Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies

Guideline – NIS Cooperation Group

2023

NIS COOPERATION GROUP

Contents

1. Introduction

Under Article 7(2) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union ('Network and Information Security' directive 2 (NIS2)), EU Member States shall, as part of their national cybersecurity strategy, in particular adopt policies managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure (CVD) under Article 12(1). Each Member State is thus required to adopt and implement national policies promoting and facilitating CVD processes. In accordance with Article 12(1) and Article 11(3)(g) of NIS2, one key element of these policies is the role assigned at the national level to at least one Computer Security Incident Response Team (CSIRT) to act as a coordinator for the purposes of CVD and receive vulnerability reports. At the same time, essential and important NIS2 entities have to apply, as part of their cybersecurity technical, operational and organisational risk-management measures, vulnerability handling and disclosure measures ([1]).

In their implementation of NIS2, Member States should therefore aim to address in their national legal order the challenges faced by CSIRT, organisations (including NIS2 entities) and reporters/researchers in CVD processes, including the related legal and practical aspects.

Target audience

The target audience of this guideline are the national competent authorities that will integrate vulnerability management and CVD processes in their national cybersecurity strategies and policies.

Goal of this guideline

The document aims to provide accessible guidance to help Member States in the development of their national CVD policies, under the requirements of NIS2. The following will be particularly applicable for these guidelines.

- They will serve as a guideline for the implementation by Member States of national CVD policies.
- They are developed in cooperation and with the input of all Member States, in order to ensure their added value.
- They should be neutral with regard to standards and technology.

Background and context

The NIS Cooperation Group is an EU collaboration group on strategic cybersecurity measures. Work Stream Cybersecurity Risk and Vulnerability Management, a working group under the NIS Cooperation Group, brings together experts from national authorities to discuss and collaborate strategically on issues regarding cybersecurity risk, security measures and vulnerability management.

([1]) Article 21(1) and Article (2)(e) NIS2.

In June 2022, Work Stream Cybersecurity Risk and Vulnerability Management formed a task force, which also included members of the CSIRT network, to develop the guidelines on implementing national CVD policies, which are part of the broader national vulnerability management policies.

This document has been drafted and endorsed by the NIS Cooperation Group members. The group, composed of representatives of the Member States, the Commission and the European Union Agency for Cybersecurity (ENISA), has been established by Article 11 of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) and confirmed by Article 14 of the NIS2.

2. Definitions and roles

In this section we present the definitions and roles that are relevant to vulnerability management and CVD.

In accordance with Article 6(15) of NIS2, a **vulnerability** means a weakness, susceptibility or flaw of information and communications technology (ICT) products or services that can be exploited by a cyber threat. Based on ISO/IEC 27002:2022, a vulnerability is a weakness of an asset or control that can be exploited by one or more threats ([2]). In terms of ISO/IEC 29147:2018 ([3]), vulnerability implies a functional behaviour of a product or service that violates an implicit or explicit security policy. For the purpose of these guidelines, we use the term 'system' or 'service' as not only including ICT systems, products or services, but also other assets such as operational technologies.

In general, we can understand vulnerability as a flaw or a weakness, a design or execution error, or the lack of updates in light of existing technical knowledge, which may affect an asset or control. A vulnerability can lead to an unexpected or unwanted event or an expression of threat, and can be exploited by malicious third parties to harm the integrity, authenticity, confidentiality or availability of a system.

CVD policy. This is a formalised set of rules for searching for and reporting vulnerabilities, with an emphasis on coordinated handling of information about these vulnerabilities, in order to limit the damage caused by unintentional or untimely disclosure or by non-responsive counterparties. These rules should ensure and be associated with, inter alia, secure means of communication and confidentiality of the information exchanged, and provide a guarantee that the entities involved in the process will not disclose vulnerability information without due coordination.

National CVD policies. These are policies adopted by Member States to promote and facilitate CVD, as part of their national cybersecurity strategy. The CVD is described in recitals 58–62 and Article 12(1) of NIS2 as the process between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or services, in which designated CSIRT(s) could play a coordinator role, acting as a trusted intermediary and facilitating, where necessary and upon the request of either party, the interaction between the concerned stakeholders ([4]).

([2]) ISO (2022), *ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls*.
([3]) ISO (2018), *ISO/IEC 29147:2018, Information technology – Security techniques – Vulnerability disclosure*.
([4]) Article 12(1) and Article 11(3)(g) NIS2.

Reward programme. This is an optional element of a CVD policy which can offer different types of rewards for submitting a valid vulnerability report, such as a vulnerability reward programme – also known as a 'bug bounty' – or a recognition/gift programme.

Vendor/supplier. This is a natural or legal person that owns, manufactures, sells, offers or manages systems, products or services, and is therefore responsible for their functionality and security. It is highly recommended for vendors/suppliers to publish a CVD policy, in order to allow researchers to identify and report vulnerabilities and to build internal capacity and governance to address CVD-related issues. Vendors/suppliers must be involved in the verification and remediation of the vulnerabilities.

System owner or manager. This is a natural or legal person, or a public authority that operates systems, products or services, including product as a service, for other customers. They are responsible for implementing CVD policy in their environment, assessing vulnerability reports, communicating with the vendor/supplier and applying the necessary measures.

Researcher. This is a natural person or legal entity who intentionally or incidentally, but always with good intentions, researches potential vulnerabilities.

Reporter. In the context of this document, a reporter is a researcher who identifies and reports potential vulnerabilities.

Coordinator. As a trusted intermediary, the coordinator can connect and coordinate further actions to remediate a vulnerability that threatens multiple vendors or the system owners. The coordinator can also provide technical analyses or expert assistance.

It should be noted that it is possible for some entities to have several roles at the same time.

3. Addressing the main legal challenges at the national level

In the course of the development and implementation of a national CVD policy, there is a high possibility of encountering specific legal challenges that hinder this effort. A non-exhaustive list of such legal challenges and proposed solutions is shown below.

Criminal law	**Problem:** criminal law may be an important challenge in implementing national CVD policies. The circumstances relating to searching for vulnerabilities could fulfil the conditions of a cybercrime (e.g., unauthorised access to an information system, use of hacking tools), according to national or international criminal law. CVD processes also have a cross-border nature, given that there are no geographic silos as to where the reporter is located and where they identify the vulnerability. For example, the finding may concern a computer system in one Member State, but the reporter may be in another Member State. As a result, the reporter may be subject to the laws of both jurisdictions.
	Possible solution: adoption of a safe harbour for researchers within a dedicated legal framework as part of the vulnerability reporting procedure created to the designated CSIRT. Member States should

	also promote the development and adoption of consistent CVD policies by vendors and system owners. In such cases, the reporter would be protected while operating within the boundaries of the safe harbour and/or the CVD policy.
Damage caused by the reporter	**Problem:** with regard to the civil law dimensions of CVD, the issue of damages caused by vulnerability research activities can be considered as the central issue. Unwilling damage may occur during actions of the reporter.
	Possible solution: inclusion of a provision in the legal framework and/or a clause in the CVD policy to waive civil liability in cases of unwilling damage occurring during the vulnerability research activities, respecting the scope and limits (e.g. prohibited actions) of the legal framework or the CVD policy.
Protection of personal data	**Problem:** despite the fact that CVD is not primarily focused on the processing of personal data, in certain cases, personal data may be processed when vulnerabilities are found. According to Article 4(2) of the general data protection regulation (GDPR), the processing of personal data is an operation or set of operations which is carried out with or without the aid of automated procedures, such as the collection, retrieval, consultation, alteration, structuring or erasure or destruction of personal data. While finding vulnerabilities, the reporter may come across personal data stored in the ICT product being tested. If so, the researcher could infringe the GDPR or other law on the protection of personal data because the data processing is done without a lawful purpose.
	Possible solution: adoption of a legal framework and/or the inclusion in each CVD policy of obligations regarding processing of personal data, and an obligation for the reporter to inform the vendor in case any personal data is collected as part of the research. When such a legal framework exists, the processing of personal data for the purpose of researching and reporting IT vulnerability is therefore lawful. The legal framework or the CVD policy could directly regulate the relationship between the reporter and the system owner or manager relating to personal data, so that the system owner or manager can keep (or not) the status of a controller according to Article 4(8) of the GDPR in case of processing personal data in CVD. Depending on its content, a CVD policy can therefore also be seen as a processing contract under GDPR, on the basis of which the reporter would lawfully process the personal data. In addition, it can be highlighted that the reporter's activities in a CVD process could be defined as, inter alia, testing the effectiveness of the technical measures in place to ensure the security of the processing of personal data pursuant to Article 32(1)(d) of the GDPR.
Intellectual property legislation	**Problem:** certain types of ICT products constitute a copyrighted work according to copyright law, which provides legal protection against unauthorised use of the work and interference with it. This situation

	can occur when vulnerabilities are found by a reporter. It is possible that certain systems or software licensed within or outside of EU could be protected by legislation or contractual conditions that can prevent reverse engineering or vulnerability research. An example of this could be the American Digital Millennium Copyright Act.
	Possible solutions: where, as part of the CVD policy, the system owner or manager authorises a reporter to investigate, study or test a copyrighted ICT product, the discovery of vulnerabilities in the product would not infringe its copyright protection. The CVD policy should mention that when in doubt about copyright protection, the researcher should avoid testing the software program and just notify the vendor of the vulnerability. Concerning trade secrets, the discovery and reporting of vulnerabilities is not prevented by the discoverer's prior knowledge of a trade secret acquired, for example, through employment. In this respect, Article 5(b) of Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure is procedurally protected.

4. Important elements of national CVD policies

4.1. Establishing procedures and capacities to support national CVD processes

National CVD policies imply a coordinating role for the designated CSIRT(s), acting as a trusted intermediary and facilitating, where necessary and upon the request of either party, the interaction between the concerned stakeholders ([5]). Those coordination tasks include identifying and contacting the entities concerned, assisting the natural or legal persons reporting a vulnerability, and negotiating disclosure timelines and managing vulnerabilities that affect multiple entities. The same provision also requires Member States to ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the designated CSIRT(s). The CSIRT shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability, ensure the anonymity of the natural or legal person reporting the vulnerability and, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network ([6]).

As a result, each Member State should:

(1) designate at least one CSIRT as coordinator for the purposes of CVD;
(2) offer a legal framework and procedure for the CVD process, including legal grounds for the actions of the designated CSIRT and the reporter (see point 4.2);
(3) offer a clear and accessible reporting procedure;

([5]) Article 12(1) and Article 11(3)(g) NIS2.
([6]) Article 12(1) and Article 11(3) NIS2.

(4) adopt internal procedures to ensure diligent follow-up actions, the anonymity of the natural or legal person reporting the vulnerability and, where appropriate, cooperation with other CSIRTs;
(5) provide comprehensive guidance on the national CVD policies, describing the procedure, respective roles, tasks and allowed actions (see point 4.3);
(6) allocate sufficient resources and capacity (including staff, appropriate and dedicated tools, etc.) to the designated CSIRT and/or competent authorities;
(7) offer recommendations to organisations to adopt their own CVD policy (see Section 5);
(8) harmonise its national CVD processes with other national policies, guidance and obligations relating to vulnerability management, including obligations for international cooperation and information exchange.

4.2. Adopting a framework ensuring legal protection

In order for the designated CSIRT to legally act as a CVD coordinator and to avoid the legal obstacles mentioned in Section 3, each Member State should establish clear rules for the reporting of vulnerabilities and offer legal grounds for the actions of the designated CSIRT and the reporter when certain conditions are met.

Member States should adopt legal solutions to make it easier for the designated CSIRT to contact the owners of vulnerable systems visible from the internet, such as granting the right to obtain the contact details (e.g. WHOIS data) of the owner of a public IP address, in a supervised manner, in order to identify, for example, how many organisations are exposed to a reported vulnerability.
Each Member State should also ensure that natural or legal persons are able, even anonymously where they so request, to report a vulnerability to a coordinator CSIRT, especially in the absence of a CVD policy adopted by the system owner or vendor. To allow such a vulnerability reporting, the reporter needs to benefit from a legal protection, naturally under strict conditions.

An example of a set of indicative conditions to offer legal protection to a researcher or reporter is shown below.

(1) Acting without fraudulent intent or malice.
(2) Notifying the designated CSIRT as soon as possible and at the latest within a pre-specified timeframe from discovery of the vulnerability. When the discovered vulnerability potentially affects NIS entities or multiple other organisations, it should be recommended for the vendor or system owner that received the initial vulnerability report to also proactively notify the national CSIRT. The practical details of the reporting procedure to the designated CSIRT should be easily identified, including secure communication means.
(3) Notifying the concerned system owner or vendor, where necessary and possible, as soon as possible and at the latest within a pre-specified timeframe from discovery of the vulnerability.
(4) Not acting beyond what is necessary and proportionate to verify and report the existence of a vulnerability. The procedure could include examples of forbidden actions considered as disproportionate and/or unnecessary.
(5) Avoiding public disclosure of the information discovered during the vulnerability research without the prior agreement of the designated CSIRT. The agreement should be given after coordination with vendors or system owners and/or all concerned parties with the vulnerability. Member States can define time limits for the CVD process, after which the researcher is allowed to disclose the vulnerability without the approval of the CSIRT or vendor. Such timeouts should not be unreasonably short (e.g. at least 1 year) and could

include exceptions (e.g. for public security reasons, when a vulnerability is still being actively exploited or when it is in the public interest not to disclose it).

Provided that the reporter strictly complies with all the defined conditions, they should not be considered as having breached criminal or civil laws and should in principle not incur liabilities regarding the necessary and proportionate actions taken to research and report the potential vulnerability. If the legal conditions are met, the legal procedure should guarantee the anonymity of the natural or legal person who has reported the vulnerability, when they so request. The procedure should also cover the case where a reporter is reporting a potential vulnerability that they have become aware of in their professional context.

With respect to tools, code or devices for vulnerability research, the reporter may develop, possess or use such solutions only for the purpose of the vulnerability disclosure policy. Such actions should not be considered unlawful, as long as they are justified by legitimate purposes relating to the detection and reporting of vulnerabilities.

4.3. Guidance on national CVD policies

The national competent authorities need to develop and provide public guidelines clarifying their framework on CVD, assisting the involved entities on their respective roles, informing on the support that national authorities could offer and sharing good practices. Their content should be easily accessible online and the guidelines should be reviewed and updated on a regular basis.

When adopting guidance on their national CVD policies (hereafter CVD framework), Member States need to do so in a way that provides incentives to researchers for reporting vulnerabilities and to vendors or system owners for using the CVD process. In order to achieve this, the following principles should be taken into account.

- **Clarity.** The CVD framework should be as clear, comprehensive and informative as possible, leaving no room for ambiguities. It should provide clear rules on where to report vulnerabilities (e.g. to the CSIRT rather than directly to the manufacturer), in which situation and how. It should also explain the conditions under which security researchers can act without fear of criminal or civil legal repercussions.
- **Simplicity.** The CVD framework should be as simple and straightforward as possible. Any unnecessary complexity in the framework will create distrust and will likely disincentivise security researchers from legally following the policy.
- **Publicity of the policy.** The rules should be properly disseminated to the public.
- **Cooperation.** Rules for the cooperation between parties in cases when the organisation has not adopted a CVD policy, does not wish to cooperate with the reporter or simply does not reply.
- **Anonymity.** There could be certain cases where the reporter of a vulnerability wishes to remain anonymous. The CVD framework should include provisions for the protection of the anonymity of the researcher in case this is requested,
- **Recognition.** Many researchers are heavily incentivised by the recognition and reputation gained from discovering and reporting a vulnerability. The CVD framework should allow ways to recognise the value of the vulnerability report, such as a ‘Hall of Fame’ web page, a letter of appreciation, symbolic gifts (such as t-shirts, coins or mugs) or financial incentives (e.g., bug bounty programmes).

The CVD framework should also clarify and at least take into account these additional elements:

- the role of the designated CSIRT to act as a trusted intermediary;
- the role of supervisory national competent authorities in case the vulnerability concerns an NIS entity;
- the rules based on which such a vulnerability should be publicly released;
- the rules based on which such a vulnerability could be shared with the public or with a limited audience (such as specific NIS entities in a sector).

Information to be included in the report

Regarding the reporting of vulnerabilities under the national CVD framework, a report should include at least the following information, when available:

1	Asset or control where the vulnerability is found (web page, IP address, product or service name)
2	The version of the product on which the vulnerability is present, or the specific configuration of the product that is vulnerable
3	Discovered weakness (such as a CWE ([7]))
4	The severity of the vulnerability (e.g., using CVSS ([8]) to calculate)
5	A detailed description of the vulnerability, including the following information ○ A summary of the vulnerability ○ Required steps to reproduce the vulnerability ○ Required configuration to reproduce the vulnerability ○ Possible mitigation measures for the vulnerability
6	Potential impact of the vulnerability
7	Whether the vulnerability has already been reported to the product manufacturer
8	Whether a request for a CVE number has been made
9	Contact information, including secure communication options (PGP fingerprint, etc.)
10	Any other important information related to the discovered vulnerability

4.4. Offering recommendations to organisations to adopt their own CVD policy

In order to facilitate the development and adoption of CVD policies by vendors or system owners, national competent authorities should offer appropriate recommendations to organisation to adopt their own CVD, along with policy templates. In addition, vendors or system owners should be encouraged to follow existing standards in the development of such policies, where possible (see Section 5).

4.5. Leading by example

Public authorities can play a key role in promoting the adoption of CVD policies by adopting their own vulnerability handling and management procedures, including the implementation and publishing of their own CVD policies. Public authorities should require CVD processes to be used by their suppliers and also include CVD provisions in public procurement contracts. The adoption of a CVD policy should also become a standard security requirement for all public authorities.

4.6. Tools

Organisations should be encouraged to adopt in their CVD policies, where appropriate and possible, the use of tools to enhance the efficiency and effectiveness of the processes of discovering, reporting and managing vulnerabilities, along with facilitating the communication between the different parties involved in CVD. An indicative, non-exhaustive list of such tools is shown below.

- **Dedicated website.** A dedicated website can be used to publish and disseminate the CVD policy, such as the standardised security.txt ([9]). This will make it much easier to be located by reporters. In addition, a dedicated website can be used as a reporting platform for the submission of vulnerabilities. This will facilitate secure communication among the parties and streamline the submission of reports by asking for specific data from the reporters.
- **Ticketing system.** A ticketing system can greatly increase the processing speed of vulnerability reports by allowing for the efficient internal prioritisation and management of vulnerabilities. Moreover, the effective use of a ticketing system can ensure that all submitted vulnerabilities are processed instead of being overlooked.
- **Validation tools.** Such tools can support the automated, quick and effective verification of submitted vulnerability reports. This automated triaging, however, can mostly deal with certain easily categorised aspects of vulnerability reports, while a full verification will probably still need to be performed by humans.
- **Communication tools.** The use of communication tools can allow for secure information exchange and communication between the involved parties. It is important to note that any communication before the public disclosure of a vulnerability must be sufficiently protected and kept only between strictly involved individuals.
- **Other custom tools** to support the overall vulnerability treatment process.

4.7. Awareness-raising / communication campaign

An important part of the success of a CVD policy relies on raising awareness, dissemination activities and communication campaigns. This should be taken into account in the national cybersecurity strategy, considering the following elements as a minimum.

([9]) https://securitytxt.org/.

Short term (1 year)

- **Awareness-raising campaigns.** There should be frequent campaigns to raise awareness of the importance of dealing with vulnerabilities and the related reporting.
- **Dedicated events and activities.** These can include dedicated and targeted webinars or seminars, thematic conferences or workshops with authorities and organisations.
- **Development of non-financial gratification systems.** These may include, for example, merit recognition, awards, gadgets or internship programmes for those who report vulnerabilities.

Medium / long term (2 years+)

- **Trainings.** There should be provisions and incentives for the establishment of dedicated training programmes aiming to increase the availability of skills in cybersecurity and dealing with vulnerabilities. These programmes can be provided either by public entities (such as national cybersecurity centres or national competent authorities) or private organisations.
- **Increase awareness of security by design and security by default.** There should be appropriate training programmes on these topics.
- **Education programmes.** There should be provisions for the establishment of academic education programmes relating to cybersecurity and dealing with vulnerabilities, aiming to increase the supply of cybersecurity experts in the long run.
- **Workshops with authorities and organisations.** As above.
- **Financial reward programme / bug bounty programme.** The establishment and promotion of financial reward programmes or bug bounty programmes can help raise awareness on vulnerability research.
- **Collaboration activities.** Collaboration between interested stakeholders (including public and private organisations) should be developed in order to take advantage of accumulated expertise, shortages of resources or a lack of specialised IT systems. Other activities could include creating a platform for sharing information and experiences on CVD or developing solutions to enable the coordinator to influence organisations to remove vulnerabilities.

4.8. Cooperation at the national and international levels

Cooperation at the national and international levels could possibly be enhanced by the establishment of a national-level registry of ICT product and service vulnerabilities, exploitation status, availability of patches/updates and risk mitigation advice. Manufacturers should also consider disclosing fixed vulnerabilities to the upcoming European vulnerability database to be established under NIS2 and managed by ENISA, or under any other publicly accessible vulnerability database.
In addition, any cooperation at the national and international level should adhere to relevant legal obligation.

5. Recommendations to organisations for adopting CVD policies

This section aims to provide guidance and harmonisation to competent authorities to give recommendation to organisations to adopt their own CVD policies, with an indicative minimum content of such recommendations.

Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk. Entities that develop or administer network and information systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered ([10]).

These recommendations are also useful for essential and important NIS2 entities that have to apply, as part of their cybersecurity technical, operational and organisational risk-management measures, vulnerability handling and disclosure measures ([11]).

5.1. Defining the CVD policy

(a) Authorisation to perform cybersecurity testing

The policy must be developed and published by entities or bodies that can validly represent the vendor or system owner and give the appropriate authorisation, and not, for example, by a member of the IT team who is not legally authorised to do so. This appropriate level of implementation will give researchers and reporters the necessary assurances and legal protection to perform their work.

(b) Policy scope

The vendor or system owner must explicitly define clearly which systems and services are in scope for the CVD policy. In this exercise, the vendor or system owner should also take into account their supply chain and contractual commitments.

The CVD policy must explicitly list systems or services provided by third parties that are excluded from the scope of the policy. In case of doubt about the scope, reporters should seek the approval of the vendor or system owner before starting their cybersecurity researches.

(c) Points of contact

The CVD policy must include detailed steps and contact information, to which any report or information on vulnerabilities can be sent. A specific email address can be used for this purpose. The responsible authority or organisation must also ensure that all other communications on vulnerabilities received from other channels are internally redirected to this contact point.

The use of an online form is also an effective way to receive information about discovered vulnerabilities. This method has the advantage that the input and processing of data and the sending of an acknowledgement of receipt can be done automatically.

In addition, it may be useful to mention contact details of the service or person authorised to deal with notifications about the vulnerabilities report.

([10]) Recital 58 of NIS2.
([11]) Article 21(1) and Article 21(2)(e) NIS2.

Lastly, the specific items of information to be provided should be clearly stated in the policy.

(d) Proportionality and necessity of the actions

In general, the reporter must commit to complying with the principle of proportionality, i.e. not to disrupt the availability of the services provided by the system and not to exploit vulnerabilities beyond what is strictly necessary to demonstrate the security problem. Their approach must remain proportionate: if the problem has been demonstrated on a small scale, no further action should be taken. Furthermore, the reporters should carry out their activities with regard to protecting information and assets from misuse, alteration, theft or destruction.

In addition, the CVD policy should clearly state that the reporter may not keep the data of the vendor or the system owner, including any personal data, longer than necessary. All personal data collected by the reporter must be deleted immediately. If it proves necessary to retain these data for a certain period of time, the reporter must ensure that they are kept secure during this period.

The policy shall make clear what actions would be considered disproportionate, unnecessary or forbidden (to clarify expectations).

(e) Acting in good faith

The vendor or system owner must undertake to carry out their coordinated disclosure policy in good faith and not to bring civil or criminal proceedings against the reporter complying with its terms.

On the part of the reporter, there can be no fraudulent intent, intent to harm or desire to use or cause harm to the visited system or its data.

(f) Confidentiality

One of the essential elements of a CVD policy should be the respect for confidentiality: reporters may not share the information collected with third parties (except with the CSIRT designated as the coordinator or national competent authorities) or disseminate it to the public without the express consent of the vendor or system owner.

The text of the coordinated disclosure policy should state that the purpose of the policy is not to permit deliberate access to the data of the system, including potential personal data. Such access can only occur incidentally in the context of the detection of vulnerabilities in the technologies concerned.

(g) Processing of personal data

The purpose of a CVD policy is not to allow the intentional processing of personal data. However, it is possible that the reporter may, even inadvertently, have to process personal data in the context of their vulnerability researches.

The processing of personal data has a broad meaning and includes in particular the storage, alteration, retrieval, consultation, use or disclosure of any data relating to an identified or identifiable natural person. The ‘identifiable’ nature of the person does not depend on the mere desire to identify the data processor, but on the ability to identify the person directly or indirectly from these data (for example: an email address, identification number, online identifier, IP address or location data).

The controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing.

Since a CVD policy constitutes a form of accession agreement that binds the researcher to the

vendor or system owner, it is necessary to specify in writing the obligations of the parties with regard to the processing of personal data, in particular the purposes of and the essential means for any processing carried out under this policy (e.g. limit the processing of personal data only to what is necessary to prove the existence of a vulnerability and apply encryption to those data).

(h) Rewarding the reporter

There are different types of reward possibilities for organisations, as shown below.

- A **vulnerability reward programme** (also VRP or bug bounty) is an explicit financial reward for a vulnerability report by an organisation. It is sometimes limited in time and the financial reward to the reporter depends on the amount, importance or quality of the information transmitted.
- A **recognition programme** offers reporters an opportunity to receive public recognition for a reported vulnerability. Recognition could take the form of a ranking of the best reporters, publications, blog posts or a Hall of Fame offered by an organisation. For organisations, implementing such a programme offers the advantage that no notable resources or budget are needed.
- **A gift programme** rewards a reporter with a physical item, for example a t-shirt or a special coin. Upon receiving a physical item, the reporter has the opportunity to share this event online (e.g. on Twitter or YouTube) and inspire others to report a vulnerability to the organisation.

Based on the resources and budget an organisation should evaluate if and what type of reward programme it can offer. Implementing a reward program can increase the attraction to potential reporters and often leads to more results for the organisation.

Rewards or public recognition (such as a ranking among reporters) given by the vendor or the system owner makes the CVD policy more attractive for the reporters and often leads to better results for the organisation. It may even be a purely symbolic gift, such as a t-shirt, a sticker or a special mug.

In a bug bounty programme, the reward depends on the quantity, importance or quality of the information transmitted.

It is essential that the responsible vendor or system owner clearly states the nature of this reward in advance in its policy. Any request for a reward outside the conditions set by the CVD policy can then be equated with an illegal attempt at extortion.

In organising bug bounties, most organisations can benefit from using a bug bounty platform, which will coordinate the technical and administrative aspects of its reward programme with the organisation.

5.2. Modalities

(a) Publicity of the policy

The publicity given to the responsible disclosure policy is an important element for its success. Its content should therefore be easily accessible to potential reporters and should preferably be accessible from the website of the vendor or the system owner. The existence of the CVD policy must therefore be clearly and visibly stated on the website of the vendor or the system owner (e.g. with a specific tab or a section with the full content of the policy). For this purpose, there is a draft

IETF internet standard, called 'security.txt' ([12]), that describes a text file which holds all the relevant details of an organisation's CVD policy, and can be placed in a known location in the web root so it can be easily found.

If a vulnerability rewards programme is introduced via a bug bounty platform, the full content of the CVD policy must also be included on that platform.

The CVD policy must be written in all languages of the website and, to the extent possible, also in English. It may also be useful to place a link to the CVD policy page in other locations (e.g. in the help section of the programme, the user manual and the user license).

Finally, it is important for the responsible vendor or the system owner to inform any subcontractors about the content of its CVD policy and to adapt its contractual engagements if necessary.

(b) Secure communication channels

In order to prevent information leakage on newly discovered vulnerabilities, the confidentiality and integrity of communications should be adequately protected.

It is therefore strongly recommended to use a secure method of communication. This can include the use of a data encryption tool ([13]), creating a secure internet portal, or even password-protecting the documents ([14]). When developing the communication methods recommended to reporters, the responsible authority or organisation must therefore pay particular attention to their security ([15]).

(c) Effective cooperation

Good cooperation requires continuous and efficient communication. The information provided by the reporter can be very useful in identifying the vulnerability and resolving it. It is therefore important to send acknowledgements of receipt, to keep reporters informed of the follow-up given to their notification, to remind them of their obligations and to specify the next steps in the procedure.

In addition, the intervention of a coordinator or a bug bounty platform can help to establish and maintain a constructive relationship between the parties, or possibly guarantee the anonymity of reporters.

(d) Information reporting requirements

The CVD policy must clearly state what information the reporter must provide when submitting a vulnerability report. This information might include items such as type of vulnerability, configuration details, actions taken, tools used, test data, evidence, IP address or URL of the affected system, screenshot and contact details. The reported information should also be aligned with the recommendations of the national CVD framework (see Section 4.3)

(e) Deadlines

It is recommended that clear and adequate deadlines be set for each stage of the procedure, in

([12]) See the project https://securitytxt.org.
([13]) For example: Transport Layer Security or its predecessor Secure Sockets Layer, Secure Multipurpose Internet Mail Extensions and Pretty Good Privacy.
([14]) Ideally, the reporter should then provide the password to the responsible organisation via another means of communication (telephone, SMS, message application, other email address, etc.).
([15]) For example, provide the public key and fingerprint of its contact point to send information in an encrypted manner, or secure its online form in HTTPS.

particular for sending an acknowledgement of receipt to the reporter, requests for communicating additional information, progress reports of vulnerability analysis, developing a solution, replying to the reporter, awarding a reward or any publication. However, deadlines should remain flexible to a certain extent, depending on the complexity of the vulnerability, the number of systems affected, the urgency or the criticality of the situation.

(f) Potential public disclosure

Any disclosure of a vulnerability should be coordinated and synchronised between the parties, in cooperation with the designated CSIRT, to allow sufficient time for the responsible vendor or system owner to resolve the issue and to inform affected critical operators in advance.

In case multiple vendors and/or system owners are affected by the identified vulnerability, there should be a coordinated process of informing all concerned parties before proceeding with publication.

The same applies where the identified vulnerability threatens to affect other organisations using similar technology more widely, or where the affected IT component is provided by the vendor or the system owner to other organisations (e.g. through user licenses). In these cases, it is essential that a report on the vulnerability and its resolution be provided to the parties concerned so that they can protect themselves.

In case of disclosure to the public, the vendor should prioritise its official customer communication channels, and at the same time offer the relevant patch or mitigation measure.

(g) Vulnerability treatment

The vendor should determine how the vulnerability can be remediated comprehensively, how to reduce the impact of successful exploitation of the vulnerability, or how to reduce exposure. In making this decision, the vendor should attempt to balance the need to create a remediation quickly, with the overall testing required to ensure the remediation does not negatively impact affected users due to quality issues. In addition, the vendor should provide support and communication towards customers to facilitate the overall process of patching and vulnerability management.

The system owners should be responsible for managing vulnerabilities, including checking the latest information on vulnerabilities, testing and applying patches or mitigation measures.

(h) Multi-party CVD process

In many cases, a product or service can be dependent on other products or services, so vulnerabilities in upstream supply chain dependencies can also affect another vendor’s products and services. Vendors should track all upstream dependencies and vulnerabilities to determine whether their own products or services are affected. Vendors should obtain vulnerability information, including remediation advice, from their upstream vendors, including in cases of use of open-source software. Vendors should also provide regular vulnerability information, including remediation advice, to their downstream customers and users.
Vendors should consider publishing machine-readable descriptions of their upstream dependencies to their customers using commonly available standards.

6. Sources and references

- **ENISA**
    - *Good Practice Guide on Vulnerability Disclosure – From challenges to recommendations*, 2015, https://www.enisa.europa.eu/publications/vulnerability-disclosure.
    - *Overview of National Vulnerability Disclosure Policies in the EU,* 2021*,* https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu
    - *Coordinated Vulnerability Disclosure Policies in the EU*, 2022, https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu.
    - *Developing National Vulnerabilities Programmes*, 2023, https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes.

- European Telecommunications Standards Institute (2022), *Cyber Security: Guide to Coordinated Vulnerability Disclosure*, ETSI TR 103 838, https://www.etsi.org/deliver/etsi_tr/103800_103899/103838/01.01.01_60/tr_103838v010101p.pdf.

- FIRST (2020), *Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure*, Version 1.1, https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1.

- Global Forum on Cyber Expertise (2017), *GFSE Global Good Practices – Coordinated Vulnerability Disclosure (CVD)*, https://thegfce.org/wp-content/uploads/2020/06/CoordinatedVulnerabilityDisclosure-1.pdf.

- Householder, A. D., Wassermann, G., Manion, A. and King, C. (2017), *The CERT Guide to Coordinated Vulnerability Disclosure*, Software Engineering Institute, Carnegie Mellon University, https://insights.sei.cmu.edu/library/the-cert-guide-to-coordinated-vulnerability-disclosure-2/.

- ISO (2020), *ISO/IEC 29147:2020, Information technology – Security techniques – Vulnerability disclosure*.

- ISO (2020), *ISO/IEC 30111:2020, Information technology – Security techniques – Vulnerability handling processes*.

- NIST (2023), *Recommendations for Federal Vulnerability Disclosure Guidelines,* NIST Special Publication (SP) 800-216, https://csrc.nist.gov/pubs/sp/800/216/final.

- Organisation for Economic Co-operation and Development, *Encouraging Vulnerability Treatment: Overview for Policy Makers'* OECD Digital Economy Papers, No. 307, February 2021, https://www.oecd-ilibrary.org/science-and-technology/encouraging-vulnerability-treatment_0e2615ba-en.

- Organization for Security and Co-operation in Europe, *Confidence building measures No 16 (CBM) Vulnerability policies*, https://www.osce.org/cyber-ict-security

- Pupillo, L., Ferreira, A. and Varisco, G. (2018), *Software Vulnerability Disclosure in Europe – Technology, Policies and Legal Challenges*, CEPS, https://www.ceps.eu/download/publication/?id=10636&pdf=CEPS%20TFRonSVD%20with%20cover_0.pdf.

- Security.txt (https://securitytxt.org/). A proposed standard which allows websites to define security policies