1. DOCUMENT INFORMATION

1.1. ABOUT THIS DOCUMENT

This document contains a description of Computer Security Incident Response Team of ARIA S.p.A. Azienda Regionale per l'Innovazione e gli Acquisti, which will be referred as CSOC-ARIA, in according to RFC 2350. It provides basic information about the CSOC-ARIA team, its channels of communication, its roles, and responsibilities.

1.2. DATE OF LAST UPDATE

Version 1.0, updated on 2023/09/04.

1.3. LOCATION WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available on CSOC-ARIA website.

Its URL is https://www.csirt.ariaspa.it/wps/portal/site/computer-security-incident-response-team/contatta-il-csirt

1.4. AUTHENTICATING THIS DOCUMENT

This document has been signed with the PGP key of CSOC-ARIA.

The public PGP key is available in CSOC-ARIA website.

1.5. DOCUMENT IDENTIFICATION

Title: RFC 2350 – CSOC-ARIA

Version: 1.0.

Document Date: 2023/09/04

Expiration: this document is valid until it is replaced by a later version.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full Name: Computer Security Incident Response Team - Azienda Regionale per l'Innovazione e gli Acquisti

Short Name: CSOC-ARIA

2.2. ADDRESS

Postal Address: Computer Security Incident Response Team c/o ARIA S.p.A.

Via Torquato Taramelli, 26

20124 – Milano (Italia)

2.3. TIME ZONE

Central European (GMT+0100 and GMT+0200 from the last Sunday of March to the last Sunday of October).

2.4. TELEPHONE NUMBER

Tel: (H24/7 365 day) +39 0239331112.

2.5. ELECTRONIC MAIL ADDRESS

CSOC-ARIA can be reached via cybersoc@ariaspa.it. All members of CSOC-ARIA Team can read messages sent to this address.

2.6. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

To guarantee the security of communications the PGP technology is supported. CSOC-ARIA public PGP key for cybersoc@ariaspa.it is available on the public PGP key in CSOC-ARIA website.

The key shall be used whenever information must be sent to CSOC-ARIA in a secure manner.

2.7. TEAM MEMBERS

CSOC-ARIA's Team Leader is the CSOC Manager. The team consist of Incident Management Team Leader, Incident Handlers, Threat Intelligence Team Leader, Threat Analysts, Laboratory Team Leader Specialist and Laboratory Specialists.

2.8. OTHER INFORMATION

General information about the CSOC-ARIA can be found at CSOC-ARIA website: https://www.csirt.ariaspa.it/

2.9. POINTS OF CUSTOMER CONTACT

The preferred method for contacting CSOC-ARIA is by mail: cybersoc@ariaspa.it.

The mailbox is checked 24h/7days.

The use of PGP is required to send confidential or sensitive information.

If is not possible to contact CSOC-ARIA via e-mail for security reasons, the contact may take place via telephone.

3. CHARTER

3.1. MISSION STATEMENT

The CSOC-ARIA, as CSIRT of Regione Lombardia, has the mission to support and protect all employees and assets of Regione Lombardia, the local government organizations, public operators in Lombardy and institutions from potentially critical cyber threats having concrete possibility to compromise Regione Lombardia's operational capability or to pose a serious threat to information security.

3.2. CONSTITUENCY

The constituency of CSOC-ARIA includes all employees and assets of Regione Lombardia, the local government organizations, public operators in Lombardy and institutions using the services provided by ARIA S.p.A., in its role of in-house company of Regione Lombardia.

3.3. SPONSORSHIP AND/OR AFFILIATION

CSOC-ARIA maintains contacts with various national and international CERT and CSIRT teams, with CSIRT Italia and local central body for the safety and regularity of telecommunications services.

3.4. AUTHORITY

The establishment of the CSOC-ARIA was mandated on the 01 January 2018.

4. POLICIES

4.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

CSOC-ARIA manage and address unknown type and critical information security incident which occur or threaten to occur in its constituency. The level of support given by CSOC-ARIA will vary depending on the severity of the incident, the related ARIA S.p.A ICT assets impacted and the CSOC-ARIA resources at the time.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

CSOC-ARIA highly considers the importance of operational coordination and information sharing among CERTs, CSIRTs, SOCs and similar bodies, and also with other organizations, which may aid to deliver its services or which provide benefits to CSOC-ARIA.

CSOC-ARIA also recognizes and supports the ISTLP (Information Sharing Traffic Light Protocol).

4.3. COMMUNICATION AND AUTHENTICATION

CSOC-ARIA protects sensitive information in accordance with relevant local regulations and policies. In particular, CSOC-ARIA respects the sensitivity markings allocated by originators of information communicated to CSOC-ARIA ("originator control"). Communication security (which includes both encryption and authentication) is achieved using PGP primarily or any other agreed means, depending on the sensitivity level and context.

5. SERVICES

5.1. INCIDENT RESPONSE

CSOC-ARIA will help system administrators of nodes belonging to its constituency in handling computer security incidents to the extent possible depending on its resources.

CSOC-ARIA will provide assistance or advice with respect to the following aspects of incident management:

- investigating the nature and extent of the incident;
- determining the initial cause (e.g., vulnerability exploited);
- keeping contacts with other sites involved;
- reporting to other CSOCs;
- helping in removing the vulnerability.

5.2. PROACTIVE ACTIVITIES

CSOC-ARIA provides to its consituency the following proactive services to the extent possible depending on its resources:

- announcements
- configuration and maintenance of security tools, applications and infrastructures
- intrusion detection services
- security audits or assessments
- security-related information dissemination
- technology watch
- trend and neighborhood watch

5.3. REACTIVE ACTIVITES

CSOC-ARIA provides to its consituency the following reactive services to the extent possible depending on its resources:

- alerts and warnings
- artifact analysis
- artifact response coordination
- forensic analysis
- incident analysis
- incident response support

- incident response coordination
- vulnerability analysis
- vulnerability response coordination

6. INCIDENT REPORTING FORM

CSOC-ARIA does not provide any Incident Response Form on its public Web site. Incident reports must be sent via encrypted e-mail to cybersoc@ariaspa.it

When reporting incidents please provide as much information as possible and specify the level of confidentiality of information sent (whether public domain or not). TLP protocol is accepted and enforced. In case of absence of this information, CSOC-ARIA will assume that the information received is in the public domain and may act accordingly.

7. DISCLAIMERS

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