RFC2350

PGGM-CERT is structured in accordance with the RFC2350 guidelines, published by the Network Working Group of IETF.org.

Document Information

- **Version**: 1.0
- **Last revision date**: 01-03-2017
- **Last review date:** 23-09-2020
- **Update notification distribution list:** Notifications for distribution of this document are not provided. Form information contact PGGM-CERT using its e-mail address.
- **Document publication location:** https://www.pggm.nl/en/security/

Contact Information

- **Team name**: "PGGM-CERT", PGGM's Computer Emergency Response Team
- **Address details**: PGGM
  Attn: PGGM-CERT
  PO Box 117
  3700 AC Zeist
  The Netherlands
- **Time zone**: PGGM-CERT uses Central European Time (CET), including Daylight Saving Time (DST). GMT+0100 in winter and GMT+0200 in summer.
- **Telephone**: +31 (0)30 277 72 40
- **Fax**: none
- **Other telecommunications**: none
- **Public keys and encryption**: PGGM uses PGP for encryption and digital signatures.
- **Team members**: The names of PGGM team members are not made public. Team members will identify themselves when contact is made in the event of a security incident.
- **Contact information**: PGGM-CERT can be reached from 08:00 to 18:00 on: + 31 (0)30 277 72 40. Outside these office hours, support is provided on a best-effort basis. PGGM-CERT can be reached via e-mail at CERT@pggm.nl .
- **Additional contact information**: valse-email@pggm.nl; informatiebeveiliging@pggm.nl

CERT Charter

Mission Statement

PGGM-CERT's mission is to minimise the impact of a threat or damage resulting from a (cyber) attack or digital break-in.

Target Group (constituents)

PGGM-CERT's target group is PGGM as a whole.

Objectives

PGGM-CERT's objectives are as follows:

- To be the first point of contact and the connecting link in information security incidents
- To be able to immediately act in the event of information security incidents relating to computers and the network
- To combine technical and functional expertise of PGGM employees in dealing with an information security incident
- To limit damage and to facilitate the recovery of services
- To promote information security awareness at PGGM

Sponsors

PGGM-CERT is part of the PGGM organisation and reports directly to the PGGM Security & Quality Office. PGGM's Executive Committee has adopted the creation, role and authorities of PGGM-CERT and its organisation structure.

Authority

PGGM-CERT registers incidents relating to information security and coordinates the handling thereof. PGGM-CERT works together with the responsible employees, including those of PGGM's suppliers and clients, and has an advisory role. However, when circumstances warrant, PGGM-CERT has the authority to take appropriate measures suitable for resolving the incident. These tasks are carried out in accordance with PGGM's crisis management structure.

Policies

Type of incidents: PGGM-CERT acts on all information security incidents that occur or threaten to occur within its target group, with a focus on:

- Cyber-related incidents and threats
- Data leaks
- Observed vulnerabilities (responsible disclosure)
- Abuse, such as phishing, spam, viruses

Cooperation and sharing of information: Information provided to PGGM-CERT will be treated as confidential and will not be shared with third parties without prior permission, unless required by law. PGGM-CERT uses the Traffic Light Protocol in its communications with external parties.

Communication and authentication: PGGM-CERT prefers to communicate by e-mail. PGGM-CERT uses PGP keys for the encryption and digital signature of confidential traffic. The PGGM-CERT public key is published on the public key servers.

Services

Incident triage: All incidents are registered and evaluated for impact and priority. The triage function is responsible for assigning the incidents to the right people and for monitoring progress.

Incident coordination: During the course of the incident, its cause is determined, the relevant contacts are established with internal and external stakeholders and, if necessary, the escalation process is activated.

Incident handling: PGGM-CERT does not solve any incidents itself. PGGM-CERT provides support in the form of the coordination between the relevant parties, external intelligence, evaluation, reporting and any follow-up activities.

Incident Reporting

No special forms for reporting incidents are made available.

Disclaimer

PGGM-CERT cannot fully guarantee the accuracy and availability of all information. PGGM-CERT does not accept any liability for damage arising from the absence or inaccuracy of the information provided.