**Coordinated vulnerability disclosure policy (CVDP)**

Name : ……………………………………………………………………………………………………………….

Address/head office: ……………………………………………………………………………………………………………….

……………………………………………………………………………………………………………………………………………………

Registration Number (CBE) :………………………………………………………………………………………………………………………………………..

Represented by: [name/name of the person authorized to legally represent the organisation] …………………………………………………………………………………………………………………………………………………..

Hereinafter referred to as the "Organisation",

1. Scope of the policy

In order to improve the performance and security of our networks and information systems, we have adopted a coordinated vulnerability disclosure policy. This policy gives participants the opportunity to search for potential vulnerabilities in our organisation's systems, equipment and products with good intentions or to pass on any information they discover about a vulnerability.

However, access to our IT systems and equipment is only permitted with the intention of improving security, informing us of existing vulnerabilities and in strict compliance with the other conditions set out in this document.

Our policy concerns security vulnerabilities that could be exploited by third parties or disrupt the proper functioning of our products, services, networks or information systems.

The participant is also permitted to introduce or attempt to introduce computer data into our computer system, subject to the purposes and conditions of this policy.

[*the list of products, services or websites in the scope of application must be drawn up]*.

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

[*the list of products, services or websites out the scope of application must be drawn up]*.

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

Systems that are dependent on third parties are excluded from the scope of this policy, unless the third party explicitly agrees to these rules in advance.

A list of systems used by the organisation and dependent on third parties that are excluded from the policy must be drawn up :

…………………………………………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………………………………………

Systems that are dependent on third parties are excluded from the scope of this policy, unless the third party explicitly agrees to these rules in advance.

A list of systems used by the organisation and dependent on third parties that are excluded from the policy must be drawn up.

The participant's research on information systems not explicitly included in the framework of this policy could lead to legal proceedings against him/her.

1. mutual obligations of the parties
2. **proportionality**

The participant undertakes to comply strictly with the principle of proportionality in all their activities, i.e. not to disrupt the availability of the services provided by the system and not to make use of the vulnerability beyond what is strictly necessary to demonstrate the security flaw. Their approach must remain proportionate: if the safety problem has been demonstrated on a small scale, no further action should be taken.

The objective of our policy is not to allow intentional knowledge of the content of computer data, communication data or personal data, and such knowledge could only occur incidentally in the context of the search for vulnerabilities.

1. **Actions that are not allowed**

Participants are not permitted to take the following actions:

* copying or altering data from the IT system or deleting data from that system;
* changing the IT system parameters;
* installing malware: viruses, worms, Trojan horses, etc.;
* Distributed Denial of Service (DDOS) attacks;
* social engineering attacks;
* phishing attacks;
* spamming;
* stealing passwords or brute force attacks;
* installing a device to intercept, store or learn of (electronic) communications that are not accessible to the public;
* the intentional interception, storage or receipt of communications not accessible to the public or of electronic communications;
* the deliberate use, maintenance, communication or distribution of the content of non-public communications or of data from an IT system where the participant should reasonably have known it had been obtained unlawfully.

-………………………………………………………………………………………………………………………………………………………….

-………………………………………………………………………………………………………………………………………………………….

-………………………………………………………………………………………………………………………………………………………….

-………………………………………………………………………………………………………………………………………………………….

If the participant wishes to use the assistance of a third party to carry out his or her research, the participant must ensure that the third party is aware of this policy and agrees, by offering assistance, to abide by its terms.

1. **Confidentiality**

The participant must strictly refrain from sharing or disclosing any information collected under our policy with third parties without our prior and explicit consent.

Similarly, it is not permitted to reveal or disclose computer data, communication data or personal data to third parties.

In the event that the vulnerability may also affect other organisations in Belgium, the participant or the organisation responsible may nevertheless inform the CCB (vulnerabilityreport@cert.be).

1. **Bonafide execution**

Our organisation undertakes to implement this policy in good faith and not to take legal action, either civil or criminal, against a participant who complies with its conditions.

The participant must be free of fraudulent intent, intent to harm, intent to use or intent to cause damage to the visited system or its data. This also applies to third-party systems located in Belgium or abroad.

If there is any doubt about any of the conditions of our policy, the participant must first ask our contact point and obtain its written consent before acting.

1. **Processing of personal data**

The purpose of a CVDP is not to intentionally process personal data, but it is possible that the participant may have to process personal data, even incidentally, in the course of his or her vulnerability research.

The processing of personal data is broad in scope and includes the storage, alteration, retrieval, consultation, use or disclosure of any information that could relate to an identified or identifiable natural person. The "identifiable" character of the person does not depend on the mere will of the data processor to identify the person, but on the possibility of identifying, directly or indirectly, the person by means of these data (for example: an e-mail address, identification number, online identifier, IP address or location data).

Thus, it is possible that the participant processes personal data to a limited extent. In the event of processing such data, the participant undertakes to comply with the legal obligations regarding the protection of personal data and the terms of this policy, in particular:

- The participant undertakes to process personal data only in accordance with the instructions of our organisation, as described in this policy, and exclusively for the purpose of investigating vulnerabilities in the systems, equipment or products of our organisation. Any processing of personal data for any other purpose is excluded.

- The participant undertakes to limit the processing of personal data to what is necessary for the purpose of vulnerability scanning.

- The participant shall ensure that the persons authorised to process personal data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality.

- The participant shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (e.g. encryption). The participant declares that he/she understands the risks associated with the implementation of this policy and that he/she has the necessary expertise and experience to test our organisation's systems, equipment and products safely and in compliance with applicable laws and regulations.

- The participant undertakes to assist us, to the extent possible and taking into account the nature of the processing and the information available to the participant, in the implementation of our obligations relating to the exercise of the rights of data subjects, the security of the processing and any impact assessment.

- The participant undertakes to inform us of any personal data breach as soon as possible after becoming aware of it at [to be completed by the responsible organisation].

- The participant may not keep any personal data processed for longer than necessary. During this period, the participant must ensure that this data is stored with a level of security appropriate to the risks involved (preferably encrypted). At the end of his/her participation in the policy, this data must be deleted immediately.

- The participant undertakes to keep a register of the categories of processing activities carried out on behalf of our organisation, including a description of the security measures implemented by the participant, in accordance with Article 30, § 2 of the GDPR.

The participant may work with a third party to carry out its research. The participant shall ensure that the third party is aware of this policy and agrees, by providing assistance, to abide by its terms, including confidentiality and the implementation of appropriate security measures. The participant acknowledges that he/she remains fully responsible to our organisation if the third party he/she has engaged does not fulfil its data protection obligations.

Should the participant process personal data, stored and/or otherwise processed by our organisation, in a manner inconsistent with this policy or for purposes other than the investigation of potential vulnerabilities in our organisation's systems, products and equipment, the participant acknowledges that he/she will be considered a data controller and will assume full responsibility for the processing carried out in this way.

 *[optional :*

1. ***Giving a reward***

*Our organisation undertakes to offer a reward to the participant under the following conditions:*

*[this reward must be clearly established in advance in this policy (depending on the number, importance or quality of the information provided)]*

*.....................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................*

*Any request for a reward outside the conditions defined by the CVDP may thus be considered as an illicit attempt at extortion].*

1. How to report a vulnerability ?
2. **Point of contact**

You should only send the information found to the following e-mail address

...................................................................................................................................................................[e.g. vulnerabilitypolicy@(organisation name).be ].

[option: email address of a bug bounty platform].

and/or by completing the following online form: [URL secured with HTTPS] .............................................................................

[option and/or by registering on the following bug bounty platform: [URL] .................................................................................................................................................................................]

Whenever possible, we invite you to use the following secure means of communication:

..................................................................................................................................................................................

[secure transmission using, for example, Transport Layer Security (TLS) or its predecessor Secure Sockets Layer (SSL) , Secure Multipurpose Internet Mail Extensions (S/MIME) or Pretty Good Privacy (PGP) with the following Key ID................................................................................]

You can also contact the department or person responsible for the policy at the following phone number(s):

…………………………………………………………………………………………………………………………………………………………….

1. **Information to communicate**

As soon as possible after the discovery, send us information on your findings using : [the form in Annex I] or [the online form available here (URL)].

1. Procedure
2. **Discovery**

Where a participant becomes aware of information relating to a potential vulnerability, the participant should, where possible, carry out prior checks to confirm the existence of the vulnerability and identify any risks involved.

1. **Notification**

The participant undertakes to notify, as soon as possible, technical information on possible vulnerabilities to the contact point (or coordinator (optional)), listed in point 3(a) of this policy. The participant must respect the designated secure means of communication.

Upon receipt of a notification, our organisation undertakes to send to the participant, as soon as possible, an acknowledgement of receipt, [with, if possible, its internal reference, a reminder of the main obligations of the CVDP] and the next steps of the procedure.

1. **Communication**

The parties undertake to make every effort to ensure continuous and effective communication. The information provided by the participant can be very useful in identifying and addressing the vulnerability.

In the absence of a reaction from one of the parties to the CVDP beyond a reasonable time, the parties can call upon the Centre for Cybersecurity Belgium (CBB) (vulnerabilityreport@cert.be), as coordinator (by default).

1. **Investigation**

The investigation phase will allow our organisation to replicate the environment and behaviour reported in order to verify the information reported.

Our organisation undertakes to keep the participant informed on a regular basis of the results of the investigations and the follow-up to the notification.

During this process, the parties will ensure that they make the link with similar or related reports, assess the risk and severity of the vulnerability, and identify any other affected products or systems.

1. **Development of a solution**

The objective of the disclosure policy is to enable the development of a solution to remove the vulnerability from the computer system before any damage is done.

Taking into account the state of knowledge, the costs of implementation, the seriousness of the risks to users and the technical constraints, our organisation will try to develop a solution within 90 calendar days.

In this phase, our organisation and its partners commit to carrying out positive tests to verify that the solution works properly and negative tests to ensure that the solution does not disrupt the proper functioning of other existing functionalities.

1. **Possible public disclosure**

Our organisation will decide, in coordination with the participant, on the modalities to eventually make public the existence of the vulnerability. This public disclosure should take place at the earliest possible time, together with the deployment of a solution and the distribution of a security notice to users.

In the event of a vulnerability that also affects other organisations, the responsible organisation must inform the Centre for Cybersecurity Belgium (vulnerabilityreport@cert.be) in any case, even if it does not want the vulnerability to be disclosed publicly.

Our organisation is also committed to collecting feedback from users on the deployment of the solution and to taking the necessary corrective measures to address any issues with the solution, including compatibility with other products or services.

1. Law applicable

Belgian law is applicable to any disputes arising from the application of this policy.

Optional:

The CCB (vulnerabilityreport@cert.be) may act as an intermediary in an attempt to reconcile our organisation and the participant for problems related to the application of this policy].

1. Duration

The rules of the policy are applicable from xx/xx/xxxx until they are modified or deleted by our organisation. Such changes or deletions will be published on our organisation's website and will apply automatically after a period of 30 days following their publication.

Date,

Place,

Signature, [person authorised to legally represent the organisation].

**Annex I : Form to report vulnerabilities**

Provide enough information to enable us to reproduce the problem and resolve it as quickly as possible.

We ask you to provide at least the following relevant information:

|  |  |
| --- | --- |
| Last name:First name: |  |
| (Address /Country) : |  |
| E-mail address:Phone number:  |  |
| Description of vulnerability: |  |
| Type of vulnerability: |  |
| Configuration details: |  |
| Operating system: |  |
| Operations performed (logs): |  |
| Tools used: |  |
| Dates and times of the tests: |  |
| IP address or URL of the system concerned: |  |
| In case of processing of personal data: | * Types of personal data accessed/processed:
* Categories of data subjects (customer, employee, supplier):
* Transfer of data to/access from a country outside the European Union or the European Economic Area?

If yes, please - indicate the country(ies) concerned:- return Annex II completed and signed.  |
| Any other relevant information: |  |
| Attachments (screenshots). |  |

**What do we do with your personal data?**

Please read our privacy policy available at [link or email address to be completed by the organisation]. If necessary, the organisation indicates below the specificities or derogations applicable to the processing of hackers' personal data compared to what is provided for in its "general" data protection policy].

**Annex II - Transfer of personal data by the participant to a country outside the European Union or European Economic Area.**

**To complete if necessary:** Annex I of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.