Alphaserver

ALPHS-SOC RFC 2350

Alphaserver Security Operations Center

Company:

Alphaserver s.r.o

Date: 03. 02. 2026

Obsah

1 About this document

This document contains a description of Security Operation Center 365 CSIRT according to RFC 2350. It provides basic information about the SOC365 CSIRT, the ways it can be contacted and describes the services offered.

1.1 Date of Last Update

This is version 1.0 of 03. 02. 2026.

1.2 Distribution List for Notifications

No distribution list for notifications exists. All specific inquiries or comments should be sent to the following address csirt@alphaserver.cz.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the Alphaserver s.r.o. website; its URL is http://alphaserver.cz/wp-content/uploads/ALPHS-SOC_RFC2350.pdf

2 Contact Information

2.1 Name of the Team

Alphaserver Security Operations Center CSIRT

2.2 Address

Mlynska 425/70

602 00 Brno-Trnita

Czech Republic

2.3 Time Zone

CET, Central European Time (UTC +1, from the last Sunday in October to the last Sunday in March)

CEST, Central European Summer Time (UTC +2, from the last Sunday in March to the last Sunday in October)

2.4 Telephone Number

+420 770 659 565

2.5 Facsimile Number

None available.

2.6 Electronic Mail Address

For communication, please use the address csirt@alphaserver.cz

2.7 Public Keys and Other Encryption Information

For communication, please use this key:

- Type: RSA/4096 Expires: 2028-04-25
- Fpr: 100B0817FFDC484DF20FA69682BD7A2322454F34
- UID: CSIRT Alphaserver <csirt@alphaserver.cz>

2.8 Team Members

Information about individual ALPHS-SOC CSIRT team members is not publicly disclosed on the website. For communication, please use the official contact e-mail address.

Team members will identify themselves to the reporting party using their full name in official incident-related communications.

2.9 Other information

General information about ALPHS-SOC can be found on the website https://alphaserver.cz

2.10 Points of Customer Contact

The preferred method of contacting the ALPHS-SOC is via e-mail.
If e-mail is not available (or not advisable for security reasons), the emergency telephone number may be used.

3 Charter

3.1 Mission Statement

Our goal is to proactively identify and assess cybersecurity threats, support timely incident detection and response, coordinate incident handling activities, and contribute to the effective prevention of cybersecurity incidents through monitoring, analysis and information sharing.

3.2 Constituency

Our constituency consists of public and private sector organisations, including research and educational institutions, government and military bodies, commercial customers, and service provider customer bases operating within the Czech Republic.

4 Policies

4.1 Types of Incidents and Level of Support

ALPHS-SOC CSIRT supports cybersecurity incident handling within its constituency based on contractual or cooperative agreements. Incidents are prioritised based on their potential impact on confidentiality, integrity and availability, with particular focus on incidents affecting critical services, shared infrastructures and systems of higher importance. The team provides analysis, coordination and advisory support, while operational remediation is performed only where contractually agreed.

4.2 Co-operation, Interaction and Disclosure of Information

ALPHS-SOC CSIRT shares information in accordance with legal, contractual and confidentiality requirements, while supporting responsible cooperation within the cybersecurity community. Incident-related information is disclosed on a need-to-know basis, subject to information classification and consent of the information owner. Cooperation with customers, trusted partners and other CSIRTs is

performed only after appropriate verification and without public disclosure of confidential or customer-identifiable information.

4.3 Communication and Authentication

ALPHS-SOC CSIRT uses communication channels appropriate to the sensitivity of the information being exchanged. Unencrypted e-mail may be used for low-sensitivity information, while sensitive or confidential information is transmitted only using encrypted communication, such as PGP/GPG. Where required, the identity and trustworthiness of communication partners are verified before information is relied upon or disclosed.

5 Services

5.1 Incident Response

ALPHS-SOC CSIRT supports customers and designated administrators in incident handling by providing analysis, coordination and advisory support. Operational remediation is performed only where contractually agreed.

5.1.1 IncidentTriage

ALPHS-SOC CSIRT performs initial incident triage to assess reported or detected events and determine their relevance, severity and priority. During triage, incidents are classified, correlated with available context and either accepted for further analysis, escalated, or closed as false positives or known issues.
Triage activities are performed in accordance with established procedures and contractual requirements.

5.1.2 Incident Coordination

ALPHS-SOC CSIRT coordinates incident handling activities among involved parties, including customers, designated administrators, service providers and other relevant stakeholders. Coordination includes information sharing, task alignment, escalation management and support for decision-making throughout the incident lifecycle. Incident coordination is performed in accordance with established procedures, contractual agreements and information handling policies.

5.1.3 Incident Resolution

ALPHS-SOC CSIRT supports the resolution of cybersecurity incidents by providing analysis, recommendations and coordination until the incident is formally closed.
Incident resolution includes validation of implemented measures, confirmation of incident containment or mitigation, and documentation of outcomes in the incident management system.
Final closure of incidents is performed in accordance with established procedures and contractual agreements

5.2 Proactive Activities

ALPHS-SOC CSIRT performs proactive activities aimed at improving the security posture and resilience of supported environments.

These activities include continuous security monitoring, vulnerability analysis, threat analysis, security assessments, information sharing, and awareness and training activities.

Proactive activities are provided in accordance with contractual agreements and are focused on early detection, prevention and mitigation of potential cybersecurity threats.

6 Incident Reporting Forms

ALPHS-SOC CSIRT accepts incident reports through established communication channels, including e-mail and a dedicated ticketing system.

There is no single mandatory reporting template; however, all incidents are recorded and handled through structured tickets containing predefined fields to ensure consistent triage, analysis and tracking.

The ticketing system supports structured communication, documentation and status tracking throughout the entire incident lifecycle.

7 Disclaimers

While ALPHS-SOC CSIRT takes reasonable care in the preparation of information, notifications and alerts, it does not assume responsibility for errors, omissions or damages resulting from the use of such information. No warranties are given with respect to the accuracy or completeness of the information, unless explicitly agreed in writing.