RFC 2350

1. Document information

This document provides a description of the security team: the Security Management Department of the Warsaw Stock Exchange (GPW DZB), in accordance with RFC 2350.

It provides basic information about GPW DZB and how to contact GPW DZB, and it describes the team's responsibilities and services offered.

1.1 Date of the last update

This is version 1.0, published on 2023-07-12.

1.2 Distribution list for notifications

GPW DZB currently does not use any distribution list to notify of changes to this document.

1.3 Locations where this document may be found

The current Polish version of the document is available at:
https://www.gpw.pl/pub/GPW/RFC2350_PL_GPW.txt
The English version of this document is available at:
https://www.gpw.pl/pub/GPW/RFC2350_EN_GPW.txt
Make sure you are using the latest version.

1.4 Authenticating this document

The Polish and English versions of this document have been signed with the PGP key of the GPW DZB team.

2. Contact information

2.1 Name of the team

Security Management Department of the Warsaw Stock Exchange, GPW DZB

2.2 Address

GPW
Giełda Papierów Wartościowych w Warszawie S.A. / The Warsaw Stock Exchange
ul. Książęca 4
00-498 Warszawa
Poland

2.3 Time zone

UTC +0100 - Central European Time (CET)
UTC +0200 - Central European Summer Time (CEST - from the last Sunday in March to the last Sunday in October)

2.4 Telephone number

+48 22 53 777 08
+48 669 55 1111

2.5 Facsimile number

Not available

2.6 Other telecommunication

Not available

2.7 Electronic mail address

security@gpw.pl

2.8 Public keys and encryption information

PGP key used by GPW DZB:
KeyID: 0x4941A9E7
Fingerprint: 49F2 6339 2259 0E47 DE3B 97F6 F174 3269 4941 A9E7
The public key can be found at:
https://www.gpw.pl/pub/GPW/RFC2350_klucz_PGP.txt

2.9 Team members

The GPW DZB team consists of experienced cyber security experts.

2.10 Other information

For general information on GPW's cybersecurity policies, visit https://www.gpw.pl/zasady-cyberbezpieczenstwa

3. Charter

3.1 Mission statement

GPW DZB is responsible for building competences and skills to avoid, identify, and mitigate cyber threats, in particular to prevent the occurrence of cyber security incidents by implementing appropriate processes, tools, policies to improve responsiveness to incidents and to provide operational support in handling major cyber security incidents which may affect the assets and interests of the GPW Group Companies.

3.2 Sponsorship and/or affiliation

GPW DZB is affiliated with the GPW Group.

3.3 Authority

GPW DZB operates in accordance with the security management standards of the Warsaw Stock Exchange and is under the authority of the Director of the GPW Security Management Department.

4. Policies

4.1 Types of incidents and level of support

GPW DZB is authorised to handle all types of cyber security incidents that occur or may occur in its area of operation. All incident reports received by GPW DZB are analysed, classified, and prioritised in accordance with internal regulations to ensure an efficient and appropriate level of service.

4.2 Co-operation, interaction and disclosure of information

GPW DZB is committed to working openly and transparently with our trusted partners, including the international CERT community, in line with the policies of the Warsaw Stock Exchange. For this reason, all CERTs worldwide may contact GPW DZB (security@gpw.pl) to establish collaboration, ask questions or participate in information sharing initiatives as necessary.

4.3 Communication and authentication

The preferred method of contacting GPW DZB is by email. Primary email address: security@gpw.pl
We encourage our clients to use PGP/GPG cryptographic tools when sending confidential information to GPW DZB.

If the use of email is not possible (or not advisable for security reasons), GPW DZB may be contacted by telephone during regular business hours at the telephone numbers provided in section 2.4. The working hours of GPW DZB are limited to regular business hours (08:00-16:00 Monday to Friday except for public holidays in Poland).

5. Services

5.1 Incident response

This service aims to conduct reconnaissance of and coordinate response to cyber security incidents. Activities to support and coordinate incidents include assessing available information, validating and verifying it, gathering additional evidence, communicating with relevant parties, and finally proposing solutions to resolve the incident.

5.2 Monitoring

This service aims to detect cyber security incidents and analyse them to determine the authenticity, cause, severity, and appropriate response to the incident.

5.3 Preventive activities

Preventive activities include the identification of existing cyber security vulnerabilities in IT systems and the ongoing expansion of the available threat data.

5.4 Proactive activities

GPW DZB provides training and periodic reports on potential threats.

6. Incident reporting forms

Security incidents are reported via encrypted email to security@gpw.pl using a PGP key. The following information should be provided in the report where possible:

- Contact information
  - First name and surname of reporting person, email address and telephone number.
- Date and time of the incident.
- Description of the security incident.
  - Type of incident
    - Data loss/data compromise
    - System damage
    - Financial loss
    - Rules violation
    - Breach of information security policy or procedure
    - Currently unknown
    - Suspicious email (spam/phishing, link or attachment)
    - Other
  - Location of person or system affected by the incident.
  - Number of persons/systems affected by the incident.
  - Technical data
    - IP address(es),
    - FQDN(s),
    - System logs,
    - Suspicious email with attachments,

- Other data that may help the analysis of the incident.
  - Actions taken to date in response to the incident.

7. Disclaimer

While every precaution is taken in the preparation of information, notifications and alerts, GPW DZB assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

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

mDMEZV8+rhYJKwYBBAHaRw8BAQdA52uyX4SpLF6RaXGa4qY4gPmojv2EWZ444vCC

IcSrpJ20HlNlY3VyaXR5IEdQVyA8c2VjdXJpdHlAZ3B3LnBsPoiZBBMWCgBBFiEE

nxnuJ/iKkWPgeSPXy/BoMSidOdAFAmVfPq4CGwMFCQ0q/YIFCwkIBwICIgIGFQoJ

CAsCBBYCAwECHgcCF4AACgkQy/BoMSidOdBDxwEAoAmJBaGOWEaLR05NZJmOvMHg

hCA97X6Bfpv9uOFb6VkA/0dAqcbimgiQP1/w/Sxlz354LmVqcENPIuICEhZNdgED

uDgEZV8+rhIKKwYBBAGXVQEFAQEHQJ4Xx5p+IWLQDPobwsUsq7tWVQT/PZ2D6ale

cMnTidt7AwEIB4h+BBgWCgAmFiEEnxnuJ/iKkWPgeSPXy/BoMSidOdAFAmVfPq4C

GwwFCQ0q/YIACgkQy/BoMSidOdDt2QEA5EODaqx5sdPnQyLFC4g/qP2CjqLMLvH6

uHDhG2cMHMIBAN5bpeEoRFCb4a42nwRFcisty4cdZMRCnK81Tqex85MH

=W1wz

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