Federal Office
for Information Security

Technical Guideline BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products

Part 3: Vulnerability Reports and Notifications

Document history

Table 1: Document History

Version	***Date***	***Description***
0.9.0	2024-09-20	Initial Draft
1.0.0	2025-08-20	Version of BSI TR-03183-3 for first publication

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
E-Mail: TR03183@bsi.bund.de
Internet: https://bsi.bund.de/dok/TR-03183-en

Table of Contents

1 Introduction

Vulnerabilities have an impact on security and probably even safety of products, their users, and the environment. However, vulnerabilities cannot be avoided when developing software and hardware. The more complex a system is and the more dependencies it includes, the more frequently vulnerabilities will occur. Moreover, hardly ever all vulnerabilities are discovered before a product is placed on the market, even after intensive testing. Therefore, a vulnerability handling process is necessary before and during the time for each product in use. As such, this process requires at least the creation, release, secure distribution, and installation of updates or the implementation of other mitigation measures for affected products.

Although secure development and operating processes minimise the number of vulnerabilities in products, they do not guarantee that the product does not contain any vulnerability at all. Establishing a responsible and efficient response process for vulnerability reports adhering to the Coordinated Vulnerability Disclosure (CVD) process is therefore of central importance and the first step in reducing the potential harm and risk caused by a vulnerability.

To enable successful CVD processes, manufacturers should react positively to incoming vulnerability reports and should not threaten with legal actions as long as no criminal intention is apparent (see BSI CVD guideline for security researchers[1]). In addition, manufacturers should be prepared for CVD processes, which require holistic internal processes involving the relevant departments, the designation and publication of contact options, the establishment of communication channels, and the actual response to vulnerability reports. Throughout the entire CVD process, manufacturers should communicate proactively with the reporting entity and strive to continuously optimise internal processes.

As every CVD process starts with vulnerability reporting, it is essential to publish the contact options and CVD policies for external communication. A dedicated web page for security information and a **security.txt**[2] in accordance with RFC 9116[3] on the manufacturer's website fulfils this purpose.

In scope of this Technical Guideline by the Federal Office for Information Security (BSI) are only vulnerabilities related to cybersecurity by causing a negative impact on the confidentiality, integrity, availability, authenticity, non-repudiation, or reliability of an impacted component or components upon exploitation.

Furthermore, vulnerabilities can also have an impact in more than one EU Member State. Hence, the European Union Computer Security Incident Response Teams (CSIRTs) network[4] (see Article 12 of the NIS Directive[5] and Article 15 of the NIS2 Directive[6]) was established. One of the network's missions is to improve the exchange of vulnerability information within the EU. Therefore, each Member State designates one of its CSIRTs as its national coordinator for the purposes of coordinated vulnerability disclosure (see Article 12 of the NIS2 Directive). In Germany, the expected designated national CSIRT is the Computer Emergency Response Team for Germany's federal authorities (CERT-Bund)[7]. It is operated by the BSI as the federal cybersecurity authority and the single point of contact for cybersecurity within the federal administration. BSI aims at elevating the level of cybersecurity in administration, businesses, and society. Hence, CERT-Bund and, consequently, the BSI always share reported plausible vulnerability information with the manufacturers in order to help eliminate or mitigate vulnerabilities[8].

[1] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html
[2] https://securitytxt.org/
[3] https://www.rfc-editor.org/rfc/rfc9116
[4] https://csirtsnetwork.eu/#network_members
[5] https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng
[6] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
[7] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html
[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.html

2 Requirements Language

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in BCP 14[9] (RFC 2119[10], RFC 8174[11]) when, and only when, they appear in all capitals, as shown here.

[9] https://www.rfc-editor.org/info/bcp14
[10] https://www.rfc-editor.org/rfc/rfc2119
[11] https://www.rfc-editor.org/rfc/rfc8174

3 Basics

3.1 Terms used

3.1.1 Manufacturer

The Cyber Resilience Act (CRA)[12] defines in Article 3 paragraph 13 'manufacturer' as a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge.

As the CRA is a market access regulation, "manufacturer" is interpreted as combining the roles of "vendor" and "creator".

"Vendor" (German: "Anbieter") describes the role of the entity that provides the product with digital elements. Alternatively, but not necessarily with a commercial background the terms "supplier" (German: "Lieferant") is used.

"Creator" (German: "Ersteller") describes the role of the entity that authored or created the product with digital elements.

As this Technical Guideline specifies technical requirements, it uses a different terminology and interprets "manufacturer" as a combination of the entity that produces tangible goods, such as devices, and the entity that creates or provides intangible goods, such as software and software components, usually described by the term "author". Therefore, this Technical Guideline does not mention the terms "distributor" or "importer", as the roles of these parties are unrelated to the technical requirements stated here. These technical requirements are independent of the role, which is fulfilling them.

3.1.2 Vulnerability

The NIS2 Directive defines in Article 6 paragraph 15 'vulnerability' as a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat.

3.1.3 Valid, validated, verified and actively exploited vulnerability

Every entity can decide, what it considers to be a valid vulnerability according to their vulnerability guideline. This guideline may include requirements from the reporting entity of the vulnerability. Requirements regarding the content of this guideline are found in section 4.4.5 and in the BSI CVD guideline for security researchers[13].

After the manufacturer has confirmed that the vulnerability complies with the requirements in its vulnerability guideline, this vulnerability is a validated vulnerability.

After the manufacturer has assessed a validated vulnerability with regard to its severity and exploitability, this vulnerability is either validated and verified, or validated but unverified.

The CRA defines in Article 3 paragraph 42 'actively exploited vulnerability' as a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner.

[12] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
[13] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html

3.1.4 Vulnerability notification

In this Technical Guideline, a vulnerability notification is a general information about a vulnerability, which usually names the product concerned and contains an initial assessment with a tentative CVSS Base Score but no deeper details of the vulnerability. Commonly, the notifications are sent by the manufacturer to one of the national CSIRTs or to the European Union Agency for Cybersecurity (ENISA)[14] and are non-public.

3.1.5 Security advisory

In this Technical Guideline, a security advisory is also an information about a vulnerability, which usually contains the information of the vulnerability notification including a reviewed CVSS Base Score and more details with the focus on remediation and mitigation of the vulnerability. Commonly, the advisories are sent by the manufacturer to all users of the product and are publicly disclosed. Their recommended distribution is the publication on the manufacture's website applying Common Security Advisory Framework (CSAF)[15].

3.1.6 Vulnerability Report

In this Technical Guideline, a vulnerability report is an information about a vulnerability. It usually contains the information of the vulnerability notification and more details with the focus of identification, exploitation and reproduction, e.g. a proof-of-concept (POC) of the vulnerability. Commonly, the reports are sent by security researchers or national CSIRTs to the manufacturer of the product and are confidential.

3.1.7 Corresponding national CSIRT

To comply with this Technical Guideline, manufacturers MUST select as its corresponding national CSIRT from any of the national CSIRTs designated from their Member State as a coordinator for the purposes of coordinated vulnerability disclosure (see Article 3 paragraph 51 of the CRA in combination with Article 12 of the NIS2 Directive). The corresponding national CSIRT MUST be determined according to Article 14 paragraph 7 of the CRA. Moreover, manufacturers MUST stay at their corresponding national CSIRT during the active handling of every single valid vulnerability except the corresponding national CSIRT transfers the handling. Furthermore, manufactures SHOULD choose the same national CSIRT as corresponding one for the communication about each and every vulnerability.

3.1.8 Anonymous reporting option

In this Technical Guideline, an anonymous reporting option provides a contact option with the manufacturer where the reporting entity can stay anonymous. This SHOULD be a web form on the manufacturer's website. This web form MUST NOT contain any third party components, e.g. advertisements or tracking pixel. While entering data and using this web form, the logging of metadata MUST be minimized. Therefore, the information that SHOULD NOT be logged includes the IP address, the browser or the computer of reporting entity.

[14] https://www.enisa.europa.eu/
[15] https://www.bsi.bund.de/dok/TR-03191-en

4 Cybersecurity requirements for receiving vulnerability reports

In order to establish a process for receiving vulnerability reports that is compliant with this Technical Guideline, at least the following requirements MUST be fulfilled. The implemented measures to fulfil these requirements, all test procedures, and all test results MUST be recorded. For clarification, the requirements in this section are considered as minimal requirements for receiving vulnerability reports. Hence, further statements e.g. in the **security.txt** (see section 4.2), on the web page for incoming vulnerability reports (see section 4.5) or in the CVD policy (see section 4.4), and additional preliminary measures for a CVD process (see section 4.3) are allowed.

4.1 Website of the manufacturer

Security related information about the manufacturer and its products should be easily accessible to external entities. Therefore, the manufacturer MUST make this information easily accessible to the public.

4.1.1 General

a. The manufacturer MUST operate a website to publicly provide at least security related information about itself and its products.
b. This website MUST be fully accessible without any login procedure or other restriction, e.g. behind a paywall.
c. At least all the security related information on this website, e.g. the CVD policy (see section 4.4) and the web page for incoming vulnerability reports (see section 4.5), MUST be in a language which can be easily understood by users and market surveillance authorities.

4.2 Security.txt file in accordance with RFC 9116

To make it easier for the reporting entity to find the right contact for vulnerability reports, a **security.txt** in accordance with RFC 9116 MUST be created and made available on the manufacturer's website. The security requirements for the **security.txt** are based on the recommendations formulated in the BSI's cybersecurity recommendation „Sicherheitskontakte mit Hilfe einer security.txt nach RFC 9116 angeben“[16] and the RFC 9116 itself. Figure 1 shows an example for a **security.txt** according to the requirements in this section.

4.2.1 Localisation of security.txt

a. The manufacturer MUST create a file with the name **security.txt** directly in the path /.well-known/ (e.g. **/.well-known/security.txt**).
b. This file MUST be accessible via HTTPS using at least HTTP 1.1 (according to RFC 7230[17] section 2.7.2) or a higher version.
c. This file MUST be a plain text file with ASCII or UTF-8 encoding. Only the ASCII characters 0x20 to 0x7E MUST be used for non-comments.
d. The manufacturer MUST comply with the respective format specifications of RFC 9116 for all information in this file.

4.2.2 Canonical URI

a. The manufacturer MUST specify the canonical URI of the **security.txt**.
b. This canonical URI MUST be a web URI (according to RFC 7230 section 2.7.2).

[16] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_149.html
[17] https://www.rfc-editor.org/rfc/rfc7230

c. This canonical URI MUST reflect the true location of the authoritative file and MUST be accessible without redirects.
d. This statement SHOULD be introduced with the comment **# Our canonical URI**.

4.2.3 Contact information

a. The manufacturer MUST provide a list of contact options for reporting vulnerabilities.
b. The declaration of the first contact option MUST be the email address of the functional mailbox of manufacturer's Product Security Incident Response Team (PSIRT) (see section 4.3.1) according to RFC 6068[18].
c. The declaration of the second contact option MUST be the email address of the functional mailbox of the manufacturer's CSIRT (see section 4.3.1) according to RFC 6068.
d. The next point of contact MUST be the web URI (according to RFC 7230 section 2.7.2) of the manufacturer's web page for incoming vulnerability reports (see section 4.5) according to RFC 7230 and RFC 3986[19].
e. This listing SHOULD be introduced with the comment **# Our security addresses**.

4.2.4 OpenPGP keys

a. The manufacturer MUST provide the encryption options of the contact list provided in section 4.2.3. Therefore, requirements of section 4.3.2 MUST be applied.
b. This listing SHOULD be introduced with the comment **# Our OpenPGP keys**.

4.2.5 Acknowledgements

a. The manufacturer SHOULD provide the web URI (according to RFC 7230 section 2.7.2) of the acknowledgements for vulnerability reports web page.
b. This listing SHOULD be introduced with the comment **# Our security acknowledgements page**.

4.2.6 Preferred languages

a. The manufacturer MUST specify the preferred languages for incoming vulnerability reports.
b. At least the language tag for English (en) MUST be specified.
c. This listing SHOULD be introduced with the comment **# Our preferred languages**.

4.2.7 CVD policy

a. The manufacturer MUST provide the web URI (according to RFC 7230 section 2.7.2) to the web page of its CVD policy.
b. This SHOULD be introduced with the comment **# Our security policy**.

4.2.8 Security advisories

a. The manufacturer SHOULD provide the web URI (according to RFC 7230 section 2.7.2) of the file **provider-metadata.json** for CSAF documents[20].
b. This statement MUST begin with the tag **CSAF:**
c. This statement SHOULD be introduced with the comment **# Our security advisories**.

[18] https://www.rfc-editor.org/rfc/rfc6068
[19] https://www.rfc-editor.org/rfc/rfc3986
[20] https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html#718-requirement-8-securitytxt

4.2.9 Expiry date

a. The manufacturer MUST specify the expiry date of the **security.txt** according to RFC 3339[21]. The separator "T" MUST be upper cases – other separators MUST NOT be used. The time zone indicator "Z" MUST be upper case as well, if applicable.
b. This value SHOULD be at the maximum of one year in the future.
c. The manufacturer MUST check the information in the **security.txt** at least quarterly and correct or supplement it if necessary.

4.2.10 Digital signature

a. The manufacturer MUST digitally sign its **security.txt** using OpenPGP according to RFC 9580[22].
Note: RFC 9580 obsoletes RFC 4880[23] ("OpenPGP Message Format"), RFC 5581[24] ("The Camellia Cipher in OpenPGP"), and RFC 6637[25] ("Elliptic Curve Cryptography (ECC) in OpenPGP").
b. The manufacturer SHOULD use dedicated OpenPGP keys for signing the **security.txt** according to RFC 9580.
c. The corresponding OpenPGP public key MUST be made available (see section 4.5.3).
d. The manufacturer MUST ensure that the digital signature complies with the requirements of the current BSI TR-03116 Part 4[26] or the current ECCG Agreed Cryptographic Mechanisms[27].
Note: The ECCG Agreed Cryptographic Mechanisms - version 2 is based on the SOG-IS Agreed Cryptographic Mechanisms[28].
e. Unless the validity period of the keys, mentioned in b, is specified otherwise in the current BSI TR-03116 Part 4 or the current ECCG Agreed Cryptographic Mechanisms, it MUST not exceed five years.

4.2.11 Visibility for web crawlers

a. The manufacturer MUST ensure that the **security.txt** can be found automatically (i.e. by web crawlers, e.g. from findsecuritycontacts.com[29] and internet.nl[30]). Hence, firewall rules and DDoS protection rules have to be adapted accordingly, if applicable.

[21] https://www.rfc-editor.org/rfc/rfc3339
[22] https://www.rfc-editor.org/rfc/rfc9580
[23] https://www.rfc-editor.org/rfc/rfc4880
[24] https://www.rfc-editor.org/rfc/rfc5581
[25] https://www.rfc-editor.org/rfc/rfc6637
[26] https://www.bsi.bund.de/dok/TR-03116-en
[27] https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en
[28] https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf
[29] https://findsecuritycontacts.com/
[30] https://internet.nl/

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

# Our canonical URI
Canonical: https://www.example.com/.well-known/security.txt

# Our security addresses
Contact: mailto:psirt@example.com
Contact: mailto:csirt@example.com
Contact: https://www.example.com/security-contact

# Our OpenPGP keys
Encryption: https://www.example.com/openpgp-key_psirt.asc
Encryption: https://www.example.com/openpgp-key_csirt.asc

# Our security acknowledgments page
Acknowledgments: https://www.example.com/hall-of-fame.html

# Our preferred languages
Preferred-Languages: en

# Our security policy
Policy: https://www.example.com/security-policy.html

# Our security advisories
CSAF: https://www.example.com/.well-known/csaf/provider-metadata.json

Expires: 2026-07-01T00:00:00.000Z
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.4

[signature]
-----END PGP SIGNATURE-----
```

*Figure 1: Example of a **security.txt** complying with this Technical Guideline*

4.3 Preliminary measures for a CVD process

For an efficient and effective response process to vulnerability reports, this has to be organised in advance. This includes at least the following.

4.3.1 Roles of responsible cybersecurity contacts

a. The manufacturer MUST create at least two roles of responsible cybersecurity contacts, its PSIRT and its CSIRT.
b. Unless the manufacturer is a microenterprise (see Article 3 paragraph 19 of the CRA), these roles MUST NOT be assigned to a single person, but MUST be divided among several different individuals.
c. The manufacturer MUST assign functional mailboxes to both roles and MUST ensure that the individuals involved in these roles have access to their corresponding functional mailbox.
d. These two roles MUST be divided on the basis of their assignment.
e. These two roles MUST be in close contact, share their information among themselves and internal forward vulnerability cases between each other, if the case concerns the involvement of the other role.
f. The first cybersecurity contact MUST be the manufacturer's PSIRT, which covers the vulnerability handling of the manufacturer's products and services.
g. The email address of the PSIRT functional mailbox MUST clearly indicate its function. Therefore, the local part of the email (email prefix) SHOULD be "psirt", e.g. psirt@example.com.

h. The second cybersecurity contact MUST be the manufacturer's CSIRT, which covers the vulnerability handling of the manufacturer's infrastructure.
i. The email address of the manufacturer's CSIRT functional mailbox MUST clearly indicate its function. Therefore, the local part of the email (email prefix) SHOULD be "csirt", e.g. csirt@example.com.
j. The manufacturer MUST use dedicated OpenPGP keys according to RFC 9580 for the respective email address of the functional mailboxes in accordance with the specifications of the current BSI TR-03116 Part 4 or the current ECCG Agreed Cryptographic Mechanisms and offer encrypted and signed communication with these keys.
k. The manufacturer MAY provide additional encryption options for the respective email address of the functional mailboxes in accordance with the specifications of the current BSI TR-03116 Part 4 or the current ECCG Agreed Cryptographic Mechanisms and offer encrypted and signed communication with these keys, e.g. S/MIME.
l. Unless the validity period of the keys/certificates, mentioned in j and k, is specified otherwise in the current BSI TR-03116 Part 4 or the current ECCG Agreed Cryptographic Mechanisms, it MUST not exceed five years.
m. Unless the manufacturer is a microenterprise, the manufacturer SHOULD provide for both roles sufficient resources to compensate for any absences and to guarantee the response times and assurances from the CVD policy (see section 4.4).
n. The manufacturer MUST ensure for both roles that vulnerability reports can be at least received and processed in English.
o. The manufacturer MUST clearly define for both roles the authorisations of those involved in these roles.
p. The manufacturer MUST clearly define for both roles the tasks of those involved in these roles.
q. The manufacturer SHOULD ensure that the email addresses of the functional mailboxes have a high readiness to receive emails. This SHOULD be tested, at least by (automatically) sending emails to the functional mailboxes from an external email address every day.

4.3.2 Providing encryption options of security contacts

In the case the manufacturer provides the email addresses of the role-oriented contact options (see section 4.3.1) somewhere on its website, e.g. in the **security.txt** (see section 4.2.3 in combination with section 4.2.4), in the CVD-policy (see section 4.4.3) or on the web page for incoming vulnerability reports (see section 4.5.3):

a. The manufacturer MUST provide the web URIs (according to RFC 7230 section 2.7.2) of the direct download locations of the corresponding OpenPGP public keys (mentioned in 4.3.1 j) in ASCII Armor according to RFC 9580 as **.asc**-files for these email addresses.
b. The manufacturer MUST quote the fingerprints of the corresponding OpenPGP public keys of these email addresses.
c. In the case additional encryption options (mentioned in 4.3.1 k) exist, the manufacturer SHOULD provide the web URIs (according to RFC 7230 section 2.7.2) of the direct download locations of the associated public keys or certificates of these additional encryption options and quote their fingerprints.
d. The web URIs (mentioned in a and c) MUST link directly to the public keys or certificates and MUST NOT link to a web page with a download option of the public keys or certificates.

4.3.3 Web form for vulnerability reports

a. The manufacturer MUST set up as contact option a web form for vulnerability reports. Therefore, a web page with this web form on its website has to be created.
b. The web page with this web form MUST be part of the website of the manufacturer.
c. This web form MUST allow to anonymously submit vulnerability reports.
d. This web form MUST be localised. At least, an English version MUST be offered.

e. This web form SHOULD guide the user through the vulnerability report in a structured manner to ensure that all essential information is entered.
f. This web form SHOULD have a high availability. This SHOULD be tested, at least by (automatically) filling in and submitting the web form every day.

4.3.4 Web page for incoming vulnerability reports

a. The manufacturer MUST create a central web page for vulnerability reporting (see section 4.5).

4.4 CVD policy

The CVD policy is intended to help, improve, standardise and speed up the entire CVD process. It defines the handling of vulnerability reports. This includes the manufacturer's assurance to the reporting entity, how the report will be handled, and what is required for a successful CVD process. Therefore, the manufacturer's CVD policy MUST fulfil at least the requirements mentioned below, which base inter alia on the “BSI CVD guideline for security researchers”[31], the “Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies”[32] and the ETSI TR 103 838 V1.1.1[33].

Providing incentives can encourage the willingness to report vulnerabilities in manufacturers’ products or infrastructure. Offering a “Hall of Fame” web page is one way for manufacturers to publicly thank reporting entities for their vulnerability reports. By establishing financial rewards (bug bounty programme) for those who find vulnerabilities, manufacturers can express their appreciation and create a positive incentive structure. The addition of a reward programme to the CVD policy is therefore RECOMMENDED (see recital 76 of the CRA).

4.4.1 General

a. The manufacturer MUST ensure that the last modification date (in the first version the creation date) of the CVD policy is clearly visible.
b. The manufacturer MUST ensure that the CVD policy is clearly assignable to the manufacturer.
c. The manufacturer MUST review the CVD policy at least yearly to ensure that it is up to date.

4.4.2 Corresponding national CSIRT

In the case of actively exploited vulnerabilities affecting one of the manufacturer’s products or the manufacturer’s infrastructure,

a. the manufacturer MUST notify without undue delay its corresponding national CSIRT (see section 3.1.7) when it becomes aware of them and
b. the manufacturer MUST inform its corresponding national CSIRT about all new information, mitigation measures and their schedules and coordinate these with its corresponding national CSIRT.

4.4.3 Contact details

a. The manufacturer MUST provide the email addresses of the functional mailboxes of the role-oriented contact options (see section 4.3.1). Therefore, requirements of section 4.3.2 MUST be applied.

[31] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html
[32] https://ec.europa.eu/newsroom/dae/redirection/document/99973
[33] https://www.etsi.org/deliver/etsi_tr/103800_103899/103838/01.01.01_60/tr_103838v010101p.pdf

4.4.4 Assurances of the manufacturer to the reporting entity

a. The manufacturer MUST ensure that each incoming vulnerability report is treated confidential to the extent permitted by law. However, information required for the public disclosure of the vulnerability (see section 4.4.10) is exempt.
b. The manufacturer MUST ensure that personal data of the reporting entity will not be disclosed to third parties without the explicit consent of the reporting entity.
c. The manufacturer MUST ensure that a response to each incoming vulnerability report or update of a previously submitted vulnerability report is provided within the guaranteed response times (see section 4.4.8).
d. The manufacturer MUST ensure that no criminal charges will be pursued against the reporting entity as long as this policy and its principles have been complied with by the notifying entity. This does not apply if recognizable criminal intentions have been or are being pursued.
e. The manufacturer MUST ensure that it is available as a contact for a trustful exchange throughout the entire CVD process.
f. The manufacturer SHOULD ensure that, if requested by the reporting entity, the name/alias and a desired reference of the reporting entity will be published in accordance to manufacturer's CVD policy on the manufacturer's acknowledgement web page (Hall of Fame) after reporting a valid vulnerability and completion of the CVD process.
g. The manufacturer MUST NOT require the reporting entity to sign a non-disclosure agreement (NDA).
h. The manufacturer MUST recommend the reporting entity to use an encrypted and digitally signed email for the transmission of confidential information.

4.4.5 Vulnerability guideline

The manufacturer MUST publish a vulnerability guideline, e.g. as part of the CVD policy, in which it defines what it regards as be a valid vulnerability. It SHOULD consider only the following requirements for its classification of a valid vulnerability:

a. The vulnerability MUST affect one of the manufacturer's products or the manufacturer's infrastructure.
b. The vulnerability report SHOULD relate to publicly unknown information.
c. The vulnerability report MAY not be a result of automated tools or scans without supporting documentation.

4.4.6 Code of conduct for the reporting entity

In order to only reward reporters with no malicious intent for purposes of good faith, the manufacturer MAY publish a code of conduct with expected behaviour of the reporting entity and the consequences of non-compliance. But the manufacturer MUST ensure that reports from non-compliant entities are still treated to the best extend possible. The code of conduct MAY contain the following points:

a. No abuse of the reported vulnerability by the reporting entity. That means that no damage has been caused beyond the reported vulnerability.
b. No attacks (such as social engineering, spam, (distributed) DoS or "brute force" attacks, etc.) were carried out against manufacturer's IT systems or infrastructures by the reporting entity.
c. No manipulation, compromise or modification of possible systems or data of third parties was carried out by the reporting entity.
d. No tools for exploiting vulnerabilities have been offered, e.g. on darknet markets, by the reporting entity for a fee or free of charge that third parties could use to commit crimes.
e. No offense regarding section 4.4.7 c by the reporting entity, e.g. in the name/alias or the desired reference for publication on the manufacturer's acknowledgement web page.

The consequences of non-compliance MAY include the following points:

a. The reporting entity does not receive any rewards, e.g. from a bug bounty programme.
b. The reporting entity will not be listed on the acknowledgement web page (Hall of Fame).

4.4.7 Good communication

a. The manufacturer SHOULD ensure that the information reported, on vulnerabilities that have already been remedied, is nevertheless received and checked, even if this report does not qualify for further processing as part of a CVD process.
b. The manufacturer SHOULD explain that good communication is important for vulnerability reports and that at least one valid contact option (preferably an email address) should be provided by the reporting entity for any queries.
c. The manufacturer SHOULD clearly emphasise that all involved entities treat each other with respect and that there is no room for unacceptable behaviour, e.g. discrimination, sexism or insults.
d. The manufacturer SHOULD declare which contact options are accepted.
e. The manufacturer MUST accept at least email addresses and telephone numbers as valid contact options.
f. The manufacturer SHOULD point out that enquiries from the reporting entity about the status of the reported vulnerability are welcome.
g. The manufacturer MUST ensure that all incoming reports are treated to the best extend possible and cannot be closed by a single analyst to avoid missing valid vulnerabilities.

4.4.8 Guaranteed response times

a. The manufacturer MUST ensure that a simple response to a vulnerability report or an update of an existing report is provided within five working days, unless a vulnerability was reported anonymously. This simple response MUST NOT be an automated response.
b. The manufacturer MUST ensure that detailed feedback after further analysis is provided within ten working days, unless a vulnerability was reported anonymously.
c. This detailed feedback MUST include at least either
    - a statement of the manufacturer as to whether it confirms or rejects the reported vulnerability,
    - meaningful queries to understand the reported vulnerability or
    - an explanation why the investigation of the reported vulnerability is taking longer, along with a commitment to provide an update within ten working days.

4.4.9 Anonymous reporting option

a. The manufacturer MUST provide an easy-to-find option to anonymously submit vulnerability reports. This SHOULD be the web form for vulnerability reports (see section 4.3.3).
b. The manufacturer SHOULD clarify that further explanations and documentation may be required, especially in the case of complex issues.
c. The manufacturer SHOULD clarify that if the reporting entity fails to respond to technical or content-related queries, the corresponding vulnerability report can only be processed to a limited extent or possibly not at all.
d. The manufacturer MUST clearly state that anonymous reports can only be processed to a limited extent or possibly not at all, due to missing option to request technical or content-related queries.

4.4.10 Vulnerability disclosure

a. The manufacturer MUST ensure that validated and verified vulnerabilities are publicly disclosed within 90 days, unless the manufacturer becomes aware of a vulnerability and fixes it before the affected product is placed on the market. However, if there is a valid justification and explanation

for a delay in mitigating or fixing the vulnerability, the period until disclosure can be extended once by further 90 days in close consultation with its corresponding national CSIRT. As an exception, the period until public disclosure can be extended further by the corresponding national CSIRT upon request of the manufacturer.

b. This public disclosure MUST take place, upon request of the manufacturer in consultation with its corresponding national CSIRT or ENISA, at least on the European Vulnerability Database (EUVD)[34] maintained by ENISA.

4.4.11 End of CVD process

a. The manufacturer MUST clearly and publicly state the conditions under which the CVD process is considered complete.
b. The manufacturer SHOULD communicate the end of the CVD process without undue delay to the reporting entity, unless the vulnerability was reported anonymously.
c. The manufacturer SHOULD consider the CVD process to be completed if the indications of the vulnerability report are unfounded.
d. The manufacturer SHOULD consider the CVD process to be completed if the vulnerability of a service (e.g. a web service) is fixed and has been publicly disclosed.
e. The manufacturer SHOULD consider the CVD process to be completed if the vulnerability has been mitigated or fixed by an appropriate patch and has been publicly disclosed.
f. The manufacturer MAY consider the CVD process to be completed if the reporting entity fails to respond to technical or content-related queries for at least 30 days and therefore the corresponding vulnerability report can only be processed to a limited extent or not at all.
g. The manufacturer MAY consider the CVD process to be completed if the vulnerability has been publicly disclosed and, in consultation with its corresponding national CSIRT, it can no longer be assumed that the vulnerability will be mitigated or fixed.

4.5 Web page for incoming vulnerability reports

External entities should find all important information regarding the submission of vulnerability reports at a central point on the manufacturer's website. Therefore, the web page for incoming vulnerability reports MUST have at least the following features.

4.5.1 General

a. The web page for incoming vulnerability reports MUST be part of the website of the manufacturer.
b. This web page MUST be accessible at least via an easy-to-find link on the home page of the manufacturer’s website without activated JavaScript or other client-side executed scripts.
c. The path of the web URI (according to RFC 7230 section 2.7.2) of this web page MUST clearly indicate its function, e.g. https://www.example.com/security-contact. A redirection to another web URI (according to RFC 7230 section 2.7.2) on the manufacturer’s website is allowed.
d. The manufacturer MUST ensure that this web page with all information is fully accessible without activated JavaScript or other client-side executed scripts and without any login procedure or other restriction, e.g. a paywall.
e. The information on this web page MUST be clearly structured.
f. The manufacturer SHOULD point to its privacy policy close to the sections about the transmission of personal data, e.g. the contact details of the reporting entities.

[34] https://euvd.enisa.europa.eu/

4.5.2 Publication of the CVD policy

a. The manufacturer MUST put an easy-to-find link on this web page for redirection, forwarding or routing to the web page where its CVD policy is published. Therefore, the manufacturer MUST create a web page with its CVD policy.
b. Requirements 4.5.1 a, d, and e also apply to the CVD policy web page.

4.5.3 Publication of contact options

a. The manufacturer MUST provide the email addresses of the role-oriented contact options (see section 4.3.1). Therefore, requirements of section 4.3.2 MUST be applied.
b. The manufacturer MAY additionally publish these addresses at the “Contact Us” web page of its website.
c. The manufacturer MUST provide the web URI (according to RFC 7230 section 2.7.2) of the direct download location of the corresponding OpenPGP public key in ASCII Armor according to RFC 9580 as an **.asc**-file for signing the **security.txt** (see section 4.2.10).
d. The manufacturer MUST quote the fingerprint of the OpenPGP public key for signing the **security.txt** (see section 4.2.10).
e. The manufacturer MUST provide the web URI (according to RFC 7230 section 2.7.2) to the web form for vulnerability reports (see section 4.3.2).
f. The expiry date of the contact options MUST be specified and updated well enough in advance before they expire. This expiry date SHOULD be at the maximum of one year in the future.

5 Annex

This section provides additional, explanatory information.

5.1 Further information

5.1.1 “Handhabung von Schwachstellen v2.0 – Empfehlungen für Hersteller”

BSI has published recommendations for manufacturers in German on how to deal with vulnerabilities correctly.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf

5.1.2 Good Practice Guide on Vulnerability Disclosure

ENISA has published this study to identify the challenges and good practices of vulnerability disclosures.
https://www.enisa.europa.eu/publications/vulnerability-disclosure

5.1.3 The CERT Guide to Coordinated Vulnerability Disclosure

The CERT Coordination Center (CERT/CC) has published a web edition of the CERT Guide to Coordinated Vulnerability Disclosure originally published by the Software Engineering Institute of the Carnegie Mellon University.

Web edition: https://certcc.github.io/CERT-Guide-to-CVD/
Original publication: https://insights.sei.cmu.edu/library/the-cert-guide-to-coordinated-vulnerability-disclosure-2/

5.1.4 DIN EN ISO/IEC 29147:2020-08 or ISO/IEC 29147:2018

This ISO standard describes further recommendations and requirements about vulnerability disclosures.

https://www.iso.org/standard/72311.html
https://www.dinmedia.de/de/norm/din-en-iso-iec-29147/324674445

5.1.5 DIN EN ISO/IEC 30111:2020-07 or ISO/IEC 30111:2019

This ISO standard describes further recommendations and requirements about vulnerability handling processes.

https://www.iso.org/standard/69725.html
https://www.dinmedia.de/de/norm/din-en-iso-iec-30111/324674587

5.1.6 ISO/IEC 20153:2025

This ISO standard describes format and distribution of automated and machine-readable security advisories according to the OASIS CSAF v2.0 specification.

https://www.iso.org/standard/89986.html
https://webstore.iec.ch/en/publication/105858

5.1.7 SecureDrop

This is an open-source software for receiving documents from anonymous sources and still communicate with them.

https://securedrop.org/
https://github.com/freedomofpress/securedrop

5.1.8 CSAF Provider

This is an open-source tool for generating all metadata and structure necessary to provide CSAF documents according to the standard in an automated manner.

https://github.com/gocsaf/csaf/blob/main/docs/csaf_provider.md