Federal Office
for Information Security

Technical Guideline 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

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

Table of Contents

1 Introduction

Vulnerabilities have an impact on security and probably even safety of products, its users and the environment. However, they 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.

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. Moreover, this Technical Guideline assumes that the manufacturer operates a website.

Although secure development and operating processes minimise the number of vulnerabilities in products, they do not guarantee that there are no vulnerabilities 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.

The members of the European Union Computer Security Incident Response Teams (CSIRTs) Network[2] are the central points of contact in the EU for preventive and reactive measures related to cybersecurity incidents in computer systems. In Germany, the designated CSIRT is the Computer Emergency Response Team for Germany's federal authorities (CERT-Bund)[3]. 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, validated and verified vulnerabilities notified to CERT-Bund and thus to the BSI are ALWAYS shared with the manufacturers or product owners to eliminate or mitigate them[4].

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**[5] in accordance with RFC 9116[6] on the manufacturer's website fulfils this purpose.

[1] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html
[2] https://csirtsnetwork.eu/#network_members
[3] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html
[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.html
[5] https://securitytxt.org/
[6] https://www.rfc-editor.org/rfc/rfc9116

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[7] (RFC 2119[8], RFC 8174[9]) when, and only when, they appear in all capitals, as shown here.

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

3 Basics

3.1 Terms used

3.1.1 Manufacturer

The CRA defines ‘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

In this Technical Guideline, a vulnerability is a flaw or weakness in a product, (web) application or service that could be exploited or triggered by a threat source[10].

3.1.3 Valid, validated and verified vulnerability

Every entity can decide, what it considers to be a valid vulnerability. These may include requirements from the reporting entity of the vulnerability. Recommendations concerning them are found in section 4.3.5 and in the BSI CVD guideline for security researchers[11].

After the manufacturer has confirmed that the vulnerability complies with its rules for a valid vulnerability, this vulnerability is a validated vulnerability.

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

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 CSIRTs or ENISA and are non-public.

[10] https://csrc.nist.gov/glossary/term/vulnerability
[11] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html

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 of 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) documents[12].

3.1.6 Vulnerability Report

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

3.1.7 Corresponding CSIRT

To comply with this Technical Guideline, manufacturers MUST choose any of the CSIRTs of the European Union CSIRTs network for vulnerability notifications as its corresponding CSIRT. The corresponding CSIRT MUST be determined according to Article 14 (7) CRA. Moreover, manufacturers MUST stay at their corresponding CSIRT during the active handling of every single valid vulnerability except the corresponding CSIRT transfers the handling. Furthermore, manufactures SHOULD choose the same 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 MUST NOT be logged includes the IP address, the browser or the computer of reporting entity.

[12] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03191/TR-03191_node.html

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 4.1), on the web page for incoming vulnerability reports (see section 4.4) or in the CVD policy (see section 4.3) and additional preliminary measures for a CVD process (see section 4.2) are allowed.

4.1 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“[13] and the RFC 9116 itself. A recommended **security.txt** is shown as an example in Figure 1.

4.1.1 Localisation of security.txt

a. The manufacturer MUST create a file with the name **security.txt** 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[14] or a higher version.
c. This file MUST be a plain text file with ASCII or UTF-8 encoding, whereby 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.

4.1.2 Contact information

a. The manufacturer SHOULD introduce the list of contact options for reporting vulnerabilities with the comment **# Our security addresses**.
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) in accordance with RFC 6068[15] (see section4.2.1).
c. The declaration of the first contact option MUST be the email address of the functional mailbox of the manufacturer’s CSIRT in accordance with RFC 6068 (see section4.2.1).
d. The next point of contact MUST be the URL of the manufacturer's web page for incoming vulnerability reports (see section 4.4) according to RFC 7230 and RFC 3986[16].

[13] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_149.html
[14] https://www.rfc-editor.org/rfc/rfc7230
[15] https://www.rfc-editor.org/rfc/rfc6068
[16] https://www.rfc-editor.org/rfc/rfc3986

4.1.3 Expiry date

a. The manufacturer MUST specify the expiry date of the **security.txt** according to RFC 3339[17]. 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.

4.1.4 OpenPGP keys

a. The manufacturer MUST provide a URI for downloading the public OpenPGP keys of its email addresses for receiving vulnerability reports (see section 4.2.1). In the case additional security options mentioned in section 4.2.1 exist, the manufacturer SHOULD provide a URL for downloading them.
b. The URIs of the direct download location of the corresponding OpenPGP public keys in ASCII Armor according to RFC 4880[18] as **.asc**-files MUST be specified.
c. An URL for a web page with a download option of the corresponding OpenPGP key files MUST NOT be specified.
d. This listing SHOULD be introduced with the comment **# Our OpenPGP keys**.

4.1.5 Acknowledgements

a. The manufacturer SHOULD provide the URL of the acknowledgements for vulnerability reports web page.
b. This listing SHOULD be introduced with the comment **# Our security acknowledgements page**.

4.1.6 Preferred languages

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

4.1.7 CVD policy

a. The manufacturer MUST provide the URL to the web page of its CVD policy.
b. This SHOULD be introduced with the comment **# Our security policy**.

4.1.8 Job offers

a. The manufacturer MAY provide the URL for the web page with current job vacancies.
b. This SHOULD be introduced with the comment **# Our vacancies**.

4.1.9 Security advisories

a. The manufacturer SHOULD provide the URI (according to RFC 7230) of the file **provider-metadata.json** for CSAF documents[19].
b. This statement MUST begin with the tag **CSAF:**
c. This statement MUST be introduced with the comment **# Our security advisories**.

[17] https://www.rfc-editor.org/rfc/rfc3339
[18] https://www.rfc-editor.org/rfc/rfc4880
[19] https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html#718-requirement-8-securitytxt

4.1.10 Digital signature

a. The manufacturer MUST digitally sign its **security.txt** using OpenPGP according to RFC 4880.
b. The manufacturer MUST use dedicated OpenPGP sub-keys (of the same OpenPGP "identity key") for signing the **security.txt** according to RFC 4880.
c. This key MUST be made available (see section 4.4.3).
d. The manufacturer MUST ensure that the digital signature complies with the requirements of the current TR-03116 Part 4[20] or the current SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms[21].

4.1.11 Canonical URI

a. The manufacturer MUST specify the canonical URI of the **security.txt**.
b. This statement SHOULD be introduced with the comment **# Our canonical URI**.

4.1.12 Visibility for web crawlers

a. The manufacturer MUST ensure that the **security.txt** can be found automatically (i.e. by web crawlers, for example from findsecuritycontacts.com[22] and internet.nl[23]). Hence, firewall rules and DDoS protection rules have to be adapted accordingly, if applicable.

[20] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html
[21] https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf
[22] https://findsecuritycontacts.com/
[23] 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 vacancies
Hiring: https://www.example.com/Jobs

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

Expires: 2025-01-01T00:00:00.000Z
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.2

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

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

4.2 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.

4.2.1 Roles of responsible cybersecurity contacts

a. The manufacturer MUST create two roles of responsible cybersecurity contacts. These roles MUST NOT be assigned to a single person, but MUST be divided among several persons.
b. The manufacturer MUST assign functional mailboxes to both roles and MUST ensure that those involved in these roles have access to their corresponding functional mailbox.
c. These two roles MUST be divided on the basis of their assignment.

d. 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 assignment of the other role.
e. The first cybersecurity contact MUST be the manufacturer's PSIRT, which covers the vulnerability handling of the manufacturer's products.
f. The email address of the PSIRT functional mailbox MUST clearly indicate its function. Therefore, the local part of the email (email prefix) MUST be "psirt", e.g. psirt@example.com. Moreover, additional mailboxes with at least "productcert" and "vulnerability" as local part of the email MUST be created. Incoming emails to these additional mailboxes MUST be redirected to the PSIRT functional mailbox.
g. The second cybersecurity contact MUST be the manufacturer's CSIRT, which covers the vulnerability handling of the manufacturer's infrastructure.
h. The email address of the CSIRT functional mailbox MUST clearly indicate its function. Therefore, the local part of the email (email prefix) MUST be "csirt", e.g. csirt@example.com. Moreover, additional mailboxes with at least "cert" and "security" as local part of the email MUST be created. Incoming emails to these additional mailboxes MUST be redirected to the PSIRT functional mailbox.
i. The manufacturer MUST publish the email addresses of the functional mailboxes at the "Contact Us" web page of its website, if this web page exists.
j. The manufacturer MUST use dedicated OpenPGP sub-keys (of the same OpenPGP "identity key") according to RFC 4880[24] for the email addresses of the functional mailboxes in accordance with the specifications of the current TR-03116 Part 4 or the current SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms and offer encrypted and signed communication with these sub-keys.
k. The manufacturer MAY provide additional security options for the email addresses of the functional mailboxes in accordance with the specifications of the current TR-03116 Part 4 or the current SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms and offer encrypted and signed communication with these keys, e.g. S/MIME or OpenPGP according to RFC 6637[25].
l. The manufacturer MUST 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 4.3).
m. The manufacturer MUST ensure for both roles that vulnerability reports can be at least received and processed in English.
n. The manufacturer MUST clearly define for both roles the authorisations of those involved in these roles.
o. The manufacturer MUST clearly define for both roles the tasks of those involved in these roles.
p. 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.

4.2.2 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. This web form MUST allow to anonymously submit vulnerability reports.
c. This web form MUST be localised. At least, an English version MUST be offered.
d. This web form SHOULD guide the user through the vulnerability report in a structured manner to ensure that all essential information is entered.
e. 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.

[24] https://www.rfc-editor.org/rfc/rfc4880
[25] https://www.rfc-editor.org/rfc/rfc6637

4.2.3 Web page for incoming vulnerability reports

a. The manufacturer MUST create a central web page for vulnerability reporting (see section 4.4).
b. This web page MUST be accessible via an easy-to-find link on the home page of the manufacturer's website without JavaScript enabled.
c. The path of the URL of this web page MUST clearly indicate its function, for example https://www.example.com/Security-Contact. A redirection to another URL on the manufacturer's website is allowed.

4.3 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 have at least the following characteristics. The requirements of the CVD policy base inter alia on the "BSI CVD guideline for security researchers[26]", Guidelines on implementing national Coordinated Vulnerability Disclosure (CVD) policies[27] and the ETSI TR 103 838 V1.1.1[28].

Providing incentives can encourage the willingness to report vulnerabilities in manufacturers' products. 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. This Technical Guideline considers reward programmes as an OPTIONAL element of a CVD policy.

4.3.1 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 itself.
c. The manufacturer MUST review the CVD policy at least yearly to ensure that it is up to date.

4.3.2 Corresponding CSIRT

a. The manufacturer MUST notify without undue delay to its corresponding CSIRT (see section 3.1.2) all valid vulnerabilities of which it becomes aware.
b. In case of validated and verified vulnerabilities, the manufacturer MUST inform its corresponding CSIRT of all new information, mitigation measures and their schedules and coordinate these with its corresponding CSIRT.

4.3.3 Contact details

a. The manufacturer MUST name the email addresses of the functional mailboxes of the role-oriented contact options (see section4.2.1).
b. The manufacturer MUST provide the URIs of the direct download locations of the corresponding OpenPGP public keys (see sections 4.1.10 and 4.2.1) in ASCII Armor according to RFC 4880 as **.asc**-files.
c. The manufacturer MUST quote the fingerprints of the corresponding OpenPGP keys (see sections 4.1.10 and 4.2.1).
d. The manufacturer SHOULD provide the URIs of the direct download locations of the public keys or certificates of the additional security options (mentioned in section 4.2.1), if they exist.

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

e. 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.

4.3.4 Assurances of the manufacturer to the reporting entity

a. The manufacturer MUST ensure that each vulnerability report is kept confidential to the extent permitted by law.
b. The manufacturer MUST ensure that personal data 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 vulnerability report is provided within the guaranteed response times (see section 4.3.8).
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 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 a contact for a trustful exchange throughout the entire CVD process.
f. The manufacturer MUST ensure that, if requested by the reporting entity, the name/alias and a desired reference of the reporting entity will be published on the manufacturer's acknowledgement web page (Hall of Fame) after reporting a valid vulnerability and completion of the CVD process. In doing so, it SHOULD be clearly emphasised that all involved entities treat each other with respect and that there is no room for in the EU unlawful behaviour, like discrimination, sexism, racism, Nazism, glorification of violence, pornography, insults, defamation and slander. In the event of an offence in this regard, the institution MUST refrain from publication.
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.

4.3.5 Requirements of valid vulnerabilities

The manufacturer SHOULD NOT request for the reporting of a valid vulnerability other than the following cases:

a. The vulnerability MUST affect one of the manufacturer’s products.
b. The vulnerability report relates to publicly unknown information.
c. The vulnerability notifications are not results of automated tools or scans without supporting documentation.

4.3.6 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. The reported vulnerability has not been abused 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.

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).

4.3.7 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 declare what contact options are accepted.
d. The manufacturer MUST accept at least email addresses and telephone numbers as valid contact options.
e. The manufacturer SHOULD point out that enquiries from the reporting entity about the status of the reported vulnerability are welcome.

4.3.8 Guaranteed response times

a. The manufacturer MUST ensure that a simple response to a vulnerability 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. The manufacturer MUST ensure that the reported vulnerability is either confirmed or rejected within ten working days, unless a vulnerability was reported anonymously.

4.3.9 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, mentioned in section 4.2.2)
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.
e. The manufacturer MUST ensure that anonymous reports are treated to the best extend possible and cannot be closed by a single analyst to avoid missing valid vulnerabilities.

4.3.10 Vulnerability disclosure

a. The manufacturer MUST ensure that validated and verified reported vulnerabilities are publicly discloses within 90 days. 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 CSIRT. As an exception, the period until public disclosure can be extended further by the corresponding CSIRT upon request of the manufacturer.
b. The manufacturer MUST ensure that, in consultation with its corresponding CSIRT, the vulnerability is publicly disclosed, for example at the National Vulnerability Database (NVD) from the National Institute for Standards and Technology (NIST)[29].

[29] https://nvd.nist.gov/

4.3.11 End of CVD process

a. The manufacturer MUST clearly and publicly state when the CVD process is considered to be completed.
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. 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 vulnerability has been publicly disclosed and, in consultation with its corresponding CSIRT, it can no longer be assumed that the vulnerability will be mitigated or fixed.

4.4 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 should have at least the following features.

4.4.1 General

a. The manufacturer MUST ensure that this web page with all information is fully accessible without activated JavaScript and without any login procedure or other restriction, e.g. behind a paywall.
b. The information on this web page MUST be clearly structured and easy to find for external entities.
c. The manufacturer SHOULD point to its privacy policy nearby the sections about the transmission of personal data, e.g. contact details of the reporting entities).

4.4.2 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 on its website where its CVD policy is published. Therefore, the manufacturer MUST create a web page with its CVD policy.
b. The manufacturer MAY make its CVD policy additionally available for free to be downloaded in PDF/A-2a format[30] on the web page with its CVD policy.

4.4.3 Publication of contact options

a. The manufacturer MUST provide the email addresses of the role-oriented contact options (see section 4.2.1).
b. The manufacturer MUST provide the URIs of the direct download locations of the corresponding OpenPGP public keys in ASCII Armor according to RFC 4880 as **.asc**-files for the email addresses mentioned in a.
c. The manufacturer MUST quote the fingerprint of the OpenPGP keys for the email addresses mentioned in a.
d. The manufacturer MUST provide the URI of the direct download location of the corresponding OpenPGP public key in ASCII Armor according to RFC 4880 as an **.asc**-file for signing the **security.txt** (see section 4.1.10).

[30] ISO 32000-1:2008 - Document management — Portable document format - Part 1: PDF 1.7

e. The manufacturer MUST quote the fingerprint of the OpenPGP key for signing the **security.txt** file (see section 4.1.10).
f. In case the manufacturer provides additional security options (according section 4.2.1) for the email addresses mentioned in a, the manufacturer MUST provide the URIs of the direct download locations of the associated public keys or certificates of these additional security options and quote their fingerprints.
g. The manufacturer MUST provide the URL to the web form for vulnerability reports, mentioned in section 4.2.2.
h. 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 this recommendations for manufacturers 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 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