National Coordinated Vulnerability Disclosure Policy (NCVDP)

P-SPG-001-01
10th December 2024

CSIRT MALTA
COMPUTER SECURITY &
INCIDENT RESPONSE TEAM

mdia MALTA DIGITAL INNOVATION AUTHORITY

Table of Contents

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

1. Introduction

1.1 Overview

ICT Systems are susceptible to Vulnerabilities, just like anything else in the world. These Vulnerabilities may leave ICT Systems prone to incidents that affect their security.

Sometimes these Vulnerabilities are not known or identified by the Responsible Organisation. Therefore, the Responsible Organisation may opt to allow a Security Researcher to test the security of its ICT System to potentially identify any Vulnerabilities. The Responsible Organisation may also permit the Security Researcher who identified the Vulnerabilities to help resolve them.

1.2 Scope

By virtue of Article 7 (2) of the 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 (so called 'Network and Information Security' directive 2, hereinafter referred to as '**NIS2**'), 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 (hereinafter referred to as '**CVD**') under Article 12 (1) of NIS 2. Other EU legislation which could come into force may also have similar impositions on Member States to adopt a CVD Policy (hereinafter referred to as '**CVDP**').[1]

Furthermore, as part of the National Cybersecurity Strategy 2023-2026, Malta also has action points 1.5 and 1.6 to fulfil.

In view of this, the scope of this document is for Malta to adopt and implement a national policy to integrate Vulnerability management and also integrate, promote and facilitate CVD processes.

The scope of this NCVDP includes, amongst others, the following objectives:

1. To aid Responsible Organisations in establishing the terms and conditions that a security researcher must be in line with prior to, during and after the security research. Therefore, where the Responsible Organisation puts into effect a CVDP and a Security

[1] Under the Proposed Cyber Resilience Act, manufacturers have the obligation to make a CVD Policy before placing on the market a product with digital elements.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Researcher performs security research, the CVDP of the Responsible Organisation will be tantamount to a binding agreement amongst the Parties.

2. To support Responsible Organisations in the implementation of a CVDP with a view to encourage the ongoing testing of its ICT Systems, allowing for Vulnerabilities to be identified and addressed, ultimately improving the security, trust and confidence of the users in ICT systems, and related research in this area.
3. To encourage the Responsible Organisations to comply with their legal obligations under any applicable EU legislation and directives.
4. To promote the adherence of Responsible Organisations with industry's best practices and applicable standards, with regards to the CVDP.
5. To ensure that any type of information regarding a Vulnerability is handled carefully and in confidentiality whilst coordinating with the Responsible Organisation.

The content of this NCVDP is without prejudice to any applicable legal provision, including the Criminal Code, Chapter 9 of the Laws of Malta[2], NIS 1/NIS 2, and any other current and future legal obligations which the Responsible Organisations and, or the Security Researcher and, or any other party may have. Moreover, this CVDP is aimed to be standards and technology neutral.[3]

1.3 Definitions and Abbreviations

Coordinated Vulnerability Disclosure Policy ('CVDP') is a formalized set of rules for searching and reporting Vulnerabilities, with an emphasis on coordinated handling of information about these Vulnerabilities to limit damage caused by unintentional or untimely disclosure, as well as by non-responsive counterparties. These rules should ensure and be associated with, inter alia, secured means of communication, confidentiality of the information exchanged and provide a guarantee that the parties involved in the process will not disclose vulnerability information without a due coordination.[4]

[2] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 5.
[3] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 3.
[4] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 4.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Coordinator can connect, as trusted intermediary, and coordinate further action to remediate a Vulnerability that threatens multiple Vendors or the Responsible Organisation. The Coordinator can also provide technical analysis or expert assistance.[5]

ICT System includes any part of the ICT System composed of integrated elements which includes software, websites, hardware, digital or physical components, elements or ICT products, including any ICT services and processes and Operational Technology managed and controlled by the Responsible Organisation and on which access right to the Security Researcher, pursuant to the CVDP, has been granted.

ICT System Owner or Manager is a natural or legal person or an organisation or public authority that is responsible for an ICT System which it manages and controls and may also provide service for other customers. The Responsible Organisation is responsible for implementing a CVDP in its environment, assess vulnerability reports, communicate with the Vendor/Supplier and apply the necessary measures.[6]

National Coordinated Vulnerability Disclosure Policies ('NCVP') are policies adopted by Member States to promote and facilitate CVD, as part of their national cybersecurity strategy. The CVD is described in recital 58-62 and Article 12(1) of NIS 2[7] 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 trusted intermediary and facilitating, where necessary and upon the request of either party, the interaction between the concerned stakeholders.[8]

Operational Technology means hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise.[9]

Responsible Organisation includes ICT System Owner or Manager.

---

[5] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 5.
[6] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 4.
[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union Articles 11(3)(g) and 12 (1) hereinafter referred to as 'NIS2'. Accessible from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.
[8] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 4.
[9] The United States Code, Title 15 Commerce And Trade, Chapter 7 National Institute of Standards and Technology, Article 3a. Accessible from 15 USC 278g-3a: Definitions (house.gov).

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Reward Program is an optional element of a CVDP which can offer different types of appreciation for a valid Vulnerability report (such as, Vulnerability Reward Program (**'VRP'**) or bug bounty, recognition program or gift programs).[10]

Security Researcher or Participant is a natural or legal person or organisation who has the required experience, and, or skillset and, or certifications and who intentionally, but always in good faith and good intent, adheres to the published CVDP of the Responsible Organisation and is thus, authorised pursuant to the same CVDP, to research, assess, identify and report a Vulnerability, if any, in the ICT System of the Responsible Organisation in order to contribute to improving the security of the ICT Systems of the Responsible Organisation. The Security Researcher should be a Security Researcher notified with the MaltaCIPD.

Vendor/s or Supplier/s – is a natural or legal person that owns, manufactures, sells, offers or manages ICT Systems, products or services and is therefore responsible for their functionality and security. It is highly recommended for Vendors/Suppliers to publish a CVDP to allow Security Researchers to identify and report Vulnerabilities, as well as build internal capacity and governance to address CVD related issues. Vendors/Suppliers must be involved in the verification and remediation of the Vulnerabilities.

Vulnerability/ies mean/s a weakness, susceptibility or flaw of an ICT System. Based on ISO/IEC 27000:2022, a Vulnerability is a weakness of an asset or control that can be exploited by one or more threats.[11] In terms of ISO/IEC 29147:2018[12], Vulnerability implies a functional behaviour of a product or service that violates an implicit or explicit security policy. In general, the term Vulnerability can be understood as a flaw or a weakness, a design or execution error, 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, expression of threat and be exploited by malicious third parties to harm the integrity, authenticity, confidentiality or availability of an ICT System or to damage an ICT System.[13]

[10] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 4.
[11] ISO/IEC 27000:2022, Information security, cybersecurity and privacy protection — Information security controls.
[12] ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure.
[13] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 4.

Twenty20 Business Centre, Triq I-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

2. Legal Framework to allow CVD process

2.1 The Parameters of the CVDP

The Responsible Organisation shall delineate the part of the ICT System, including any digital components, for which the Security Researcher is thus authorised to act pursuant to the respective CVDP.

The Responsible Organisation must also inform the Security Researcher of any applicable intellectual property rights together with any ensuing limitations.[14]

Should the Responsible Organisation wish to omit certain parts of the ICT System from its CVDP, it shall also clearly indicate these in its CVDP.

Before rolling out an applicable CVDP, the Responsible Organisation will need to assess all related agreements with any third-party provider, the controller/ processor clauses which will be required, as well as its privacy policy, to ensure that all the required legal considerations, including any relevant authorisations, if applicable, have been made.

If the Security Researcher encounters any type of uncertainty prior to or during the Security Research, written approval must be obtained by the Security Researcher from the Responsible Organisation prior to performing any Security Researching that relates in any way to the mentioned uncertainty.[15]

Legal proceedings may be taken against the Security Researcher who would have breached the CVDP and failed to abide by the CVDP. Provided that if any part of the CVDP is amended by the Responsible Organisation after the Security Researcher commenced the Security Research, the applicable CVDP to the security research would be the one in force at the time when such Research started.

[14] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 7.
[15] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 7.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

2.2 Civil Liability[16]

The Security Researcher shall always act in good faith and be responsible for adherence to any applicable Law and the contents of the CVDP of the Responsible Organisation and hereby represents to the Responsible Organisation that neither the execution of this CVDP, nor compliance with its terms and conditions, will result in the creation of any rights or lien on any part of the ICT System.

The Participant is not permitted to make use of unethical, illicit, unreasonable or imprudent practices including, but not limited to, practices which would disrupt the ICT System, or alter production or consumer data.

The Participant may only conduct the authorised access as specified in the CVDP of the Responsible Organisation and specifically only in the period of time indicated.

The Participant must make use of any secure methods indicated by the Responsible Organisation to communicate with the same.

The Participant must at all times act proportionately in the sense that the Participant should not intentionally interrupt the ICT Systems of the Responsible Organisation and should refrain from intentionally exploiting the Vulnerabilities that go beyond what is strictly necessary to show the same Vulnerability. This includes avoiding the unnecessary utilisation of data.

The Participant should not act beyond what was necessary and proportionate to verify and report the existence of a Vulnerability.[17] Techniques such as, social engineering attacks, Distributed Denial-of-Services (**'DDoS'**) attacks and supply chain attacks are considered disproportionate and to this extent should be ruled out.

The Participant should not have any intention that is fraudulent and, or harmful in any way.[18]

[16] Ideally, the Responsible Organisation should incorporate this clause in its CVDP and thus, limit the liability of the Security Researcher (NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023)).
[17] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 8.
[18] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 8.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

The Participant is permitted to make use of lawfully permitted and acquired hardware and soft-based tools that facilitate the process by virtue of which a Vulnerability can be detected, provided that the said devices are deemed to be secure and safe for use by the Security Researcher and their use should be in adherence with the CVDP of the Responsible Organisation.[19] The Participant shall use secure methods when conducting the Security Research such as, amongst others, following known penetration testing standards, for example, PTES[20] and OWASP[21] . This is without prejudice to any other secure method which the Responsible Organisation may oblige the Participant to make use of.

In determining and setting up the conditions, it is suggested that the Responsible Organisation conducts an assessment of the conditions of the CVDP of the Responsible Organisation.

The Responsible Organisation agrees to indemnify the Security Researcher and keep the Security Researcher indemnified from and against any and all damage or injury resulting from the intentional acts or omissions performed in line with the performance of the CVDP of the Responsible Organisation.[22]

The Security Researcher shall not be liable for any lost profits, loss of business, loss of use, lost savings or other consequential, special, incidental, indirect, exemplary or punitive damages whilst adhering to the CVDP of the Responsible Organisation.

Nothing in this NCVDP and the CVDP of the Responsible Organisation shall exclude or limit Security Researcher's liability for fraud, intentional infringement of intellectual property rights, breach of the CVDP, death or personal injury resulting from its negligence and any act of gross negligence.

2.3 Protection of Personal Data

The Responsible Organisation and the Security Researcher must abide by REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**'Regulation (EU) 2016/679'**) at all times.

[19] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 9.
[20] Refer to the following link: http://www.pentest-standard.org/index.php/Main_Page.
[21] Refer to the following link: https://owasp.org.
[22] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 9.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

In case the Security Researcher detects a vulnerability that may lead to any form of processing within the meaning of article 4(2) of the Regulation (EU) 2016/679, irrespective of the extent of personal data involved or the nature of personal data, the Security Researcher shall not proceed any further and inform the Responsible Organisation immediately.

Provided that, if the Security Researcher processes personal data without being instructed by the Responsible Organisation, the Security Researcher shall assume the functional role of a separate controller within the meaning of article 4(7) of Regulation (EU) 2016/679 and shall fully comply with the provisions of Regulation (EU) 2016/679.

The Security Researcher's activities in a CVD process may include, *inter alia*, testing, assessing and evaluating the effectiveness of the technical measures implemented by the Responsible Organisation to ensure the security of the processing of personal data pursuant to article 32(1)(d) of Regulation (EU) 2016/679.

In case the Responsible Organisation instructs and authorises the Security Researcher to process personal data on its behalf, the processing shall be governed by a bilateral controller-processor agreement, that is binding on the Security Researcher with regard to the Responsible Organisation. The controller-processor agreement shall contain the requirements set forth in article 28(3) of Regulation (EU) 2016/679. The Responsible Organisation may use standard contractual clauses set out in the Annex to the Commission Implementing Decision (EU) 2021/915 of 4 June 2021.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

3. Computer Security Incident Response Team/s (CSIRT/s)

In terms of NIS 2, designated CSIRT/S could play a Coordinator role, acting as a trusted intermediary facilitating, where necessary and upon the request of either party, the interaction between the concerned stakeholders.[23] Article 12 of NIS 2 goes into further detail on the coordination tasks of CSIRT/S.

The CSIRTMalta within the Malta Critical Infrastructure Directorate ('**MaltaCIPD**') currently situated at 43A, St. Paul Building, Suite 1, West Street, Valletta, VLT 1532, has been designated as the Coordinator for the purposes of CVD.

The MaltaCIPD should be allocated sufficient resources and capacity, including staff, appropriate and dedicated tools.[24]

The CSIRTMalta may develop in a separate document further details on its internal procedure relating to Vulnerability handling which will incorporate the diligent follow-up actions, the anonymity of the natural or legal person reporting the vulnerability and, where appropriate, cooperation with other CSIRTs.[25]

The CSIRTMalta shall keep a registry of the Responsible Organisations that establish a CVDP, and of their respective CVDPs. The CSIRTMalta shall also keep a registry of all the Security Researchers that shall follow the CVDPof a particular Responsible Organisation/s. The process for registration and any ancillary requirements shall be at the discretion of the CSIRTMalta.

[23] Articles 11(3)(g) and 12 (1) NIS2.
[24] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 8.
[25] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 8.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

4. Reporting Procedure

4.1 The Report

Once the Security Researcher has confirmed the presence of a Vulnerability, the Security Researcher shall formulate a written report to the CSIRTMalta and the Responsible Organisation.

The report, when available, must include but not limited to the following:

(a) the type of Vulnerability,
(b) the version of the product on which the Vulnerability is present, or the specific configuration of the product that is Vulnerable,
(c) the details of its configuration, including the following information:

i. A summary of the Vulnerability
ii. The steps executed to find the Vulnerability
iii. Required steps to reproduce the Vulnerability
iv. Required configuration to reproduce the Vulnerability
v. Possible known mitigation measures for the Vulnerability,

(d) potential impact of the Vulnerability,
(e) the resources employed,
(f) any testing data used by the Security Researcher,
(g) any proof of the Vulnerability and Security Researching such as, screen captures,
(h) asset or control where the Vulnerability is found (web page, internet protocol address, product or service name),
(i) the necessary proof that the Vulnerability exists,
(j) any technical information,
(k) the Security Researcher's contact information including secure communication options (PGP fingerprint, etc.),
(l) whether the Vulnerability has already been reported to the product manufacturer,
(m) whether a request for a common vulnerabilities and exposures ('CVE') number has been made or if there already is a CVE number to refer to accordingly,
(n) any other important information related to the discovered Vulnerability, and
(o) the name/s and surname/s of Security Researcher/s and confirmation of notification to the MaltaCIPD.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

When formulating the report, the aforementioned details should be included in the following sections of the report:

(i) **Executive summary**: The executive summary provides a high-level overview of the assessment for non-technical executives. The goal of this summary should be to help executives gauge their current security posture and highlight any critical issues that might impact corporate cybersecurity and may include regulatory compliance.

(ii) **Details**: This report section should provide in-depth technical detail about how the Vulnerability assessment was performed. This section should build on the overview by describing the exact steps performed at each assessment stage and their results.

(iii) **Findings**: This section of the report provides more details about the assessment findings. Vulnerabilities as well as any potential data breaches may be ranked by severity to draw attention to the biggest issues within a Responsible Organisation's environment. For each potential Vulnerability checked, this section should describe the result, affected system(s) and severity level.

(iv) **Recommended mitigations**: The goal of a Vulnerability assessment is to help a Responsible Organisation move towards a better security posture, so providing recommended mitigations can be helpful. In many cases, this can be as simple as recommending an update to the software, a stronger password on an ICT System, or a change to an insecure security setting.

The report must be communicated in a secure manner with CSIRTMalta and the Responsible Organisation.

The CVDP may delineate the process which needs to be followed should the Security Researcher find a Vulnerability in the ICT System of a third-party whilst performing Security Researching in the ICT System of the Responsible Organisation.

4.2 Anonymous Reporting

In case of anonymous reporting, the anonymous reporting should be done solely and exclusively on a Vulnerability/Vulnerabilities found on the ICT System of the Responsible Organisation and specifically to the CSIRTMalta.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

4.3 Disclosure

Without prejudice to any other right conferred on CSIRTMalta, the Security Researcher shall be prohibited from conducting any public disclosure of the information discovered during the Security Researching without the prior written agreement of the designated CSIRT and the Responsible Organisation. The agreement should be given after coordination with Vendors or Systems Owners and/or all concerned parties with the Vulnerability.[26] Any disclosure with third parties should be carried out on a need-to-know basis, provided that it is in line with the CVD of the Responsible Organisation.

Nonetheless, should the Vulnerability effect multiple parties, the CSIRTMalta shall have the right to provide early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, Vulnerabilities and incidents, if possible in near real time.[27] If it is in the public interest and in extreme rare cases as determined by the CSIRTMalta, the CSIRTMalta could consider where permitted by law allowing for public disclosure without the consent of the Responsible Organisation.

Once the report is provided to the Responsible Organisation and CSIRTMalta, the Security Researcher must cooperate with the Responsible Organisation and allow ample time, as deemed fit by the Responsible Organisation for it to remedy the Vulnerability, or as otherwise determined by CSIRTMalta.

Should the Responsible Organisation and CSIRTMalta decide to disclose publicly a Vulnerability that has been found in the ICT System of a third-party provider, the latter needs to be informed prior to the said public disclosure. The same applies when the affected ICT System component is supplied by the Responsible Organisation to another organisation. In informing such third-parties and also in case of public disclosure, it is pertinent for the Responsible Organisation to provide the Report together with the related solution.

The CVDP of the Responsible Organisation should stipulate the conditions that should be followed when there is a disclosure of the Vulnerability.

[26] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 8.
[27] NIS2, Article 11(3)(b).

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

4.4 Deadlines

The content of the CVDP of the Responsible Organisation should set clearly any deadlines for the phases of the process that would aid in facilitating the process for the Security Researcher. These deadlines could be stipulated in regards to the communication between the parties, the advancement of a remedy to fix the Vulnerability, the applicable reward and where necessary, the issuance of any report or information. Notwithstanding this, the CVDP of the Responsible Organisation should oblige the Responsible Organisation to provide an acknowledgement of receipt of communication within three (3) working days.

Although such deadlines are recommended, it is important that the parties adapt according to the exigencies that may arise in certain cases, namely, where the Vulnerability which would have been found by the Security Researcher is complicated and where a considerable amount of technology components of an ICT System would have been impacted.

Twenty20 Business Centre, Triq I-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

5. Obligations of the Responsible Organisation

5.1 Communication

(a) Accessibility for Security Researcher

The Responsible Organisation must provide a version of its CVDP in English and in all the other languages used in its website. The CVDP of the Responsible Organisation should be published in a location where it can be obtained without difficulty, ideally, on a specific section on the website of the Responsible Organisation, in a 'security.txt' file in the tree structure of the Responsible Organisation's website and in the web browser extensions that locates those websites which contain a CVDP. A link to the webpage which contains the CVDP would ideally be provided in any other relevant location such as, but not limited to, an FAQ webpage on the website of the Responsible Organisation.

(b) Vulnerability Disclosure Contact Point

The CVDP must clearly delineate how communication with the Responsible Organisation should be done and the Responsible Organisation must indicate the secure methods of communication. For instance, the CVDP should specify the Responsible Organisation's contact point, such as, but not limited to, a specific e-mail address or an online form, which is assigned to receive details and queries regarding Vulnerabilities. The Responsible Organisation may also provide a specific telephone number for urgent matters regarding Vulnerabilities.

An internal procedure should be set up by the Responsible Organisation so that if information regarding Vulnerabilities is received in other means of communication, the received information is passed on to the specified contact point.

(c) Security and Confidentiality

It is important for the Responsible Organisation to ensure that a secure and confidential method of communication is used in order to prevent any data from being leaked. Therefore, the Responsible Organisation should ideally either implement a secure Internet portal (such as a PGP Encryption Key) with the use of a data encryption tool or require documents containing information about Vulnerabilities to be password-protected.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

(d) Information to Security Researchers

It is essential for the Responsible Organisation to develop a good relationship with the Security Researcher which ensures an ongoing and effective chain of communication for the benefit of both parties. It would be ideal for the Security Researcher to receive the following from the Responsible Organisation:

- an automated receipt notification upon sending information to the contact point of the Responsible Organisation,
- feedback and updates related to the identified Vulnerability,
- reminders about the responsibilities of the Security Researcher and
- results which would be produced from the analysis made by the Responsible Organisation.

(e) Notification to Third Parties

The protection of third parties, especially of the users of the ICT System of the Responsible Organisation should be a fundamental aspect of the principles and values of the Responsible Organisation. This could be achieved by amongst others, enabling automatic updates to be performed to the ICT System, putting up on the website of the Responsible Organisation security announcements, sending any necessary sanitised webpage links by email and sharing the necessary information to the suppliers of the Responsible Organisation.

Should the Responsible Organisation decide to conduct a disclosure as previously mentioned, it is suggested that third parties are informed by clear means of communications such as, a security notice on the website of the Responsible Organisation.

(f) Reviews and Updates

The Responsible Organisation should ideally review its CVDP on a timely basis to ensure that all the information is up to date and corresponding to its ICT System. Should the Responsible Organisation perform any updates to its CVDP, it must disseminate and publicly announce the modifications made and also inform the CSIRTMalta.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

(g) Notification to CSIRTMalta

The Responsible Organisation shall notify in writing to the CSIRTMalta that the former has established a CVDP of its own and shall communicate such CVDP with the MaltaCIPD.

It is encouraged that the Responsible Organisation communicates with the CSIRTMalta, any report/s which it receives from Security Researchers in relation to any Vulnerability in the ICT System of the Responsible Organisation.

5.2 Vulnerability Remediation Process

It is recommended that, the Security Researcher as well as the Responsible Organisation have the required Vulnerability remediation process in place when utilising the CVDP. This should, as a minimum, include the following parameters:

1. Collection:
   (a) The way how the Security Researcher collects the Vulnerability reports;
   (b) After receiving a report, the way how the Responsible organisation performs its initial analysis to assess the Vulnerability;
   (c) The respective cataloguing of the Vulnerability and, or report, including all respective information.
2. Analysis: Once the Vulnerability reports are catalogued, the process how the Responsible organisation analyses the Vulnerabilities (e.g., by examining the technical issue and the potential risk that the Vulnerability represents).
3. Mitigation Coordination: The process to be followed by the Responsible Organisation and the Security Researcher after the analysis of the Vulnerability, including, any potential workflows to mitigate and provide solutions.
4. Application of Mitigation: In furtherance to the above, any additional work and coordination which might be required by the Security Researcher to mitigate the Vulnerability and, or provide a solution.
5. Disclosure: A coordination procedure on how to conduct any disclosure to any third parties.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

5.3 Good Faith and Solution

The content of the CVDP should be in line with any applicable laws and the Responsible Organisation must ensure to also act in good faith.

The fact that the Responsible Organisation would have devised a CVDP does not only mean that the Responsible Organisation is welcoming Security Researchers to find a Vulnerability, but it also entails that the Responsible Organisation is willing to find a solution to fix that Vulnerability in the least time possible or as otherwise determined by the CSIRTMalta.

5.4 Public Entities

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 CVDPs. Public authorities should require CVD processes to be used by their suppliers, including also such CVD provisions in the public procurement contracts. The adoption of a CVD policy should also become a standard security requirement for all public authorities.[28]

[28] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 15.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

6. Rewards

The Responsible Organisation may choose to provide a reward, as it deems fit, to Security Researchers when a Vulnerability is identified. It is up to the discretion of the Responsible Organisation on whether to grant such reward and which rewards it gives out based on the significance of the identified Vulnerability and the information provided by the Security Researcher.

There are different types of reward possibilities for organisations such as:

- A Vulnerability Rewards Programme (**'VRP'**, also called bug bounty) is an explicit financial reward paid for a vulnerability report by an organisation. Such a program is sometimes limited in time and the paid reward to the Security Researcher depends on the amount, importance or quality of the information transmitted.[29]
- Recognition Program offers to the Security Researcher an opportunity to receive public recognition for a reported vulnerability. These recognitions could be a ranking of best Security Researchers, publications, blog posts or a hall of fame offered by the Responsible Organisation. For Responsible Organisations such a program offers the advantage that there are no notable resources or budget needed to implement those programs.[30]
- Gift Programs reward a Security Researcher with a physical item. By giving out a physical item the Security Researcher has the opportunity to share such item online (e.g., Twitter, YouTube) and inspire others to report a Vulnerability to the Responsible Organisation.[31]

Based on the resources and budget a Responsible Organisation should evaluate if and what type of Reward Program it can offer. Implementing a Reward Program can increase the attraction to potential Security Researcher and often leads to more results for the Responsible Organisation.

Nonetheless, it is essential that the Responsible Organisation clearly states the nature of this reward in advance in its policy.[32]

[29] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 15.
[30]NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 15.
[31] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 15.
[32] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 15.

Twenty20 Business Centre, Triq I-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

It is prohibited for the Security Researcher to demand a reward which is beyond the parameters established by the CVDP.[33]

7. Jurisdiction

This CVDP shall be governed by and construed in accordance with the laws of Malta, and any disputes to its application or interpretation shall be submitted to the Courts of Malta.

8. Conclusion

This document provides points of principle and criteria for use of a CVDP.

The adherence in good faith by the Security Researcher to these points of principle and the applicable CVDP pursuant to this document aims to create a presumption of authorisation on the Security Researcher from the Responsable Organisation publishing such CVDP.

This document does not however, purport to amend, replace or prevail of any applicable laws in particular the Criminal Code, Chapter 9 of the Laws of Malta.

This document is meant solely and exclusively for guidance purposes. It is suggested that the respective Responsable Organisation as well as the Security Researchers seek the required advice on any of these points of principles.

[33] NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023) pg. 15.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Table of References

Legislation

Criminal Code, Chapter 9 of the Laws of Malta.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data.

Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act.)

Standards

ISO/IEC 27000:2022, Information security, cybersecurity and privacy protection — Information security controls.

ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure.

Guidelines

ENISA, Coordinated Vulnerability Disclosure Policies in the EU (2022).

NIS Cooperation Group, Guidelines on implementing national Cooperated Vulnerability Disclosure (CVD) policies (2023).

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt