RFC 2350

CSIRT-AD

1. DOCUMENT INFORMATION

1.1. ABOUT THIS DOCUMENT

This document contains a description of ANDORRA CSIRT, which will referred, in according to RFC 2350. It provides basic information about the CSIRT team, its channels of communication, its roles and responsibilities.

1.2. DATE OF LAST UPDATE

Version 1.0, updated on 2022/04/07.

1.3. LOCATION WHERE THIS DOCUMENT MAY BE FOUND

The current and latest version of this document is available on CSIRT-AD website.
Its URL is https://www.csirt.ad.

1.4. AUTHENTICATING THIS DOCUMENT

This document has been signed with the PGP key of CSIRT-AD.
The public PGP key is available in CSIRT-AD website.

1.5. DOCUMENT IDENTIFICATION

Title: RFC 2350 – CSIRT-AD
Version: 1.0.
Document Date: 2022/04/07
Expiration: this document is valid until it is replaced by a later version.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full Name: CSIRT-AD
Short Name: CSIRT

2.2. ADDRESS

Postal Address: CSIRT-AD. Ctra Comella s/n, AD500, Andorra la Vella

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) +376 655 001.

2.5. ELECTRONIC MAIL ADDRESS

CSIRT-AD can be reached via csirt.anc@govern.ad . All members of CSIRT-AD Team can read messages sent to this address.

2.6. PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

In order to guarantee the security of communications the PGP technology is supported. CSIRT-AD public PGP key for csirt.anc@govern.ad is available on the public PGP key servers and in AND-AD website.

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

2.7. STAFF MEMBERS

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

3. OTHER INFORMATION

General information about the CSIRT-AD can be found at CSIRT website:
https://www.anc.ad

3.1. POINT OF COSTUMER CONTACT

The preferred method for contacting CSIRT-AD is by mail: csirt.and@govern.ad.

The mailbox is checked 24h/7days.

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

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

3.2. CHARTER

3.2.1. MISSION STATEMENT

The CSIRT-AD mission is to support and protect Andorra cyberspace from potentially critical cyber threats having concrete possibility to compromise company operational capability or to pose a serious threat to information security.

3.2.2. CONSTITUENCY

The constituency of CSIRT-AD refers to all the legal entities in Andorra.

3.2.3. SPONSORSHIP AND/OR AFFILIATION

CSIRT-AD maintains contacts with several national and international CSIRT teams

3.2.4. AUTHORITY

The establishment of the CSIRT was mandated via Company directive on 2021/10/20

3.3. POLICIES

3.3.1. TYPE OF INCIDENT AND LEVEL OF SUPPORT

CSIRT-AD 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 CSIRT-AD will vary depending on the severity of the incident

3.3.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

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

3.3.3. COMMUNICATION AND AUTHENTICATION

CSIRT-AD protects sensitive information in accordance with relevant local regulations and policies. In particular, CSIRT-AD respects the sensitivity markings allocated by originators of information communicated. 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.

4. SERVICE

4.1. INCIDENT MANAGEMENT

The CSIRT-AD performs incident handling, response on-site, support and coordination for its constituency. The incident management services as developed by CSIRT-AD covers all “5 steps”:

- Preparedness and prevention
- Detection
- Analysis
- Response
- Recovery

4.2. THREAT INTELLIGENCE

The CSIRT-AD performs the threat intelligence services in order to improve prevention, detection, identification and information security incidents response capabilities.

5. INCIDENT REPORTING FORM

CSIRT-AD provide an incident reporting form in a public web page. The form contains the different fields to report the incident.

6. DISCLAIMERS

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