The Computer Security Incident Response Team

Cyber security incident reporting

Who can report the incident to the CSIRT GOV?

At the national level incidents may be reported to the CSIRT GOV by entities listed in Article 26 (5) the Act of 5 July 2018 on the National Cyber Security System. The entities falling within the constituency of CSIRT GOV comprise:

o listed entities of the public finance sector;

o entities subordinated to or supervised by the Prime Minister;

o National Bank of Poland;

o National Holding Bank;

o entities in charge of facilities, installations, equipment, and services in the field of critical infrastructure referred to in Article 5b (7) (1) of the Act of 26 April 2007 on crisis management.

If you are a foreign CSIRT/CERT or other entity in charge of cyber security you can report an incident that, in your opinion, remains within the purview of the CSIRT GOV by sending a relevant information and complying with the procedure described in the section below.

Whenever an incident remains outside the CSIRT GOV constituency, it will be forwarded to the other Polish national CSIRTs respectively with a relevant notification to the reporting entity.

How can you report the incident to the CSIRT GOV?

Where an incident occurs which needs to be reported to the CSIRT GOV, you are asked to provide as much information as you can to allow the CSIRT GOV to handle your incident expediently and accordingly.

The notification about incident should include information on a reporting entity and description of the incident (i.e. date of occurrence, category of incident, incident impact, relevant IoC’s, if possible).

Do not copy and paste malicious code directly into your report.

In case of suspicious emails and any content of this nature, please attach them to your report.

You can report an incident by:

1. forwarding an e-mail containing all relevant information
at {mailto(incydent@csirt.gov.pl,encode = secure)} (preferred mode);

2. calling the watchkeepers by phone +48 22 58 59 373;

3. sending information by fax: +48 22 58 58 833.

What about the maintaining the confidentiality of the transmitted data?

In order to maintain the confidentiality of the provided data, encryption of electronic data may be used when an incident is handed over to the CSIRT GOV. The PGP/GPG can be used for this purpose. The currently valid public PGP key for the CSIRT GOV team is available at www.csirt.gov.pl in the PGP section.

Submission of contact persons to the CSIRT GOV

If you are a national CSIRT or any other foreign entity and you need to establish contact with CSIRT GOV, please send your contact details directly via email
at {mailto(incydent@csirt.gov.pl,encode = secure)} (the PGP encryption recommended).