies to. Basic tasks:

- Assessment of potential risk causing genuine effects
- Assessment of potential extent of the incident and resources it affects.
- Defining incident priority
- Defining the initial cause of the incident
- Defining appropriate response
- Collecting proof and indicators of compromise

## 5.2. Proactive measures

1. COIG CSIRT publishes information on its website regarding new risks about which there in no, common knowledge.
2. COIG CSIRT publishes on its website education materials regarding user behavior, potential global and local risks, training on subsidiary resources.
3. Creating and improving tools and security mechanisms to continuously increase level of security.

## 6. Reporting the incident

Incidents are to be reported through e-mail: helpdesk@gk.wasko.pl

## 7. Disclaimers

Any disclaimers addressed to COIG CSIRT may be formed exclusively by entities having effective service provider agreement with COIG.

COIG CSIRT and COIG have taken all means and measures while preparing information, notices and security alarms and does not bear any responsibility for errors, omissions or damages arising in connection with information contained within.