INFORMATIE
BEVEILIGINGS
DIENST

RFC-2350

INFORMATIE
BEVEILIGINGS
DIENST

Version management

Version	Changes	Date
1.2		Juli 2014
1.3	Textual changes such as new corporate name and URL's	Juni 2018
1.4	Phone number change	Januari 2022

About the IBD

The Information Security Service for municipalities (IBD) is the CERT of all Dutch municipalities. The IBD is the linking pin between municipalities and the national CSIRT, the National Cyber Security Center (NCSC). The IBD's main goal is to increase resilience of Dutch municipalities in the field of information security.

INFORMATIE
BEVEILIGINGS
DIENST

IBD CERT profile

1. About this document

The purpose of this document is to express the general Internet community's expectations of the Informatiebeveiligingsdienst voor gemeenten (Municipalities CERT).

Established according to RFC-2350, version 1.01, published 01-03-1997

1.1. Date of Last Update

This is version 1.4, dated January 18, 2022.

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3
E-mail notification of updates are sent to:

- All IBD Team members
- All IBD constituents
- NCSC (cert@ncsc.nl)

Any questions about updates please address to the info@IBDgemeenten.nl e-mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on
https://www.informatiebeveiligingsdienst.nl/product/rfc-2350/

2. Contact Information

2.1. Name of the Team

Full name: Informatiebeveiligingsdienst voor gemeenten
Short name: IBD
IBD is the CERT or CSIRT team for all municipalities in The Netherlands.

2.2. Address

VNG Realisatie
Informatiebeveiligingsdienst (IBD)

Visitors address
Nassaulaan 12
2514 JS The Hague
The Netherlands

Postal address
PO-Box 30435
2500 GK The Hague
The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Telephone Number

+31 70 204 55 11

2.5. Facsimile Number

IBD CERT can NOT be contacted by Facsimile.

2.6. Other Telecommunication

Not available.

2.7. Electronic Mail Address

incident@IBDgemeenten.nl

This address can be used to report all security incidents to which relate to the IBD constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information
Only PGP is currently supported for secure communication.

The IBD public PGP key is available on the public keyservers.
Its key-id is 0x7A413714 and its fingerprint is
9F4A C182 544E A3E2 04BA D5F8 FD76 AADE 7A41 3714

2.9. Team Members
No information is provided about the IBD team members in public.

2.10. Other Information
General information about the IBD, as well as links to various recommended security resources, can be found at the IBD webpages https://www.informatiebeveiligingsdienst.nl

2.11. Points of Customer Contact
The preferred method for contacting the IBD is via e-mail at info@IBDgemeenten.nl e-mail address.
Regular response hours: Monday-Friday, 09:00-17:00 (except public holidays in The Netherlands).

3. Charter

3.1. Mission Statement
The mission of the IBD is to co-ordinate the resolution of IT related security incidents related to their constituency (see 3.2), and to help prevent such incidents from occurring.

3.2. Constituency
The constituency for the IBD is all municipalities in The Netherlands.
This constituency consists of:
- Municipalities

3.3. Sponsorship and/or Affiliation
The IBD is part of VNG Realisatie.

3.4. Authority
The IBD coordinates IT related security incidents on behalf of the municipalities in the Netherlands and has no authority reaching further than that. The team is however expected to make operational recommendations in the course of their work. Such recommendations can include but are not limited to blocking addresses or networks. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made.

4. Policies

4.1. Types of Incidents and Level of Support
All incidents are considered normal priority unless they are labelled URGENT. The IBD itself is the authority that can set and reset the URGENT label. An incident can be reported to the IBD as URGENT, but it is up to the IBD to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information
ALL incoming information is handled confidentially by the IBD, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.

The IBD supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/processes/standards.html) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

The IBD will use the information you provide to help solve security incidents, as all CERTs do. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymised fashion.

If you object to this default behaviour of the IBD, please make explicit what the IBD can do with the information you provide. The IBD will adhere to your policy, but will also point out to you if that means that the IBD cannot act on the information provided.

The IBD does not report incidents to law enforcement, unless national law requires so. Likewise, the IBD only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that the IBD cooperates in an investigation. When a court order is absent, the IBD will only provide information on a need-to-know base.

4.3. Communication and Authentication
See 2.8 above. Usage of PGP/GnuPG in all cases where sensitive information is involved is highly recommended.
In cases where there is doubt about the authenticity of information or its source, the IBD reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident Response (Detection, Coordination and Resolution)
The IBD is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). The IBD therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency – however the IBD will offer support and advice on request.

5.2. Proactive Activities
The IBD pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking. The IBD is not responsible for implementation.

6. Incident reporting Forms
There are no special forms required to report an incident.

7. Disclaimers
The information in this document is provided for information purposes only. The IBD makes no warranties about the accuracy or completeness of any information contained in this document. The IBD does not accept liability for any damages, losses or personal harm whatsoever, arising out of, or in any way related to, the use of this document.