1 Information about this document

1.1 Last update date

Version 1.0 published on 2023/09/16.

1.2 Distribution lists for notifications

There is no distribution channel to notify changes on this document.

1.3 Access to this document

The updated version of this document and its Portuguese version can be found at https://www.ipv.pt/csirt-ipv/#documentos.

1.4 Authenticity of this document

This version and a portuguese version of CSIRT.IPV's service description are signed with a PGP key which can be found on https://www.ipv.pt/csirt-ipv/#documentos.

2 Contact information

2.1 Team Name

CSIRT.IPV

2.2 Postal Address

Avenida Coronel José Maria Vale de Andrade
Campus Politécnico
3504-510 Viseu
Portugal

2.3 Time zone

Portugal/WEST (GMT+0, GMT+1 during summertime)

2.4 Phone Number

+351 232 480 700 (working hours – 09h00-12:30 e 14:00-17h30).

2.5 Fax

Non existent.

2.6 E-mail

csirt@sc.ipv.pt

2.7 Other Types of Telecommunications

Non existent.

2.8 Public Keys and Encryption Information

User ID: CSIRT.IPV csirt@sc.ipv.pt
Key ID: 0x844C654E Key type: RSA
Key size: 4096 Expires: Never
Fingerprint: 2B1D72D5B2F9E1FFEE8F71FE920C3985844C654E
Public key can be found at https://www.ipv.pt/csirt-ipv/#documentos.

2.9 Team Members

Coordination: Filipe Caldeira
Members: João Branco
Pedro Carvalho
Luís Almeida
Carlos Barros
Legal advice: Paula Bettencourt

2.10 Further Information

Further Information about CSIRT.IPV can be found at https://www.ipv.pt/csirt-ipv/.

2.11 Types of contact for users

CSIRT.IPV has the following types of contact (in order of preference):
Email: csirt@sc.ipv.pt
Phone number: +351 232 480 700

3 Charter

3.1 Mission Statement

CSIRT.IPV's mission is to promote a culture of security in IT resources within the academic community of the Polytechnic Institute of Viseu, using awareness raising, counseling and responding to IT security incidents detected internally or reported by security incidents response teams from academic and national networks.

3.2 Constituency

CSIRT.IPV responds to computer security incidents in the context of the Polytechnic Institute of Viseu community. The ranges of IP addresses covered by CSIRT.IPV are:

IPV4: 193.137.7.0/24
193.137.141.0/24
194.210.123.0/24
IPV6: 2001:690:20C0::/48

3.3 Affiliation

CSIRT.IPV is a center integrated into the IT Services of the Polytechnic Institute of Viseu.

3.4 Authority

CSIRT.IPV has the authority to respond to Incidents that occur within IPV, as well as to respond on behalf of the organization in Incident response processes in collaboration with external entities.

4 Policies

4.1 Incident types and support level

CSIRT.IPV responds to incidents in the areas of computer security, namely intrusion or intrusion attempts, malicious code, availability, information collection, information security, fraud, abusive content and vulnerabilities.

4.2 Cooperation, interaction and privacy policy

CSIRT.IPV's privacy and data protection policy predicts that sensitive information may be passed on to third parties, solely and exclusively if necessary and with the express prior authorization of the individual or entity to whom that information concerns.

4.3 Communication and authentication

From the communication means made available by CSIRT.IPV, non-ciphered e-mail and phone are considered to be sufficient to non-sensitive information transmission. In order to transmit sensitive information, PGP usage is mandatory.

5 Services

5.1 Handling of security incidentes

CSIRT.IPV plans to support system administrators in managing incidents' technical and organizational aspects. In particular, we can provide assistance and advice with the following aspects of incident management:

5.1.1 Incident Triage

- Determine when an incident is authentic.
- Assess and prioritize an incident.

5.1.2 Incident Coordination

- Determine the organizations involved.
- Contact the organizations involved to investigate the incident and take appropriate action.

- Facilitate contact with other parties who can help resolve the incident.
- Send reports to other CERTs.
- We see ourselves as an information hub that knows the institution and can forward incidents to help and facilitate the resolution of IT security incidents.

5.1.3 Incident resolution

- Advising local systems administration teams on appropriate actions to take.
- Monitor the progress of systems administration teams regarding security issues.
- Request reports.
- Respond to requests.

CSIRT.IPV will also collect statistics on incidents in the context of its operation.

5.2 Proactive activities

CSIRT.IPV coordinates and maintains the following services to expand its capabilities:

- Production of alerts and dissemination of security-related information.
- Monitor infrastructure, applications and systems from the perspective of IT security vulnerabilities.
- Promote security audits or assessments.
- Define, implement and guarantee the execution of technical standards and procedures in their areas of competence.

6 Incident report forms

There are no forms available for this purpose.

7 Liability Safeguard

Although all precautions are taken in preparing the information disclosed either on the Internet portal or through distribution lists, CSIRT.IPV assumes no responsibility for errors or omissions, or for damages resulting from the use of this information.