ATEA

RFC 2350

Version 1.0 Oct 13 2025

TLP:CLEAR

Table of Contents

1 Document information

This document contains a description of AteaIRT in accordance with RFC 2350. It provides basic information about AteaIRT, its channel of communication, and its roles and responsibilities

Date of last update

Version 1.0 – 13 Oct 2025

Distribution list for notifications

N/A.

Location where this document may be found

The current version of this document can be found at:

https://www.atea.com/it-security/incident-response-team/

Document identification

Title	RFC2350
Version	1.0
Document date	13 Oct 2025
Expiration	This document is valid until superseded by a later version

2 Contact information

Name of the team

Full name	Atea Incident Response Team
Short name	AteaIRT

Address

Atea AS
Karvesvingen 5, 0579, Oslo, Norway

Time zone

CET/CEST

Telephone number

+47 22 09 52 00

Electronic email address

For notifications, incident reporting and operational matters, please contact us at:

irt@atea.com

This is an email alias that relays mail to the human(s) on duty for AteaIRT.

In case of an emergency, please contact us by phone at +47 22 09 52 00 and ask for Incident Response Team.

AteaIRT operates on a 24/7/365 basis.

Other telecommunications

N/A.

Public keys and encryption information

Atea IRT use PGP

Fingerprint	FDA88C5652E923DE62C6554EAA3A553171BB4809
Location	https://www.atea.com/media/ey4kfvcs/atea_irt_pgp_asc.txt

Team members

This information is not publicly available. Atea IRT will provide a list of team-members upon request.

Other information

N/A

3 Charter

Mission statement

Atea IRT is a virtual team within Atea ASA.

The main purpose is to provide an Incident response as a service for any kind of organization requesting an external provider for their Cyber security Incident response team. Atea IRT is not limited to responding to cyber security incidents. The services should be proactive and aim to get organizations resilient and ready to face the current threat landscape.

Constituency

Atea IRTs constituency is external to Atea. This means assisting new and existing Atea-customers seeking cyber security incidents-handling expertise or escalating to- and engaging an IR function as part of an Atea Managed Service (e.g. SOC/MDR).

Atea itself is on the client list of Atea IRT. Therefore, Atea IRT delivers IR services to all the Atea companies and is part of the incident response process and capacity for Atea.

Sponsorship and/or affiliation

Atea IRT is fully sponsored, operated and supported by Atea AS.

AteaIRT is approved by the Norwegian NCSC as a qualified incident response vendor, see https://nsm.no/fagomrader/sikkerhetsstyring/leverandorforhold/kvalitetsordning-for-leverandorer-som-handterer-ikt-hendelser for details.

4 Policies

Types of incidents and level of support

Incidents are handled according to their priority, which is determined by the contract terms, incident category, and the agreed service level. If the affected constituent does not have a Service Level Agreement (Incident Response Retainer), the response will be prioritized based on incident severity, organizational impact, and resource availability to maintain compliance with existing service commitments.

Co-operation, interaction and disclosure of information

Sensitive information encompasses sensitive personal data, as defined by relevant privacy legislation, and business confidential information. All information related to security incidents is considered sensitive, unless all concerned parties specifically state otherwise.

Atea IRT supports the Traffic Light Protocol v2.0, and all labelled information will be handled in accordance with https://www.first.org/tlp

5 Services

Service Area: **Information Security Event Management**

- Event Analysis

Service Area: **Information Security Incident Management**

- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination

Service Area: **Situational Awareness**

- Data Acquisition
- Analysis and Synthesis
- Communication

Service Area: **Knowledge Transfer**

- Awareness Building
- Exercises
- Technical and Policy Advisory

6 Incident reporting

Whenever possible, incidents should be reported by email at ateairt@atea.no, preferably encrypted with AteaIRT PGP public key. For emergency contact AteaIRT by phone.

When you contact us, please provide the following information:

- Contact details and organisational information – name of person, organisation name and address, email address, telephone number
- Short summary of the incident / emergency / crisis and type of event.
- The event / incident source (e.g. which system produced an alert).
- Affected system(s).
- Estimated impact (e.g. loss of communications)
- Additional information such as details of the observations that led to the discovery of the incident – scanning results (if any), and extract from the log showing the problem/alarm, etc.

7 Disclaimer

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