Amphia Ziekenhuis profile

This profile of Amphia-CERT is established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version 1.1 of 12-7-2018.

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3 .
E-mail notification of updates are sent to:

- All Amphia-CERT members
- All Amphia-CERT constituents
- SURFcert (see https://www.surf.nl/diensten-en-producten/surfcert/index.html)

Any questions about updates please address to the Amphia-CERT e-mail address:
amphiaCERT@amphia.nl

1.3. Locations where this Document May Be Found

The current version of this profile is always available on http://www.amphia.nl

2. Contact Information

2.1. Name of the Team

Full name: Amphia CERT

Amphia CERT is the CERT or CSIRT team for Amphia Ziekenhuis Breda/Oosterhout in the Netherlands.

2.2. Address

Amphia Ziekenhuis
Amphia CERT
Department IMT
P.O Box 90157
NL – 4800RL Breda
The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Telephone Number

+31(0)76-5955000

From 8.00 until 17.00 you can call our helpdesk at +31(0)76-5951025 and after 17.00 until 8.00 hour +31(0)76-5955000 and ask for the system engineer of IMT.

2.5. Facsimile Number

+31(0)76-5951430
Note: this is not a secure fax.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address
amphiacert@amphia.nl

This address can be used to report all security incidents related to the Amphia-CERT constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information
PGP is currently only on request supported for secure communication.

An Amphia CERT public PGP key is not yet available on the public keyservers.

2.9. Team Members
No information is provided about the Amphia-CERT team members in public. The Amphia CERT team members are selected from the ranks of the Amphia ICT professionals.

Further details can be foud at
https://www.amphia.nl/amphia-cert

2.10. Other Information
- See the Amphia webpages https://www.amphia.nl
- Amphia-CERT is registered by SURFcert, see https://wiki.surfnet.nl/display/CSIRTs

2.11. Points of Customer Contact
Regular cases: use Amphia CERT e-mail address.
Regular response hours: Monday-Friday, 08:00-17:00 (except public holidays in the Netherlands).

EMERGENCY cases:
send e-mail with EMERGENCY in the subject line.

The Amphia CERT phone number is available outside the regular response hours

3. Charter

3.1. Mission statement
The mission of Amphia CERT is to coordinate the resolution of IT security incidents related to the Amphia Ziekenhuis constituency (see 3.2), and to help prevent such incidents from occurring.

For the world, Amphia CERT is the Amphia interface with regards to IT security incident response. All IT security incidents (including abuse) related to the Amphia Ziekenhuis can be reported to Amphia CERT.

3.2. Constituency
The constituency for Amphia CERT is Amphia Ziekenhuis and institutions connected to the Amphia Ziekenhuis network, with all related medical staff, Amphia employees and suppliers.

3.3. Sponsorship and/or Affiliation
Amphia CERT is part of IMT, the ICT-department of Amphia Ziekenhuis.

3.4. Authority
Amphia CERT coordinates security incidents on behalf of Amphia Ziekenhuis and has no authority reaching further than that. Amphia CERT is however expected to make operational recommendations in the course of their work. Such recommendations can include but are not limited to blocking addresses or networks. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made.

4. Policies

4.1. Types of Incidents and Level of Support
All incidents are considered normal priority unless they are labeled EMERGENCY. Amphia CERT itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to Amphia CERT as EMERGENCY, but it is up to Amphia-CERT to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information
ALL incoming information is handled confidentially by Amphia-CERT, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.

Amphia-CERT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.first.org/tlp/) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

Amphia CERT will use the information you provide to help solve security incidents, as all CERTs do. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymized fashion.

If you object to this default behavior of Amphia CERT, please make explicit what Amphia CERT can do with the information you provide. Amphia CERT will adhere to your policy, but will also point out to you if that means that Amphia CERT cannot act on the information provided.

Amphia CERT does not report incidents to law enforcement, unless national law requires so. Likewise, Amphia CERT only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that Amphia-CERT cooperates in an investigation. When a court order is absent, Amphia CERT will only provide information on a need-to-know base.

4.3. Communication and Authentication
See 2.8 above. Usage of PGP/GnuPG in all cases where sensitive information is involved is highly recommended.

5. services

5.1. Incident Response (Triage, Coordination and Resolution)
Amphia CERT is responsible for the coordination of security incidents somehow involving Amphia Ziekenhuis. Amphia CERT therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the Amphia Ziekenhuis and externally – however Amphia CERT will offer support and advice on request.

5.2. Proactive Activities

Amphia CERT pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking.

Amphia CERT advises Amphia Ziekenhuis on matters of computer and network security. It can do so pro-actively in urgent cases, or on request.

Both roles are roles of consultancy: Amphia CERT is not responsible for implementation.

6. Incident reporting Forms

Not available. Incidents are reported in Amphia Ziekenhuis central Incident-registration system.

7. Disclaimers

On the website https://www.amphia.nl/disclaimer is an disclaimer available.