The following profile of the Danish Centre for Cyber Security (CFCS-DK) has been established in adherence to RFC-2350.

1 Document Information

1.1 Date of Last Update

This is version 2.0, published April 16, 2018.

1.2 Distribution List for Notifications

Changes to this document are not distributed by a mailing list. Please address questions or remarks to cert (at) cert.cfcs.dk

1.3 Locations where this Document May Be Found

The current version of this profile is always available on:
http://www.cfcs.dk

2 Contact Information

2.1 Name of the Team

The Danish Centre for Cyber Security (CFCS-DK)

2.2 Address

Danish Defence Intelligence Service
Centre for Cyber Security
Kastellet 30
2100 Copenhagen Ø
Denmark

2.3 Time Zone

* CET, Central European Time (UTC+1, between last Sunday in October and last Sunday in March)
* CEST (also CET DST), Central European Summer Time (UTC+2, between last Sunday in March and last Sunday in October)

2.4 Telephone Number

+45 3332 5580

2.5 Facsimile Number

none

2.6 Other Telecommunication

None

2.7 Electronic Mail Address

cert (at) cert.cfcs.dk

2.8 Public Keys and Encryption Information

CFCS-DK uses PGP for digital signatures and to receive encrypted information. The key is available on public PGP/GPG key servers and at https://www.cfcs.dk.
Information about the key: Key-ID: 6740E2CD
Fingerprint: 2CE4 BA61 B873 B089 0BE9 4ED2 3CDA 6879 6740 E2CD

2.9 Team Members

A list of CFCS-DK team members is not publicly available.

2.10 Other Information

General information about Centre for Cyber Security is available at https://www.cfcs.dk

2.11 Points of Customer Contact

The main point of contact is the CFCS-DK mail address,
cert (at) cert.cfcs.dk

In case of reporting internet security incidents, please contact cert (at) cert.cfcs.dk.
Regular response hours (local time, save public holidays in Denmark) are Monday to Friday from 09:00 - 16.30.
Outside working hours is the Duty Officer available for incident reporting and can be reached at +45 3289 8989.

3 Charter

3.1 Mission Statement

The Centre for Cyber Security is the national IT security authority, Network Security Service and National Centre of Excellence in cyber security. The Centre's mission is to advise Danish public authorities and private companies that support functions vital to society on how to prevent, counter and protect against cyberattacks and incidents that may harm the Danish communications infrastructure.

3.2 Constituency

CFCS-DK is the Danish Government Computer Emergency Response Team for the Danish Government.
The constituency is Danish government institutions and selected critical infrastructure owners.

3.3 Sponsorship and/or Affiliation

CFCS-DK is part of Danish Defence Intelligence Service under the Ministry of Defence.

3.4 Authority

CFCS-DK's purpose in incident warning and handling is guidance and coordination of incident response. As such, we advise constituents and have no authority to demand certain actions.

4 Policies

4.1 Types of Incidents and Level of Support

CFCS-DK handles various types of security incidents. The level of support depends on the type of the incident and the severity as determined solely by CFCS-DK.

4.2 Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by CFCS-DK, regardless of its priority.

Sensitive or classified Information is only communicated and stored in a secure environment, if necessary using encryption technologies.

CFCS-DK will use the information obtained to help solve security incidents. Information will only be distributed to other teams and team members according to relevant legislation and on a need-to-know basis, preferably as anonymized data.
CFCS-DK uses the Traffic Light Protocol (TLP) for marking information and uses the NATO/EU classification scheme.

4.3 Communication and Authentication

The preferred method of communication is via e-mail. When the content is sensitive or requires authentication, the CFCS-DK PGP key is used for signing e-mail messages. All sensitive communication to CFCS-DK should be encrypted against CFCS-DK's PGP key.

5 Services

5.1 Incident response

Incident response is provided 24/7. CFCS-DK will investigate incidents

and coordinate responses from relevant stakeholders. This may include involvement of experts, tools and other capabilities to act, analyse and communicate with stakeholders and media.

5.1.1 Incident Triage

* Investigating whether an incident occurred.
* Determining the extent of the incident.

5.1.2 Incident Coordination

* Determining the initial cause of the incident.
* Facilitating contact with other sites which may be involved.
* Communicate with stakeholders and media.

5.1.3 Incident Resolution

* Providing advice to the reporting constituent that will help removing the vulnerabilities that caused the incident and help securing the systems from the effects of the incidents.
* Evaluate and give advice to stakeholders which actions are most suitable to provide desired results regarding the incident resolution.
* Provide assistance in evidence collection and data interpretation when needed.

5.2 Proactive Activities

CFCS-DK informs the constituency using advisories, factsheets and whitepapers to prevent ICT related incidents or to prepare for such incidents and reduce the impact.

6 Incident Reporting Forms

There are no special forms required to report an incident, but constituents are encouraged to supply the necessary information as defined on the CFCS-DK website www.cfcs.dk.

7 Disclaimers

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