CERT Danone

RFC 2350

DANONE
ONE PLANET. ONE HEALTH

Version	Version 1.0
History	Creation 07/09/2021 (Version 1.0)
Approval procedure	Approved by CISO on 26/08/2021
Target Group	Public
Document Owner	Chief Information Security Officer
Level of Confidentiality	Public (TLP:White)
Number of Pages	6
Languages	English

01 About this document

This document contains a description of CERT Danone according to RFC 2350. It provides basic information about the CERT Danone, its channels of communication, and its role and responsibilities.

Date of last update

This is version 1.0, published on 26/08/2021.

Distribution list for notifications

There is no distribution list for notifications.

Locations where this document may be found

The current version of this document can be found at:
https://www.danone.com/content/dam/danone-corp/danone-com/about-us-impact/policies-and-commitments/en/2021/Danone-CERT-RFC-2350-2021.pdf

02 Contact information

Name of the team

CERT Danone : The Danone Computer Emergency Response Team.

Address

CERT Danone
IT & Data direction
17 Boulevard Haussmann
75009 PARIS
FRANCE

Time zone

CEST / Central European Summer Time

Telephone number

None available

Facsimile number

None available

Other Telecommunication

None available

Electronic Mail Address

cert@danone.com

Public keys and other encryption information

Our current PGP-key may be obtained by sending a request by mail at cert@danone.com

Team members

The team is made up of IT security analysts. The list of the team members is not publicly available.

Other information

None available

Points of customer contact

The preferred method to contact CERT Danone is via email. Please request and use our cryptographic key to ensure integrity and confidentiality.
CERT Danone's hours of operations are 24/24, 7/7.

03 Charter

Mission statement

CERT Danone's mission is to manage and investigate IT security incidents and coordinate IT security incident response for the Danone company.

The Danone CERT's scope covers prevention, detection, response and recovery. It will investigate any cybersecurity incident which may involve Danone either as a source or a target of a cyber attack or cyber threat.

Constituency

Our constituency is composed of the whole Danone company including all its brands.

Sponsorship and affiliation

CERT Danone is the Computer Security Incident Response team for Danone. Its funding is provided by Danone SA.

Authority

CERT Danone operates under the authority of the management of the Danone company.

04 Policies

Types of incidents and levels of support

CERT Danone addresses all types of security incidents which occur, or threaten to occur, within its constituency.

The level of support depends on the type and severity of the security incident and our availability at the time of the incident.

Cooperation, interaction and disclosure of information

CERT Danone regards as very important operational cooperation and information sharing in the course of incident prevention and resolution. CERT Danone can collaborate with other CSIRTs and CERTs as well as with other affected third parties to the extent they are involved in the incident or incident response process. Information received by CERT Danone may be shared with other teams within Danone, as well as to cybersecurity service providers, on a need-to-know basis.

No incident or vulnerability related information will be provided to other persons.

Communication and authentication

All emails sent to the Cert Danone should preferably be signed using PGP.

All emails containing confidential information should be encrypted and signed using PGP.

CERT Danone supports the Information Sharing Traffic Light Protocol (TLP).

05 Services

Incident response

The CERT Danone provides the following services :

- Incident analysis
- Incident response support
- Incident response coordination
- Vulnerability response coordination

Proactive activities

The CERT Danone performs the following activities:

- Intrusion detection services

- Vulnerability scans services
- Technical auditing services

06 Incident reporting forms

CERT Danone does not have a generic incident reporting form, however a data breach reporting form is available on demand. Please report any security incident via encrypted email to cert@danone.com.

This email should contain the following information:

- Incident date and time (please specify the time zone)
- Contact details
- Context and short summary of the incident
- Estimated impact
- Source Ips, ports, and protocols (if relevant)
- Destination Ips, ports, and protocols (if relevant)
- Full email including headers (if relevant)
- And any other relevant information

07 Disclaimer

This document is provided as is without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

If you notice any mistakes within this document, please send a message to cert@danone.com.