

# Alintrust

## RFC 2350

# Alintrust

## 1. DOCUMENT INFORMATION

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

### 1.1 DATE OF LAST UPDATE

February 19th, 2026

### 1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

N/A

### 1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

On the company web page <https://www.alintrust.cz>, About us, section "Official Credentials"

## 2. CONTACT INFORMATION

### 2.1 NAME OF THE TEAM

Alintrust SOC

### 2.2 ADDRESS

Alintrust s.r.o.

Vyskočilova 1481/4, Nusle, 140 00 Prague 4, Czech Republic

### 2.3 TIME ZONE

CET/CEST

### 2.4 TELEPHONE NUMBER

+420 296 182 014

## 2.5 ELECTRONIC EMAIL ADDRESS

csirt@alintrust.cz

## 2.6 OTHER TELECOMMUNICATION

N/A

## 2.7 PUBLIC KEYS AND ENCRYPTION INFORMATION

We do not offer a public key for encryption, please contact us for other ways of secure communication and information sharing. In case of an incident, secure encrypted communication will be established.

## 2.8 TEAM MEMBERS

The team of Alintrust SOC includes around 10 staff members.

## 2.9 OTHER INFORMATION

N/A

## 3. CHARTER

### 3.1 MISSION STATEMENT

The mission of our SOC is to protect the organization's information systems and critical assets by providing proactive and reactive cybersecurity services. We aim to monitor, detect, respond to, and recover from security incidents with the highest level of professionalism and efficiency. Our team is committed to enhancing organizational resilience through continuous improvement, collaboration, and knowledge-sharing to mitigate cyber threats and ensure the availability, confidentiality, and integrity of our systems.

### 3.2 CONSTITUENCY

The SOC provides cybersecurity monitoring, detection, and incident response services to multiple customers across diverse industries

under a Security Operations Center as a Service (SOCaaS) model. The scope of our responsibility varies based on individual customer agreements and includes monitoring and protecting systems, networks, and applications specified in each service contract. Our team serves as a trusted partner to enhance the security posture of our customers by safeguarding their critical assets against cyber threats, ensuring confidentiality, integrity, and availability within the agreed-upon boundaries. The SOC does not take responsibility for systems or assets outside the contracted scope of work.

### 3.3 SPONSORSHIP AND/OR AFFILIATION

Alintrust SOC is a department of Alintrust s.r.o.

### 3.4 AUTHORITY

In case of security incidents, Alintrust SOC cooperates with representatives of its constituency.

Alintrust SOC is in charge of the service provided to the customer.

## 4. POLICIES

### 4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

Alintrust SOC addresses all kinds of security incidents which occur, or threaten to occur, within its constituency.

Incidents are prioritized according to contract status, type and therefore the service level agreed with the affected constituent.

### 4.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

Alintrust SOC cooperates with the relevant public authorities and regulatory bodies. Alintrust SOC cooperates at national level with other entities.

Alintrust SOC follows industry best practices, including anonymization and data minimization when sharing data with public authorities or other teams.

## 4.3 COMMUNICATION AND AUTHENTICATION

For normal communication not containing sensitive information Alintrust SOC might use conventional methods like unencrypted e-mail. For secure communication telephone or end-to-end encrypted messaging will be used.

## 5. SERVICES

Alintrust SOC can be considered as a Security Operations Center (SOC).

### 5.1 SECURITY INFORMATION EVENT MANAGEMENT

#### 5.1.1 MONITORING AND DETECTION

- Log and sensor management
- Detection use case management
- Contextual data management

#### 5.1.2 EVENT ANALYSIS AND EVALUATION AND ORCHESTRATION

- Correlation
- Orchestration and automation
- Qualification

### 5.2 SECURITY INCIDENT MANAGEMENT

Alintrust SOC coordinates incident prevention, handling and response within its constituency.

#### 5.2.1 INCIDENT TRIAGE

- Determine whether an event is incident or not
- Determine whether severity of incident is relevant
- Assessing and prioritizing the incident
- Determine the involved applications and customers

## 5.2.2 INCIDENT COORDINATION

- Contact involved customers to investigate and take appropriate mitigation steps
- Notify other customers if appropriate
- Facilitating contact to other parties which can help resolve the incident

## 5.2.3 INCIDENT RESOLUTION

Advise customer security teams on appropriate actions

- Follow up on the progress of the concerned customer security teams
- Request information
- Report back

Alintrust SOC collects statistics about incidents within its constituency.

## 5.3 VULNERABILITY MANAGEMENT

- VULNERABILITY RESPONSE
- Vulnerability detection/scanning
- Management of vulnerability tools

## 5.4 EMAIL ABUSE

- Management and evaluation of reported emails
- Cooperation on blocking malicious domain
- Recommendation on email filtering

## 5.5 PROACTIVE ACTIVITIES

Alintrust SOC collects statistics about incidents within its constituency.

- Enhance security awareness within the constituency
- Monitor emerging technology trends
- Share relevant knowledge with the constituency

## 6. INCIDENT REPORTING

There are no local forms available yet. Please use our basic rules for sending incident reports using e-mail:

- A report must contain:
  - first name and last name of the reporter
  - telephone number
  - e-mail address
  - name of reporting organization
  - IP address and type of incident
  - approximate time when the incident started
  - time, when the incident was detected
  - relevant description of the problem

## 7. DISCLAIMER

While every precaution will be taken in the preparation of information, notifications and alerts, Alintrust SOC assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within. This document is subject to change without prior notice, and Alintrust SOC reserves the right to update its policies and procedures as necessary.