# RFC 2350 – CSIRT of the ERGO Group

**Contact**

CSIRT of the ERGO Group

Tel.: +49 211 477 4700

**Scope of application**
ERGO Group Companies

**Valid from**
08.04.2024

**Version**
1.0

**Classification**
Unrestricted / Public

# Index

# 1. Document Information

This document contains a description of ERGO Global IT Security Computer Incident Response Team (CSIRT of the ERGO Group) in accordance with RFC 2350. It provides basic information about CSIRT of the ERGO Group, the ways it can be contacted and describes the services offered.

### 1.1. Date of Last Update

The document was last updated on 8 April 2024.

### 1.2. Distribution List for Notifications

There are no distribution lists defined for the notification about updates to this document.

### 1.3. Locations where this Document May Be Found

The current version of the description of the CSIRT of the ERGO Group is available at: https://www.ergo.com/en/Unternehmen/Corporate-Governance/Richtlinien-Regelwerke
.

# 2.Contact Information

### 2.1. Name of the Team

CSIRT of the ERGO Group.

### 2.2. Address

Flowing text Visiting and postal address is:
ERGO Group AG
ERGO-Platz 1
40198 Düsseldorf
Germany

### 2.3. Time Zone

UTC+2h (CEST) summertime between the last Sunday of March and the last Sunday of October. UTC+1h (CET) otherwise.

### 2.4. Telephone Number

+49 211 477 4700.

### 2.5. Facsimile Number

None.

### 2.6. Other Telecommunication

None.

### 2.7. Electronic Mail Address

csirt@itergo.com.

### 2.8. Encryption Information

In case of a required confidential exchange, please write an e-mail with request for a key exchange (see 2.7).

### 2.9. Team Members.

No information is provided in public.

### 2.10. Other Information

None.

### 2.11. Points of Customer Contact

Hours of operation are generally restricted to business hours: Mon-Fri, 9 a.m. - 5 p.m. CET/CEST. The preferred way of contacting the CSIRT of the ERGO Group is by sending an e-mail to csirt@itergo.com. In case of urgent situations, the CSIRT of the ERGO Group can be contacted by calling the hotline (see Ch. 2.4), available 24/7.

# 3.Charter

### 3.1. Mission Statements

The purpose of the CSIRT of the ERGO Group is to coordinate and operate activities regarding IT security incidents for the audience defined in Ch. 3.2 to avoid or reduce potential risks..

### 3.2. Constituency

Services are available to the ERGO Group AG and its subsidiaries. The CSIRT of the ERGO Group has authority over ASN AS28674.

### 3.3. Sponsorship and/or Affiliation

The CSIRT is part of the ERGO Group AG.

### 3.4. Authority

The main purpose of the CSIRT of the ERGO Group is the group-wide and multinational coordination of security incident response and operative security incident handling on behalf of its constituency and/or at their request (see Ch. 3.2).

# 4.Policies

### 4.1. Types of Incidents and Level of Support

The CSIRT of the ERGO Group duties include proactive and reactive handling of all possible kinds of IT security incidents. Starting of response activities is based on the impact severity of the security incident.

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

The CSIRT of the ERGO Group cooperates with the relevant public authorities and regulatory bodies and interacts with trusted CSIRTs on a national and international level where considered useful mainly by sharing experience and best practices. This type of cooperation may also include the exchange of information about security incidents and vulnerabilities. The CSIRT of the ERGO Group always protects the privacy of its partners and constituents, and process the information in compliant with the restrictions by German Federal Data Protection Act (BDSG) and the EU General Data Protection Regulation (GDPR).

### 4.3. Communication and Authentication

The Information Sharing Traffic Light Protocol (ISTLP) is applied on any information exchanged between the CSIRT of the ERGO Group and other CSIRTs, regardless of the communication media (e.g., e-mail, telephone, or face-to-face meetings). Confidential information shall be exchanged according to the procedure in chapter 2.8.

# 5. Services

### 5.1. Incident Triage

- determine whether a reported incident is authentic and true positive
- determine which constitutes are or might be affected
- assess and prioritize the incident

### 5.2. Incident Response

- lead the security incident response process
- assure that security incidents are responded properly and provide support for mitigation when it is needed
- contact the affected organizations to collaborate with and inform them to take the appropriate actions
- establish communication channels and communicate necessary topics with relevant parties in cases of security incidents

### 5.3. Digital Forensics

- log analysis
- memory forensics
- physical/virtual drive forensics
- network forensics
- malware analysis

# 6. Incident Reporting Forms

Incidents can be reported via communication channels mentioned in this document (2.4 and 2.7) and are not required to meet any particular form.

# 7. Disclaimers

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