ENERGOTEL.SK-CSIRT description document according to RFC 2350

1. Document Information
This document provides formal description of the ENERGOTEL.SK-CSIRT based on RFC 2350. It provides basic
information about the CSIRT team, the ways it can be contacted, describes its responsibilities and the services offered.

1.1. Date of Last Update
This is version 1.0, published on 9.1.2021

1.2. Distribution List for Notifications
E-mail notifications of updates are sent to:
- All ENERGOTEL.SK-CSIRT constituencies

1.3. Locations where this Document May Be Found
The current version of this document can always be found at http://www.energotel.sk/csirt

2. Contact Information

2.1. Name of the Team
ENERGOTEL.SK-CSIRT - Computer Security Incident Response Team of Energotel, a.s.

2.2. Address
Computer Security Incident Response Team (CSIRT)
Energotel, a.s.
Miletičova 7
821 08 Bratislava
Slovak Republic

2.3. Time Zone
Central European Time: GMT+1,
DST: GMT+2 (DST starts at 01:00 UTC on the last Sunday in March and ends at 01:00 UTC on the last Sunday in October.)

2.4. Telephone Number
+421 2 573 855 88

2.5. Facsimile Number
Not available.

2.6. Other Telecommunication
Not available.

2.7. Electronic Mail Address
Official e-mail address: csirt@energotel.sk

2.8. Public Keys and Encryption Information

ENERGOTEL.SK-CSIRT PGP Key Fingerprint: 9D48 BBB5 E658 D17D E91B AC52 E994 FE88 3944 4188
Please use this key when you want/need to encrypt messages that you send to ENERGOTEL.SK-CSIRT.
These keys can be found on most key-servers.

2.9. Team Members
Pavol Krigler is team coordinator for CSIRT team. No other information is provided about the ENERGOTEL.SK-CSIRT team members in public.

2.10. Other Information
General information about the ENERGOTEL.SK-CSIRT can be found at http://www.energotel.sk/csirt

2.11. Points of Customer Contact
Regular cases: the preferred method for contacting ENERGOTEL.SK-CSIRT is via e-mail csirt(at)energotel.sk.
Regular response hours: from Monday to Friday, 08:00 – 16:30 (except holidays).
Urgent cases: use phone number +421 257 385 588

3. Charter

3.1. Mission Statement

The goals of ENERGOTEL.SK-CSIRT are:
- to assist customers of Energotel, a.s. network in responding to such incidents when they occur
- to create trustworthy central contact point for ICT infrastructure at Energotel, a.s.
- to prevent, detect and resolve computer security incidents related to the Energotel, a.s. ICT infrastructure
- to raise IT security awareness among our constituents

3.2. Constituency
The constituency are employees of Energotel, a.s. organization:
- internal infrastructure in the whole Autonomous system AS31117 marked as INFRA-AW in the RIPE database
- domain services: Cache DNS, Authoritative DNS
- domain: energotel.sk
- domain: energotel.eu
- Due to nature of provided services to customers of Energotel, a.s. Slovak Republic, different Level of Support is given to different types of constituents

3.3. Sponsorship and/or Affiliation
ENERGOTEL.SK-CSIRT is sponsored by Energotel, a.s. Slovak Republic, which is part of.

3.4. Authority
ENERGOTEL.SK-CSIRT operates under the auspices of, and with authority delegated by, the management of Energotel, a.s. Slovak Republic.

4. Policies

4.1. Types of Incidents and Level of Support
The ENERGOTEL.SK-CSIRT is authorized to address all types of computer security incidents which occur, or threaten to
occur, in its constituency. The level of support given by ENERGOTEL.SK-CSIRT 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 ENERGOTEL.SK-CSIRT's resources at the time. Special attention will be given to issues affecting important
infrastructure.

No direct support will be given to end-users, as they are expected to contact their
system administrators. ENERGOTEL.SK-CSIRT is committed to keep the constituency informed of potential
vulnerabilities and existing threats, and where possible, will inform theirs of such threats and vulnerabilities
before they are actively exploited.

4.2. Co-operation, Interaction and Disclosure of Information
ENERGOTEL.SK-CSIRT will cooperate with other organisations in the field of computer security. This cooperation also includes and often requires the exchange of vital information regarding security incidents and vulnerabilities. In such cases CSIRT-MU conforms to the Information Sharing Traffic Light Protocol (TLP). Nevertheless ENERGOTEL.SK-CSIRT will protect the privacy of their customers.
ENERGOTEL.SK-CSIRT operates under the restrictions imposed by Slovak law.

4.3. Communication and Authentication
For normal communication not containing sensitive information ENERGOTEL.SK-CSIRT will use conventional methods like unencrypted e-mail.
For secure communication PGP-encrypted e-mail or telephone will be used.

5. Services

5.1. Reactive Services
- Alerts and Warnings
- Incident detection
- Incident analysis
- Incident response
- Incident containment, eradication and recovery
- Assistance with incident handling on site
- Reaction to incidents
- Support of incident response efforts
- Coordinating responses to incident handling
- Design of countermeasures to prevent further continuation, propagation and recurrence of incidents

5.2. Preventive Activities

- Education and raising awareness in the field of information security

- Training
- Cooperation with other CSIRT teams
- Monitoring and documentation of incidents
- Connecting to Unified information system of cybersecurity
- Providing information to Unified information system of cybersecurity
- Receiving and sending early warnings of incidents via Unified information system of cybersecurity

6. Incident Reporting Forms
If possible, please write an email with detailed description of the incident to csirt@energotel.sk.

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