GovCERT Austria

GovCERT Austria RFC 2350

Version: 1.0
Date: Monday, March 8, 2021
Author: govcert@bka.gv.at

1. Document information

This document contains a description of GovCERT Austria according to RFC 2350. It provides basic information about the CERT, the ways it can be contacted, and describes its responsibilities and the services offered.

1.1 Date of last update

Monday, 08 March 2021

1.2 Distribution list for notifications

There is no distribution list for notifications as of 2021/03.

1.3 Locations where this document may be found

The current version of this document is available at our website: https://www.govcert.gv.at/.

2. Contact information

2.1 Name of the team

GovCERT Austria
The Computer Emergency Response Team for the Austrian Government

2.2 Address

Federal Chancellery of Austria (Bundeskanzleramt Österreich)
Department I/8 – Cyber Security, GovCERT, NIS Office and ZAS
Ballhausplatz 2
1010 Vienna
Austria

2.3 Time zone

We are located in the central European timezone (CET) which is GMT+0100 (+0200 during day-light saving time).

2.4 Telephone number

+43 1 5056416 930

2.5 Facsimile number

None.

2.6 Other telecommunication

Members of the team are active in various online forums of the international CSIRT community.

2.7 Electronic mail address

Please send incident reports to reports@govcert.gv.at.

Non-incident related mail should be addressed to team@govcert.gv.at.

2.8 Public keys and encryption information

GovCERT Austria uses a master signing key to sign all keys used for operational purposes. This trust anchor is:

```
pub   rsa4096/13F59859835FB520 2019-02-25 [SC] [expires: 2034-02-21]
      B9AA8215E37F19F40C128D4913F59859835FB520
uid         GovCERT Austria master key signing-key-only-no-email@govcert.gv.at
sub   rsa4096/49997F6D04C654C8 2019-02-25 [E] [expires: 2034-02-21]
```

It can be found on our website and most key-servers. Please DO NOT use this key for communications with us.

All official communication by GovCERT Austria will be signed by the current team key:

```
pub   rsa4096/712728E78C5A903E 2019-02-25 [SC] [expires: 2024-02-24]
      5B941FC42C56084F8D69324D712728E78C5A903E
uid           GovCERT Austria (Incidents) reports@govcert.gv.at
uid           GovCERT Austria (General Communications) team@govcert.gv.at
sub   rsa4096/28391275B6869619 2019-02-25 [E] [expires: 2024-02-24]
```

Encrypted communications with GovCERT Austria should use this - and only this - operational key. All keys (including the keys of individual team members) can be found on our https://www.govcert.gv.at/.

Since the team key and the master signing key expire regularly, GovCERT Austria will always sign younger master signing keys with the older master signing keys, as well. The current master signing key always signs the team key.

2.9 Team members

Management, liaison and supervision are provided by Robert Schischka, Technical Manager of nic.at. Clemens Moeslinger, Head of the Department for Cybersecurity at the Federal Chancellery of Austria, is the the Strategic Lead of GovCERT Austria.

2.10 Other information

The Government Computer Emergency Response Team (GovCERT) was established December 2008 within the purview of the Federal Chancellory of Austria and in close cooperation with the Austrian national CSIRT (CERT.at).

The Austrian NIS Act, which went into force in late 2018, provides the current legal foundation for the operation of the GovCERT. More information on the Austrian NIS Act can be found at https://www.nis.gv.at. Documents in English are available.

2.11 Points of customer contact

The preferred method for contacting GovCERT Austria is via e-mail.

For incident reports and related issues, please use reports@govcert.gv.at.

For general inquiries, please send your e-mail to team@govcert.gv.at.

If it is not possible (or advisable due to security reasons) to use e-mail, you can reach us via telephone at +43 1 5056416 930.

For incident reports according to the Austrian NIS Act, please use the form at https://nis.govcert.gv.at/ (for other reports, please use e-mail).

Hours of operation are generally restricted to local regular business hours: Mon-Fri (except public holidays and Dec 24th/31st), 8 a.m. - 6 p.m. CET/CEST.

NIS notification for entities of public administration can trigger a 24x7 response by GovCERT Austria.

3. Charter

3.1 Mission statement

The purpose of GovCERT Austria is to coordinate security efforts and incident response for IT-security problems in the public administration sector of Austria.

3.2 Constituency

The constituency of GovCERT Austria is the public administration of Austria. GovCERT Austria supports the entities of public administration, in handling risks, incidents and security incidents.

GovCERT Austria will first try to coordinate with IT-security teams and more specific CERTs/CSIRTs in the constituency.

Please note that usually no direct support will be given to end users; they are expected to contact their local help desk, system administrator, network administrator, or department head for assistance. GovCERT Austria will support the latter.

Pro-active and educational material are provided for the constituency.

3.3 Sponsorship and/or affiliation

GovCERT Austria is established within the purview of the Federal Chancellor of Austria.

Technical manpower is provided by CERT.at, the accredited national CSIRT according to the Austrian implementation of the EU NIS Directive.

3.4 Authority

The main purpose of GovCERT Austria in incident handling is the coordination of incident response. As such, we can only advise our constituency and have no authority to demand certain actions.

We have authority over AS42685.

4. Policies

4.1 Types of incidents and level of support

The primary role of GovCERT Austria during incidents is information exchange and coordination, and not on-site incident response.

GovCERT Austria is committed to keep its constituency informed of potential vulnerabilities, and, where possible, will inform this community of such vulnerabilities before they are actively exploited.

GovCERT Austria is authorised to address all types of computer security incidents which occur, or threaten to occur, in our constituency (see 3.2) and which require cross-organisational coordination. The level of support given by GovCERT Austria will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and our resources at the time.

4.2 Co-operation, interaction and disclosure of information

GovCERT Austria will cooperate with other organisations in the field of computer security. This cooperation also includes and often requires the exchange of vital information regarding security incidents and vulnerabilities. GovCERT Austria will protect the privacy of reporters, partners and our constituents, and therefore (under normal circumstances) pass on information in an anonymised way only, unless other contractual agreements apply.

GovCERT Austria operates under the restrictions imposed by Austrian law. This involves careful handling of personal data as required by Austrian Data Protection law, but it is also possible that according to Austrian law GovCERT Austria may be forced to disclose information due to a court order.

The Austrian NIS Act provides a legal framework for cooperation and information sharing. GovCERT Austria participates in the "Inner Circle of the Operational Coordination Structure" (ICOCS) and acts as a reporting point for incident reporting under the NIS framework. On one hand, the Austrian NIS Act explicitly allows the sharing of personal data (to GovCERT Austria and from GovCERT Austria to affected parties) for the purpose of reacting to, or preventing incidents. On the other hand, the NIS Act defines what information from the NIS reporting needs be passed by GovCERT to the Austrian Ministry of the Interior respectively to the ICOCS. For details on the Austrian NIS Act and related secondary legislation see https://nis.gv.at/.

GovCERT Austria treats all submitted information as confidential per default, and will only forward it to concerned parties in order to resolve specific incidents when consent is implicit or expressly given.

For example: incoming report "Malware on www.example.com/malware, please get it cleaned up". In this case, we would forward the information only to the concerned parties (domain-holder, hoster/ISP) to help them quickly fix the problem. We will not forward information about incidents to other government authorities or the press without explicit prior permission by the submitting party.

GovCERT Austria is an active participant in various collaboration mechanisms, e.g. the Austrian CERT Verbund (association of CERTs), the Austrian Trust Circle (ATC), the EU CSIRTs Network and TF-CSIRT.

4.3 Communication and authentication

For normal communication not containing sensitive information GovCERT Austria might use conventional methods like unencrypted e-mail. For secure communication PGP-encrypted e-mail or telephone will be used. If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. FIRST, TI, CNW) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. Services

5.1 Incident response

GovCERT Austria will assist IT-security teams in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident triage

- determining whether an incident is authentic
- assessing and prioritizing the incident

5.1.2. Incident coordination

- determine the involved organizations
- contact the involved organizations to investigate the incident and take the appropriate steps
- facilitate contact to other parties which can help resolve the incident
- send reports to other CERTs

We mainly see ourselves as an information hub which knows where to send the right incident reports to in order to help and facilitate the clean-up of IT security incidents.

5.1.3. Incident resolution

- advise local security teams on appropriate actions
- follow up on the progress of the concerned local security teams
- ask for reports
- report back

GovCERT Austria will also collect statistics about incidents within its constituency.

5.2 Proactive activities

GovCERT Austria tries to

- raise security awareness in its constituency
- collect contact information of local security teams
- publish announcements concerning serious security threats
- observe current trends in technology
- distribute relevant knowledge to the constituency
- provide fora for community building and information exchange within the constituency

5.3 Service levels

GovCERT Austria will always strive to react to incoming incident reports from humans within one business day. Due to current staffing levels this can not be guaranteed, though. If you have not received feedback on an incident report after two business days, we would kindly ask you to contact us again. Auto-generated reports and data-feeds will be handled as automatically as possible.

6. Incident reporting forms

For reports within the NIS framework, please use the portal at https://nis.govcert.gv.at/.

There are no forms available for informal reports to GovCERT Austria.

7. Disclaimers

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