CENTRE FOR
CYBER SECURITY
BELGIUM

GUIDE TO COORDINATED VULNERABILITY DISCLOSURE POLICIES

PART I: GOOD PRACTICES

COORDINATED VULNERABILITY DISCLOSURE POLICIES -"CVDP"
RESPONSIBLE DISCLOSURE POLICIES -"RD

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de Loi,16
1000 Brussels

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

A. TABLE OF CONTENTS

CENTRE FOR
CYBER SECURITY
BELGIUM

Warning:

This guide provides an overview of the concepts, objectives, legal issues and good practices surrounding the adoption of coordinated vulnerability disclosure policies ("CVDP") in the current state of Belgian legislation - see the examples on the CCB website.

We would like to point out that the documents drawn up by the CCB in no way change the existing legal rules. Unauthorized intrusion into a third party's computer system, even with good intentions, is a criminal offence.

Participants in a CVDP must be aware that they cannot invoke a general exclusion of liability when participating in that policy: they must act prudently and scrupulously comply with all the conditions of the policy as well as the applicable legal provisions.

** Shutterstock - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

B. INTRODUCTION

I. Background

The increasing importance of information systems in our society significantly increases the risk of incidents related to the security of these systems. These incidents can, for example, compromise the availability of a particular service or the integrity, authenticity or confidentiality of data. As more and more devices are being used that are connected to the Internet, any incident will have even greater consequences.

As far as the causes of these incidents are concerned, vulnerabilities pose a major risk. However, this risk is inherent in the development, use and update process of these systems. Taking into account the extent and technicality of this problem, it seems an illusion to believe that all device manufacturers or those responsible for IT systems will be able to solve it on their own.

An organisation may choose to rely on a particular company to verify the security of its information systems (e.g. through a security audit), or, publicly, on persons with good intentions ("*ethical hackers*") who wish to contribute to improving the security of these technologies by identifying existing vulnerabilities and helping to resolve them.

II. Concepts

A. *A coordinated vulnerability disclosure policy*[1]*(CVDP)* is a set of rules pre-determined by an organisation responsible for IT systems that allows participants[2] (or "*ethical hackers*"), with good intentions, to identify possible vulnerabilities in its systems, or to provide it with all relevant information about them. These rules, usually published on a website, make it possible to define a legal

[1] Also called "responsible disclosure policy": we prefer the term "coordinated" rather than "responsible" as it avoids any confusion with the concepts of civil liability and emphasizes the reciprocal nature of the process.
[2] These could be, for example, cyber security researchers or users. Participants may be subject to selection by a third party who acts as a confidential adviser ("coordinator").

framework for the cooperation between the responsible organisation and participants under the policy. These rules should ensure, inter alia, the confidentiality of the information exchanged and provide a responsible and coordinated framework for any disclosure of discovered vulnerabilities.

Thus, the term 'disclosure' does not necessarily mean that the vulnerability is made public, but rather that the participant communicates it to the responsible organisation. The participant is obliged to communicate the vulnerability to the responsible organisation, but the public disclosure of the vulnerability (by the participant or the organisation concerned) is optional in the context of a CVDP.

B. ***A vulnerability***[3] is a flaw or a weakness, a design[4] or execution error[5] the lack of updates in light of existing technical knowledge, which may affect IT security.[6] A vulnerability can lead to an unexpected or unwanted event and be exploited by malicious third parties to harm the integrity, authenticity, confidentiality or availability of a system[7]or to damage a system.

[3] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, p. 14, item 2.2, www.enisa.europa.eu/publications/vulnerability-disclosure.

[4] For example, an error or omission in the design of a system or protocol that makes it intrinsically vulnerable.

[5] For example, an error during implementation, configuration or use.

[6] For example, a system, network, process, program, application, service, protocol or component.

[7] Or the information it contains.

C. ***A responsible organisation*** is a natural person or legal entity who manages, owns, sells or manufactures systems or products related to IT and is responsible for their security and proper functioning.

D. ***CVDP participant*** [8] ***(or "ethical hacker***") is a person with good intentions who, with the consent of the responsible organisation, wishes to contribute to improving the security of IT systems. They may, for example, carry out pentests or use other methods to check the security of information systems. This is completely different from *hackers* who use their skills to illegally break into systems with bad intentions[9]. Participants want to inform the IT manager or coordinator of any vulnerabilities discovered, so that they can be eliminated.

E. ***A coordinator*** is a natural person or legal entity who acts as an intermediary between the participants and the organisation in charge of an IT system by providing logistical, technical and legal assistance or other functions[10] to facilitate cooperation. If no CVDP coordinator is appointed, the Centre for Cybersecurity Belgium (vulnerabilityreport@cert.be) can fulfil this role.

F. ***A Vulnerability Rewards Program (or bug bounty program)***[11] relates to all rules set by a responsible organisation to give rewards to participants who identify vulnerabilities in the technologies it uses. This reward can be a sum of money, but also a gift or simply public recognition (ranking among the best participants, publication, conference, etc.). This is a coordinated vulnerability disclosure policy that provides for a reward to be paid to the participant according to the amount, importance or quality of the information transmitted.

[8] Sometimes called "white hats", as a reference to the fact that heroes in American westerns usually wore white hats.
[9] Sometimes called "black hats", as a reference to the fact that bad guys in American westerns usually wore black hats.
[10] For example, to review the vulnerability reports or as mediator.
[11]« Program de récompense pour la découverte de vulnérabilités » in French or « beloningsprogramma voor het opsporen van kwetsbaarheden » in Dutch.

This policy is more attractive to potential participants and often leads to better results for the organisation. The organisation may, for example, use a *bug bounty platform* that provides technical and administrative assistance to manage of its vulnerability detection reward program (coordinator role).

III. Goals

a. To provide a legal framework for useful, fair, effective, legal and budget-friendly cooperation

When an organisation uses a particular external service provider to check the security of its IT systems, it enters into a security audit agreement which may include pentests (or "penetration tests"), simulating an attack by persons with malicious intentions, to demonstrate existing vulnerabilities. In that case, the mutual legal obligations of the parties are, in principle, described in a specific agreement or general terms and conditions[12].

However, this is not always the case when an organisation wants to co-operate with unspecified individuals *(*participants or ethical hackers) who can identify vulnerabilities in its IT systems. In that case, there is no clear contractual framework between the parties. It is then necessary for the organisation to define its expectations and the legal obligations of the participants prior to each cooperation.

In this respect, the coordinated vulnerability disclosure policy is a type of accession agreement outlining all contractual provisions for the responsible organisation and subsequently accepted by the participant when it freely decides to participate in the program.

[12]The responsible organization can also entrust these tasks to certain employees. The respective obligations of the parties will then be described in specific internal regulations or in general employment contract.

The adoption of such a policy clarifies the participants' legal position. After all, they can demonstrate that they have prior authorization to access the IT systems concerned and therefore do not intrude into those systems unlawfully, provided that the conditions set out in the policy are met *(see Coordinated Vulnerability Disclosure Policies Guide. Part II: Legal aspects*).

This cooperation can provide the responsible organisation with fair and lawful information about vulnerabilities in its systems and enable it to take adequate and timely action. In this way, potential risks and harm that these vulnerabilities may cause can be prevented or mitigated as effectively as possible.

The coordinated vulnerability disclosure policy provides an opportunity for continuous and effective monitoring of the security of systems or equipment. Obviously, the policy is more attractive and effective when the responsible organisation decides to give rewards to participants, depending on the importance and quality of the information provided (as part of a Vulnerability Rewards Program or bug bounty program[13]).

Even when the organisation grants rewards and calls on an external coordinator (ethical hacking platform), setting up costs of a coordinated vulnerability disclosure policy are more budget-friendly than having external companies perform audits.[14] After all, the reward for a bug bounty program is the result of a commitment on the part of the participant to achieve a certain result, whereas an external auditor is usually only bound by a commitment of means. The latter must therefore be compensated for all their activities, even if they have not found any vulnerabilities or only minor vulnerabilities at the end of their investigation.

[13] In addition to a vulnerability rewards program, the responsible organization may still decide to give a reward to participants following the procedure.
[14] Some costs need to be budgeted for, such as the costs for the technical team needed to analyze the information provided by the participants.

b. Improving the security of IT systems and driving research

Introducing such a policy provides the responsible organisation with the opportunity to obtain information about the security of its IT systems from various sources. Taking into account the current complexity and technically advanced nature of these systems, it is very useful to involve a large number of potential experts instead of using a few external service providers who cannot be experts in all the technologies used by the organisation.

In addition to other technical and organisational measures, setting up such a cooperation may be an appropriate measure to prevent incidents that would compromise the security of its network and information systems. It has the undeniable advantage of identifying and resolving vulnerabilities before a security incident occurs.

Improved security can be achieved by addressing vulnerabilities, minimising the risks associated with certain vulnerabilities and continually evaluating these risks to the responsible organisation's IT systems.

The introduction of a CVDP obviously implies that the organisation has security measures that can be tested and an internal (or external) team that can follow up the information provided by the participants.

In addition to increasing security, this type of policy can also improve knowledge about cyber security and drive research in this field. The work of researchers makes it possible to identify new vulnerabilities, as well as the circumstances in which they occur, methods for avoiding them and the means of remedying them.

c. Ensuring users have confidence in IT technologies

Implementing a CVDP demonstrates to the public and users that the responsible organisation attaches great importance to the security of its IT technologies.

After all, this approach implies a commitment by the organisation to process the information provided by the participants and to try to remedy the vulnerabilities identified, or at least to inform the users of the risks.

This commitment can also be a marketing tool. The organisation can refer to this in its communication. Trust in IT systems is certainly an important bonus for users or consumers.

d. Guaranteeing confidentiality

The confidentiality of information concerning a vulnerability in an IT system must be guaranteed as far as possible.

Full disclosure of a vulnerability[15], while it still exists among many users, poses a major IT security risk. Indeed, third parties with bad intentions can develop and disseminate specific tools to exploit this vulnerability.

[15] A disclosure to the general public.

It is therefore not desirable to make a security problem public before it has been resolved by the responsible organisation, which should be given the necessary time to do so, or before the responsible organisation has been able to inform the authorities responsible for the security of network and IT systems[16] about it.

Full disclosure may also delay the effective application of a solution for the vulnerability, as the responsible organisation is forced to respond in a crisis situation.

Disclosing security problems may also harm the reputation of the responsible organisation and undermine user confidence in the technologies concerned.

In addition, the dissemination or making available to the public of IT data, such as software or instructions, that make it possible to penetrate the security of IT systems may be a criminal offence[17] or may involve the civil liability for the person who published the information[18] *(see Guide - Part II Legal Aspects*).

Consequently, public disclosure of information about a vulnerability must be made with the utmost care and in coordination with the responsible organisation.

[16] In Belgium, this role is played mostly by the Centre for Cyber Security Belgium (CCB). Where appropriate, the CCB may inform organizations of vital interest (public authorities, providers of essentials services, digital service providers, critical infrastructures, etc).
[17] Art. *550 bis)* § 5 of the Belgian Criminal Code.
[18] Art. 1382 of the Belgian Civil Code.

The responsible organisation must respond within a reasonable period of time: it will implement a solution or at least inform the IT systems' users affected by the vulnerability. After all, the organisation may, for example, be held liable for leaving its customers in the dark about the vulnerability (see item e below).

It may also prove very useful, once the main security risks have been eliminated, to publish information on the vulnerabilities detected and their resolution, in an appropriate framework[19], in order to advance research on IT security.

The interest of a CVDP therefore lies in the establishment of a legal framework that reinforces confidentiality and provides the best possible framework for a possible public disclosure.

e. Ensuring better compliance with legal obligations in the area of IT security

By implementing a coordinated disclosure policy, the organisation demonstrates its commitment to comply with its legal obligations to ensure the security of its network and IT systems: General Data Protection Regulation EU No 2016/679 ("GDPR"), Act of 7 April 2019 establishing a framework for the security of network and IT systems of general interest for public security ("NIS Act"), Civil Liability Regulation, Economic Law Code, etc.

Article 32 of the GDPR provides that the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented, taking into account the state of the art and the cost of their implementation, as well as the nature, scale, context and purposes of the processing operations and the risks to the rights and freedoms of natural persons (which vary in their likelihood and seriousness).

[19] For example, in scientific publications or technical reports distributed to researchers in the area of IT security.

The provision clarifies that the controller and the processor may use:

(a) pseudonymisation and encryption of personal data;
(b) the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on a permanent basis;
(c) the ability to restore timely availability of and access to personal data in the event of a physical or technical incident;
(d) a procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the security of processing.

In its Recommendation on security measures to prevent data breaches (No 01-2013), the Belgian Commission for the Protection of Privacy (now Data Protection Authority) recalls the importance of documenting, monitoring and improving IT security measures as often as necessary[20].

The guidelines on information security for personal data issued by the former Belgian Commission for the Protection of Privacy also point out that the controller should regularly organise a proper information security audit of personal data and take management measures to ensure the confidentiality and integrity of the data.[21]

[20] Commission for the Protection of Privacy, Recommendation on security measures to be observed to prevent data breaches (No 01-2013), www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf, p. 3, point 6.
[21] Commission for the Protection of Privacy, *Guidelines on information security of personal data*, (version 2.0 Dec. 2014), p. 20 and 27, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Richtsnoeren_CBPL_V%202%200%20FR_TRA.pdf.

The implementation of a CVDP is an appropriate technical and organisational measure to demonstrate, among other measures, the controller's commitment to ensuring the confidentiality, integrity, availability and resilience of his processing systems on a permanent basis[22] and to regularly test, assess and evaluate the effectiveness of the processing security measures[23]. Moreover, the international technical standards on IT security explicitly recommend the implementation of a CVDP (see, for example, international ISO/IEC standards 29147[24] and 30111[25]).

The responsible organisation can then rely on its CVDP to demonstrate to the personal data supervisory authorities that it is making efforts to assess and manage the risks associated with vulnerabilities in its IT systems.

In the same vein, a CVDP allows the controller to be better informed of possible personal data breaches and to assess which breaches should be reported as soon as possible to a supervisory authority[26] or a natural person[27].

Also, article 20 of the Belgian NIS Act states that the operator of essential services ("OES") must "take appropriate and proportionate technical and organisational measures to manage the risks to the security of the network and information systems on which its essential services depend. These

[22] Art. 32 (1) (b) of the GDPR.
[23] Art. 32 (1) (d) of the GDPR.
[24] ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (https://www.iso.org/standard/72311.html).
[25] ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html).
[26] Art. 33 of the GDPR provides that the controller must notify personal data breaches to the competent supervisory authority without undue delay and, if possible, no later than 72 hours after becoming aware of them, unless such breaches are not likely to jeopardize the rights and freedoms of natural persons. The processor should also inform the controller without delay as soon as they become aware of a personal data breach.
[27] Art. 34 of the GDPR requires the controller to notify the data subject without delay of a personal data breach where the breach is likely to pose a great risk to the rights and freedoms of a natural person.

measures shall ensure a level of physical and logical security of network and information systems appropriate to the risks presented, taking into account the state of technical knowledge".

The OES must also "take appropriate measures that are appropriate to prevent or minimise incidents affecting the security of the network and information systems used for the provision of essential services in order to ensure the continuity of these services"[28].

Security measures are defined in the NIS Act as measures that enable a system, with a certain degree of reliability, to withstand actions that compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by or accessible via those network and information systems[29]. In order to take appropriate measures commensurate with the risks involved, [30]the risks associated with incidents should be identified and their impact on the security of network and information systems must be minimised.

In this case, the implementation of a CVDP enables the AED or digital service provider to have a better understanding of possible vulnerabilities and threats to its network and information systems in order to provide an adequate response to the requirements of the NIS Act.

[28] Art. 20 of the NIS Act; see also art. 33 of the NIS Act for the security measures of digital service providers (DSPs) - e.g. providers of cloud computing services.
[29] Art. 6, 9°, of the NIS Act.
[30] Art. 6, 15°, of the NIS Act defines the risk as 'any reasonably foreseeable circumstance or event with a potential negative impact on the security of network and information systems'.

In addition, the Cyber Security Act[31] provides that a European cybersecurity certification scheme should at least include rules concerning how previously undetected cybersecurity vulnerabilities in ICT products[32], ICT services[33] and ICT processes[34] are to be reported and dealt with.[35]

The Regulation requires thus manufacturers or providers of certified ICT products, ICT services and ICT processes to make publicly available information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers.[36]

In addition, the responsible organisation may be held civilly liable (contractually or extra-contractually) if a security flaw in its technologies has caused harm to a third party.[37]

Finally, the responsible organisation selling ICT systems must guarantee its customers against hidden defects or non-conformity of the goods sold.[38] As a manufacture of a product (physical object) or provider of a service, it may also only market safe products and provide safe services.[39]Compliance with that general safety obligation may be assessed taking into account national or international standards, the codes of conduct in force in the industry concerned, the current state of knowledge and the state of the art and the security which users may reasonably expect.[40]

---

[31] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Cybersecurity Agency), and on the certification of cybersecurity of information and communication technologies and repealing Regulation (EU) No 526/2013.
[32] An element or group of elements of a network or information system (art. 2, 12 of the Cyber Security Act).
[33] A service which consists wholly or mainly in the transmission, storage, retrieval or processing of data by means of network and information systems (Art. 2, 13 of the Cyber Security Act).
[34] A series of activities carried out to design, develop, deliver or maintain an IT product or service (art. 2, 14 of the Cyber Security Act).
[35] Art. 54, 1, m, of the Cyber Security Act.
[36] Art. 55, 1, c, of the Cyber Security Act.
[37] Art. 1382 of the Civil Code.
[38] See art. 1641 and 1625 of the Civil Code on the indemnity for hidden defects or art. 1649 *bis et* seq. of the Civil Code on the indemnity for lack of conformity for sales to consumers.
[39] See Article IX.2 et seq. of the Code of Economic Law.
[40] In the absence of harmonized European standards.

C. GOOD PRACTICES

Currently, many companies in Belgium already apply a coordinated vulnerability disclosure policy and use bug bounty platforms.

There are two international ISO/IEC standards on CVDP: ISO/IEC 29147[41] and ISO/IEC 30111[42]. The first describes the procedure for disclosing a vulnerability, while the second deals with the processing procedures for the reported vulnerability. These two standards describe a complete model with the different aspects of a CVDP.

ENISA (European Union Cybersecurity Agency) has also published recommendations on good practices regarding the introduction of a CVDP.[43]

[41] ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (https://www.iso.org/standard/72311.html).

[42] ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html).

[43] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure. Art. 6 (1) (b) of Regulation (EU) 2019/881, tasks ENISA with assisting the Member States of the Union and the European institutions in drawing up and implementing a voluntary disclosure policy on vulnerabilities.

** Colored-security-background-flat-design Free license - Designed Freepik - 2020*

I. Content of a CVDP

a. Authorized persons

The policy must be implemented by persons or bodies that can validly represent the responsible organisation and not, for example, by a member of the IT team who is not legally authorized to do so[44].

[44]Subject to the doctrine of sham representation or to the general legal principle of respect for the legitimate expectations of the other.

Indeed, the authorizations provided under the coordinated disclosure policy must necessarily come from a person authorized to do so by the holder of the rights to the system or equipment concerned[45].

b. Publicity

The publicity given to the responsible disclosure policy is an important element for its success[46]. Its content should therefore be easily accessible to potential participants and should preferably be accessible from the website of the responsible organisation. The existence of the CVDP must therefore be clearly and visibly stated on the website of the responsible organisation (e.g. with a specific tab or a section with the full content of the policy)[47]. For this purpose, there are standardisation proposals where an organisation's CVDP is included in a "security.txt" file in a known location of the tree structure of each website[48] or extensions for web browsers to track down websites that have a CVDP[49].

If a Vulnerability Rewards Program is introduced via a bug bounty platform, the full content of the CVDP must also be included on that platform[50].

The CVDP 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 CVDP page in other locations (for example, in the help section of the program, in the user manual, in the user licence, etc.).

[45] By default, this is the system's owner.
[46] In order to prevent a crime from being committed (unauthorized intrusion into an IT system), the coordinated disclosure policy must be in place before participants take steps. The best way to avoid doubts about the existence or not of a coordinated vulnerability disclosure policy is to make it public. (See Part II. Legal aspects). However, organizations may have a non-public CVDP limited to a few pre-selected participants (see in particular some private bug bounty programs).
[47] For example: https://www.[organisatie].be/security or /disclosurepolicy or /vulnerability-policy.
[48] See the project https://securitytxt.org/
[49] See for example the YesWeHack VDP Finder extension for Chrome and Firefox.
[50] For example, www.intigriti.be; www.yeswehack.com; www.bugcrowd.com; www.hackerone.com.

Finally, it is important for the responsible organisation to inform any subcontractors about the content of its CVDP and to adapts its subcontracting contracts if necessary.

c. Point of contact

The responsible organisation must include a contact point in its policy, to which any information on vulnerabilities can be sent. A specific e-mail address can be used for this purpose[51]. The responsible organisation must also ensure that e-mails received at other e-mail addresses[52] are forwarded internally to this contact point.

The use of an online form is also interesting 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 the telephone details of the service or person authorized to deal with notifications about IT vulnerabilities.

Lastly, the information to be provided by the participant should be clarified (see Section II Procedure below).

[51] For example: vulnerabilitypolicy@organisation.com; security@organisation.com; csirt@organisation.com; support@organisation.com; security-alert@organisation.com, etc.
[52] For example: info@organisation.com or contact@organisation.com.

d. Security and confidentiality of communications

This is crucial as risks of information leakage on vulnerabilities should be avoided as much as possible by ensuring the confidentiality and integrity of communications.

It is therefore strongly recommended to use a secure method of communication. This can include the use of a data encryption tool[53] creating a secure internet portal[54]or at least password-protecting the documents[55]. When developing the communication methods recommended to participants, the responsible organisation must therefore pay particular attention to their security[56].

e. Description of mutual obligations

1. Policy scope

The responsible organisation must explicitly define the scope of its coordinated disclosure policy: which sites, products, devices, services, systems or networks are in scope for the policy?

Ideally, the responsible organisation should apply the rules of its CVDP to its various IT systems and to its contractual commitments (suppliers, clients, subcontractors, staff, etc.).

If this is not the case, the CVDP must explicitly list IT systems of third parties that are excluded from the scope of the policy (in the absence of the consent of these third parties). In case of doubt about the scope of the CVDP, participants should seek the approval of the responsible organisation before continuing their analysis.

---

[53] For example: Transport Layer Security (TLS) or its predecessor Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP).
[54] in HTTPS or via encryption in the web browser.
[55] Ideally, the participant should then provide the password to the responsible organization via another means of communication (telephone, SMS, message application, other e-mail address, etc.).
[56] 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.

Also, the CVDP should clearly state that the participant's research on information systems not explicitly included as part of the policy could lead to legal action against the participant (by the public prosecutor, the responsible organisation or third parties to the CVDP).

2. Policy conditions

The very existence of a coordinated vulnerability disclosure policy or a bug bounty program necessarily implies that - at least tacitly - authorization to access the computer system has been granted to the participant[57]. In principle, the participant also has an authorization to enter data into the system concerned or to attempt to do so (see *Guide - Part II Legal Aspects*).

The responsible organisation must, however, clearly state in its coordinated disclosure policy the conditions under which participants may access the computer system and attempt to enter or modify data. The actions that may or may not be authorized must be clearly defined, based on the intended purposes.

The authorization to modify or delete IT data[58] depends on the way in which the coordinated vulnerability disclosure policy has been drawn up. In drawing up this policy, the responsible organisation must assess the benefits, the specific conditions imposed, and the risks involved in order to decide whether or not to allow these actions. It should be noted that participants have to strictly adhere to the terms of the policy on changing and deleting IT data. If not, they are guilty of a crime, i.e. an offence relating to IT data.

[57] The coordinated vulnerability disclosure policy will include provisions which, depending on their exact wording, may be considered as explicit or tacit authorizations.
[58] Or to try such actions.

For example, it is good practice to prohibit participants from using Distributed Denial of Service (DDoS) attacks or social engineering attacks, installing malware or viruses, stealing passwords, sending phishing or spam mails, removing or altering data/parameters from the system, etc.

The CVDP must expressly exclude any deliberate attempt[59] to intercept, record or become aware of communications that are not accessible to the public or electronic communications.[60] Nevertheless, it may be permitted for the content of communications to be disclosed to participants, in a strictly accidental manner, for the purposes of vulnerability detection[61]

It should also be stated that the participant may not use, retain, divulge or disclose any communication that is not accessible to the public, nor any data from an IT system which it has reasonable grounds to believe has been obtained illegally.

It should also be prohibited for participants to install or have installed a device enabling the interception, knowledge or recording of communications not accessible to the public, unless they can prove that they have no intention of using the device in question for the aforementioned purposes, either with the consent of all participants in the communication or by participating in the communication himself.

3. Reporting

The CVDP must clearly state what information the participant must provide when reporting a vulnerability: type of vulnerability, configuration details, actions taken, tools used, test data, evidence, IP address or URL of the affected system, screenshot, contact details, etc.

[59] Which is different from accidental interception (see Guide Part II Legal Aspects).
[60] Except in the rather exceptional case where the participant has the consent of all participants or participates in the electronic communication himself.
[61] See the confidentiality of electronic communications (Act of 13 June 2005).

4. Proportionality

In general, the participant 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.

If the use of personal data by the participant is not necessary to demonstrate IT vulnerability, it must be expressly excluded.

In addition, the Coordinated Disclosure Policy should clearly state that the participant may not keep the data of the responsible organisation, including any personal data, longer than necessary. All personal data collected by the participant must be deleted immediately. If it proves necessary to retain these data for a certain period of time, the participant must ensure that these data are kept secure during this period.

5. Confidentiality

One of the essential elements of a coordinated disclosure policy must be respect for confidentiality: participants may not share the information collected with third parties or disseminate it to third parties without the express consent of the responsible organisation[62].

[62] Again, subject to limited disclosure to the authorities competent in cyber security.

Also, any disclosure of IT, communication or personal data to persons outside the responsible organisation or dissemination of such data to persons outside the responsible organisation by the participant must be expressly excluded, subject to the prior consent of the responsible organisation.

The text of the coordinated disclosure policy should state that the purpose of the policy is not to permit the deliberate access to the content of IT, communication or personal data and that such access can only occur accidentally and occasionally in the context of the detection of vulnerabilities in the technologies concerned.

6. Act in good faith

The organisation responsible for the IT system must undertake to carry out its coordinated disclosure policy in good faith and don't pursue civil or criminal action against the participant complying with its terms.

On the part of the Participant, there can be no fraudulent intent, intent to harm, or desire to use or cause harm to the visited system or its data. This also applies to third party systems located in Belgium or abroad.

With respect to devices enabling a computer data breach to be committed, the participant may develop, possess or make available such devices as part of participation in a vulnerability disclosure policy. Such actions are not unlawful as long as they are justified by legitimate purposes relating to the detection of vulnerabilities with the consent of the organisation responsible for the IT system concerned.

7. Processing of personal data

The purpose of a CVDP is not to intentionally process personal data. However, it is possible that the participant may, even by accident, have to process personal data in the context of its 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 e-mail address, identification number, online identifier, IP address or still, 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.[63]

Since the GDPR constitutes a form of accession agreement that binds the ethical hacker to the responsible organisation, it is necessary to specify the obligations of the parties with regard to the processing of personal data, in particular the purpose of and the essential resources for any processing carried out under this policy *(see Guide - Part II Legal Aspects).*

8. Procedural deadlines

It is recommended that clear deadlines be set for each stage of the procedure, in particular for sending an acknowledgement of receipt to the participant, communicating additional information, studies, developing a solution, replying to the participant, 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 seriousness of the situation.

[63] Art. 4, 7), of the GDPR.

9. Continuous communication

Good cooperation requires continuous and efficient communication. The information provided by the participant can be very useful in identifying the vulnerability and resolving it. It is therefore important to send acknowledgements of receipt, to keep participants 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 (preferably designated in the CVDP) or of a bug bounty platform can help to establish and maintain a constructive relationship between the parties, or possibly guarantee the anonymity of participants.

If one of the parties or the designated coordinator does not respond, the parties can always call upon the Centre for Cyber Security Belgium (vulnerabilityreport@cert.be).

10. Giving a reward

Rewards or a public recognition[64] given by the responsible organisation makes the CVDP more attractive for the participants and often leads to better results for the organisation. It may even be a purely symbolic gift: for example, a t-shirt, a sticker or a special mug.

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

[64] Ranking among the best participants, publication, conference, etc.

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

The organisation can use a bug bounty platform[65], which will coordinate the technical and administrative aspects of its reward program together with the organisation.

11. Possible public disclosure

Any disclosure of a vulnerability should be coordinated and synchronised between the parties to allow sufficient time for the responsible organisation to resolve the issue and to inform affected critical operators in advance.

Where a vulnerability is identified in a program, component, protocol or format provided by a third-party vendor, the responsible organisation will notify them directly before any public disclosure is made.

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 responsible organisation to other organisations (e.g. through user licences). 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 public disclosure, the vulnerability report and the solution should ideally be published at the same time.

[65] For example: www.intigriti.com (platform based in Belgium); www.yeswehack.com (platform based in France); www.yogosha.com; www.hackerone.com (platform based in the US).

The responsible organisation must offer various means to inform and protect its users: for example, automatic system updates, publication of security notices on its website, mailings with a link to a specific internet page, distribution of this information to its network of vendors etc.

If a vulnerability is not yet known and threatens to have a direct or indirect impact elsewhere, the organisation responsible must inform the Centre for Cyber Security Belgium (vulnerabilityreport@cert.be) and the other organisations potentially concerned in advance, even if it does not want the vulnerability to be made public.

** tech-support concept. Free license. Designed by macrovector / Freepik (2020)*

CENTRE FOR CYBER SECURITY BELGIUM

II. Procedure

a. Discovery

Where a participant discovers information about a potential vulnerability, he should to the extent possible, conduct prior checks to confirm the existence of the vulnerability and identify any risks involved.

Then, he must provide the responsible organisation with at least sufficient technical information to confirm the existence of this problem and provide their contact details. These elements may be supplemented according to the specifications of the coordinated publication policy or the content of the responsible organisation's online form.

b. Reporting

Participant must provide as soon as possible the technical information to the contact point or to the coordinator designated by the responsible organisation by secure means of communication.

When the responsible organisation receives a notification, it must send an acknowledgement of receipt to the participant as soon as possible, indicating the internal reference and the next stage of the procedure.

Together with this acknowledgement of receipt, the responsible organisation may indicate the content of its coordinated publication policy, or at least provide a link to it, and request any additional information.

It is particularly interesting to ask whether the participant has already reported this problem to other responsible organisations.

c. Investigation

During the investigation phase, the responsible organisation can reproduce the environment and the identified behaviour, in order to check the information provided.

Participant must be regularly informed of the results of the investigation and of the action taken on the report.

During this process, parties should ensure to link to similar or related reports, to assess the risk and severity of the vulnerability and to identify any other affected products or systems.

d. Deployment of a solution

The objective of the disclosure policy is to enable the development and deployment of a solution to remove the vulnerability from the IT system.

Unless legally or contractually obliged to do so, the responsible organisation remains free to choose to develop and implement a solution or not.

Of course, the choice not to resolve a proven security flaw could, if necessary, engage the civil liability of the organisation responsible if a third party suffers damage as a result[66].

To the extent possible, the solution should be developed within 90 calendar days at the latest.

[66] This is independent of the existence of a responsible disclosure policy.

These deadlines should be kept to the strict minimum if users of the affected systems are at risk or if there are risks to the protection of personal data. If the organisation is unable to solve the problem immediately, the IT system concerned should be taken completely out of service temporarily.

However, the supply chain and the multiple interdependencies between information systems can complicate the time needed to develop a solution and deploy it.

During this phase, the responsible organisation (or its service provider) must, on one hand, perform positive tests to verify that the solution is working properly and, on the other hand, negative tests to ensure that the solution does not disrupt the proper functioning of other existing functionalities.

If the solution is ready and the vulnerability would affect other organisations as well, it should be communicated to the CCB as a matter of priority and before any public disclosure (vulnerabilityreport@cert.be).

The responsible organisation should respect a reasonable period of time from this transmission before a possible general disclosure to users, in order to allow operators of vital interest (operators of essential services NIS, critical infrastructures, public administrations, etc.) to implement the solution as a priority.

e. Possible public disclosure

Unless there is a specific legal requirement, the public disclosure of a vulnerability is not a mandatory step in a CVDP. Indeed, the participant and the responsible organisation can agree not to disclose the existence of the vulnerability. This could be the case if the vulnerability proves too difficult or impossible to resolve, or if resolving it would involve disproportionate costs compared to the potential risks involved.

However, this should remain the exception, as the purpose of a CVDP is to improve security and transparency vis-à-vis users. In addition, certain legal provisions require the responsible organisation to inform the users of the IT systems[67] or the natural persons involved in a personal data breach[68].

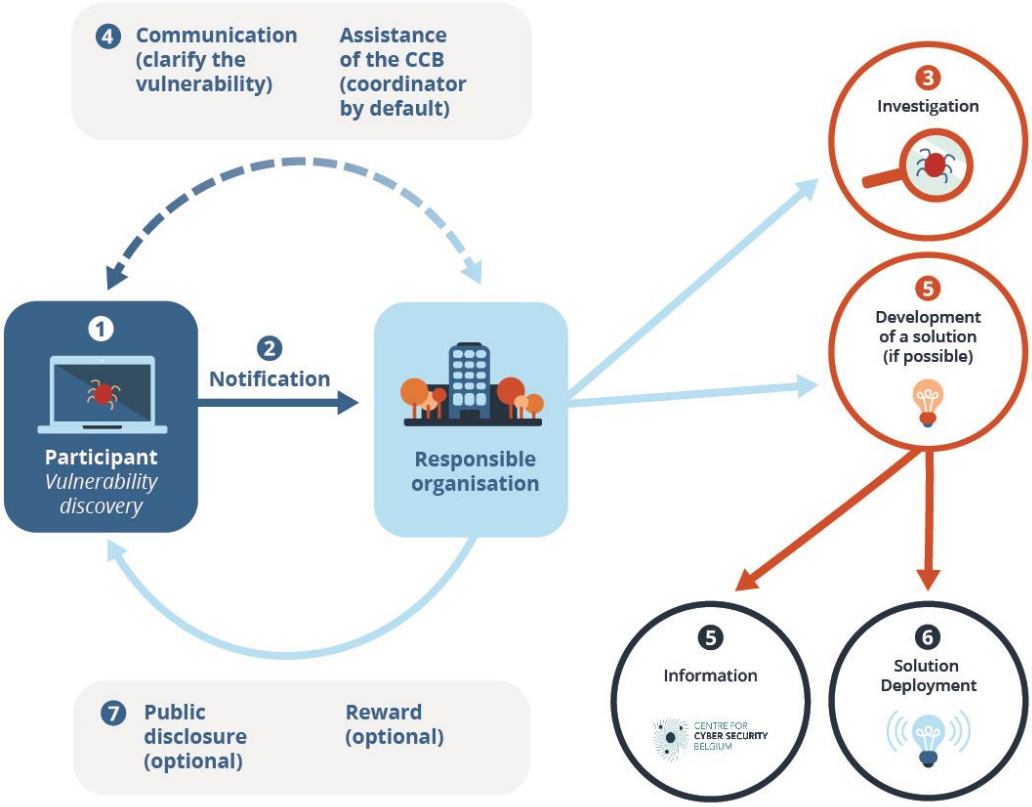
In any case, information relating to a vulnerability that would also affect other organisations will at least be submitted to the CCB (vulnerabilityreport@cert.be**).**

If the vulnerability is made public, the responsible organisation will, in consultation with the participant, lay down the terms and conditions for the disclosure. Ideally, information about the vulnerability should be disclosed at the same time as the solution. The responsible organisation is recommended to inform its customers by posting a security notice on its website or by other means of communication (e-mail, information letter, system update, etc.).

The responsible organisation should also inform other organisations likely to be involved in the same vulnerability. The possible interdependence of IT systems or the supply chain may lead to wider coordination of possible disclosure.

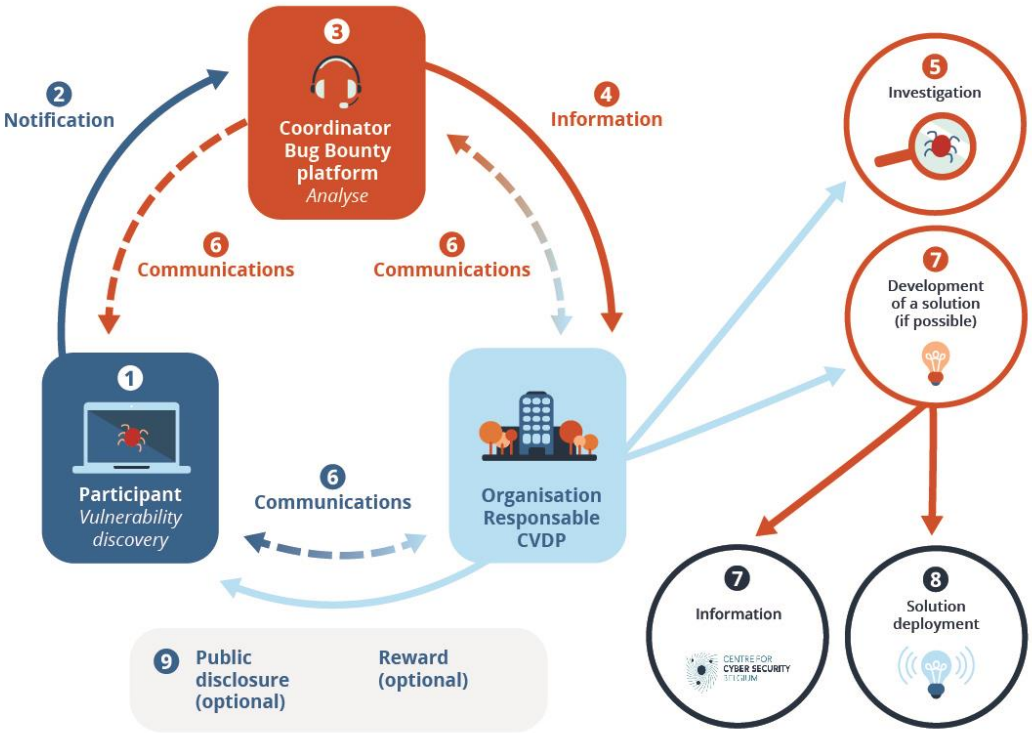
It is also important to collect users' comments on the application of the solution and to take the necessary corrective action to resolve any problems caused by the solution, including those relating to compatibility with other products or services.

[67] See in particular the rules on contractual and non-contractual liability.
[68] Art. 34 of the GDPR.



1. Participant finds a vulnerability in the context of a CVDP.
2. Participant informs the responsible organisation based on the CVDP details.
3. The responsible organisation analyses the vulnerablity.
4. Communication between the participant and the responsible organisation continues to clarify the vulnerability. assistance from the CCB (as coordinator by default) can be asked if there is a lack of communication in this process.
5. A solution is developed (if possible). In case the vulnerability could affect also others organisations, the responsible organisation informs the CCB.
6. The responsible organisation deploys the solution to its users or customers.
7. Approval for public disclosure can be discussed and a reward can be given based on the CVDP.

** Designed by CCB and Intigriti - 2020*



1. Participant finds a vulnerability in the context of a CVDP.
2. Participant informs the responsible organisation through a coordinator, such as a bug bounty platform, based on the CVDP details.
3. The Coordinator analyses the vulnerablity.
4. After validation the coordinator will inform the responsible organisation.
5. The responsible organisation analyses the vulnerablity.
6. 6 Communication between the participant and the responsible organisation continues to clarify the vulnerability, if desired through the coordinator.
7. 7 A solution is developed (if possible). In case the vulnerability could affect also others organisations, the responsible organisation informs the CCB.
8. The responsible organisation deploys the solution to its users or customers.
9. Approval for public disclosure can be discussed and a reward can be given based on the CVDP.

** Designed by CCB and Intigriti - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

D. REFERENCES

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure and *Economics of Vulnerability Disclosure*, 2018, www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

CENTRE FOR EUROPEAN POLICY STUDIES (CEPS), *Software vulnerability disclosure in Europe. Technology, Policies and Legal Challenges, Report of a CEPS Task Force, 2018,* www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges

GLOBAL CONFERENCE CYBER SPACE, *Best practice guide Responsible Disclosure*, 2015, www.gccs2015.com/sites/default/files/documents/BestPracticeRD-20150409_0.pdf

INTERNET ENGINEERING TASK FORCE (IETF) - CHRISTEY S. & WYSOPAL C., *Responsible Vulnerability Disclosure Process*, 2002, https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00 (www.circl.lu/pub/responsible-vulnerability-disclosure)

ORGANIZATION FOR INTERNET SAFETY, *Guidelines for responsible disclosure*, 2004, www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf

SOFTWARE ENGINEERING INSTITUTE, *The CERT Guide to Coordinated Vulnerability Disclosure, 2013 (updated in 2019)* https://vuls.cert.org/confluence/display/CVD

NATIONAL CYBER SECURITY CENTRE (NL), *Leidraad Coordinated Vulnerability Disclosure (Coordinated Vulnerability Disclosure: the Guideline),* 2019, //english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline and *Policy for arriving at a practice for Responsible Disclosure*, 2013

CIO PLATFORM NEDERLAND - CEG INFORMATION SECURITY, *Coordinated Vulnerability Disclosure. Model Policy and Procedure*, 2016, www.cio-platform.nl/en/publications and *Coordinated Vulnerability Disclosure 1.4. Implementation guide*, 2016, www.cio-platform.nl/en/publications

ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (https://www.iso.org/standard/72311.html)

ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html)

CENTRE FOR CYBER SECURITY BELGIUM

GUIDE FOR THE COORDINATED VULNERABILITY DISCLOSURE POLICY
PART I: GOOD PRACTICES

This document and its annexes were drawn up by the Centre for Cyber Security Belgium (CCB). This federal public service was created by the Royal Decree of 10 October 2014 and is under the authority of the Prime Minister.

The information provided:
• is purely general in nature and does not aim to cover all specific situations;
• is not necessarily complete, accurate or up to date in all respects.

Responsible publisher:
Centre for Cyber Security Belgium
M. De Bruycker, Director
Wetstraat 16
1000 Brussels

Legal deposit:
D/2020/14828/014

2020