[POL] ISO27001 - Coordinated Vulnerability Disclosure Policy

ℹ️ Object and field of application

This policy is designed to enhance the performance and security of our networks and information systems.
It allows third parties, acting in good faith, to identify potential vulnerabilities in our systems, equipment, or products, or to share any relevant information they may discover.

However, access to our IT systems and equipment is permitted solely for the purpose of:

- Improving their security
- Reporting existing vulnerabilities
- Complying strictly with the conditions outlined in this document

🔎 Scope

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.
This policy applies to the following components that are currently within their supported lifecycle :

- All proprietary softwares and API's developed and maintained by Macq
- Firmwares and embedded systems in hardware developed and maintained by Macq
- Public web applications and portals under the *.macq.eu domain
- Exposed administration interfaces
- Cloud-based services and SaaS provided by Macq

Out of scope (systems or activities)

- Third-party platforms or software not owned or operated by Macq
- See article 1.2

Vulnerabilities affecting systems, software, or products that are no longer maintained or supported (i.e. out of lifecycle) are not covered by this policy, except in cases where they may still pose a significant risk to active environments.

Policy

1 - Mutual obligations of the parties

1.1 - Proportionality

In all his actions, the participant undertakes to scrupulously respect the principle of proportionality, i.e. not to disrupt the availability of the services provided by the system and not to use the vulnerability beyond what is strictly necessary to demonstrate the security flaw. Its attitude must remain proportionate: if the demonstration is established on a small scale, there is no need to extend it further.

The aim of our policy is not to allow the intentional acquisition of knowledge of the content of computer data, communications data or personal data, and such knowledge could only be acquired incidentally as part of the search for vulnerabilities.

1.2 - Prohibited actions

Participants may not take any of the following actions :

- copying, modifying or deleting data from the computer system.
- modifying the parameters of the computer system.
- Installing malicious software (malware): viruses, worms, Trojan horses, or similar.
- Distributed Denial Of Service (DDOS) attacks.
- social engineering attacks.
- phishing attacks.
- spamming attacks.
- the installation of a device enabling the interception, reading or recording of a communication not accessible to the public or of an electronic communication.
- intentionally intercepting, recording or acquiring knowledge of a communication not accessible to the public or an electronic communication.
- the use, possession, revelation, use or intentional disclosure of the content of communications not accessible to the public or of data from a computer system, which the participant could not reasonably be unaware had been obtained illegally.
- Use of automated vulnerability scanners or intrusive testing tools without prior coordination

1.3 - Confidentiality

The participant must strictly refrain from sharing or disclosing to third parties any information collected under our policy, 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).

1.4 - Good faith execution

Our organisation undertakes to implement this policy in good faith and not to take legal action, either civil or criminal, against any participant who complies with its conditions.
The participant must be devoid of fraudulent intent, malicious intent, intent to use or cause damage to the system visited or to its data. This also applies to third-party systems located in Belgium or abroad.
If in doubt about any of the conditions of our policy, the participant must first ask our contact point and obtain its written agreement before taking any action.

1.5 - Processing of personal data

The goal of a CVDP is not to process personal data. However, during vulnerability research, participants may incidentally come across or process such data.

1.5.1 - What is personal data?

Personal data refers to any information that can directly or indirectly identify a person. For example, names, email addresses, IP addresses, or location data.
Processing includes any action such as storing, modifying, consulting, or sharing this data.

1.5.2 - Rules for Handling Personal Data

If a participant processes personal data while searching for vulnerabilities, the following rules apply:

- **Purpose limitation**: Data must only be processed to identify vulnerabilities in our systems, equipment, or products. Any other use is forbidden.

- **Minimization**: Only process personal data that is strictly necessary.
- **Confidentiality**: Ensure that anyone with access to the data is bound by a confidentiality agreement or legal obligation.
- **Security**: Apply technical and organizational measures (e.g., encryption) to protect the data based on the level of risk.
- **Competence**: The participant must have the necessary expertise to handle our systems securely and in accordance with applicable laws.
- **Cooperation**: The participant agrees to help us meet our legal data protection obligations, such as supporting data subjects' rights and conducting impact assessments.
- **Incident notification**: If the participant becomes aware of a data breach, they must inform us as soon as possible at securityreports@macq.eu.
- **Data retention**: Personal data must not be kept longer than necessary. It must be stored securely during use (preferably encrypted) and deleted immediately once the work is completed.
- **Documentation**: The participant must keep a record of the types of personal data processed and the security measures applied, as required by Article 30(2) of the GDPR.
- **Third parties**: If the participant works with others, they must ensure those third parties follow this policy, especially regarding confidentiality and data security.
  The participant remains fully responsible for any failure on the third party's part.

Finally, if the participant processes personal data, stored and/or otherwise processed by our organisation, in a way that is incompatible with this policy or for purposes other than the search for potential vulnerabilities in our organisation's systems, products and equipment, the participant acknowledges that it will be considered as a data controller and will assume full responsibility for such processing.

1.5 - Rewards and Recognition

At this time, no monetary or material rewards are planned for participants.
However, with the participant's explicit consent, we may publicly acknowledge their contribution by listing their name or pseudonym on a *Wall of Fame* or similar recognition page.
This recognition is optional and does not constitute a right or obligation on the part of our organisation.

2 - How to report security vulnerabilities

All communication related to vulnerability disclosures must be carried out exclusively via email at the following address : securityreports@macq.eu.

If your message or any attachment contains sensitive or confidential information, you are required to encrypt only the content using the following PGP public keys : Macq Security Reports_0x1F8C96F8_public.asc
This helps ensure that any sensitive data shared with us remains protected during transmission.

2.1 - Information to be provided

As soon as possible after identifying a potential vulnerability, please send us all relevant information by email,
You may use your own templates, provided that all the information listed below is included. Alternatively, you can use the table provided :

Last name :	*Your family name (surname).*
First name :	*Your given name.*
(Address/Country) :	*Optional - But precise at least your country of residence.*

Email Address :	*Where we can contact you securely.*
Phone Number :	*Optional. Only if you agree to be contacted by phone.*
Vulnerability Description :	*Describe clearly what the vulnerability is and how it affects the system.*
Type of Vulnerability :	*E.g. XSS, SQL injection, privilege escalation, etc.*
Configuration Details :	*Details about the environment or setup where the vulnerability was observed.*
Operating System :	*Name and version of the operating system used during testing.*
Actions Performed (Logs) :	*Describe the steps taken and, if possible, provide logs or command lines used.*
Tools Used :	*List any tools or software used during testing.*
Dates and Times of Testing :	*Specify when the tests were conducted (date and time).*
IP Address or URL of the Affected System :	*Provide the exact IP or URL where the vulnerability was found.*
If Personal Data Was Processed :	1. *Types of personal data accessed/processed :* *Ex : names, email addresses, login details.* 2. *Categories of data subjects (ex: customer, employee, supplier):* 3. *Was data transferred to or accessed from outside the EU/EEA?* ◦ *If yes, specify the countries involved.*
Any Other Relevant Information :	*Add anything that may help us understand or reproduce the issue.*
Attachments (screenshots):	*Include any supporting files, such as screenshots, logs, or scripts. sensitive or confidential information are required to be encrypted*

3 - Operation

3.1 - Discovery

When a Participant discovers information relating to a potential vulnerability, it should, as far as possible, carry out prior checks to confirm the existence of the vulnerability and identify any risks involved.

3.2 - Notification

The participant undertakes to notify, as soon as possible, technical information on any vulnerabilities to the contact point by respecting the designated secure means of communication.
When it receives a notification, our organisation undertakes to send the participant, as soon as possible, an acknowledgement of receipt.

3.3 - Communication

The parties commit to maintaining continuous and effective communication throughout the process.
Information shared by the participant can play a key role in identifying the vulnerability and helping to develop a solution.

3.4 - Investigation

The investigation phase will enable our organisation to reproduce the environment and behavior reported in order to verify the information communicated.
Our organisation undertakes to keep the participant regularly informed of the results of the investigations and the action taken on the notification.
During this process, the parties will take care to make the link with similar or related notifications, to assess the risk and the seriousness of the vulnerability, and to identify any other affected products or systems.

3.5 - Development of a solution

The objective of the disclosure policy is to enable the development of a solution to eliminate the vulnerability in the IT system, before any damage is caused.

Taking into account the state of knowledge, implementation costs, the seriousness of the risks incurred by users and technical constraints, our organisation will attempt to develop a solution within 45 calendar days at the latest. During this phase, our organisation and its partners undertake to carry out both positive tests to check that the solution works correctly and negative tests to ensure that the solution does not disrupt the correct operation of other existing functionalities.

3.6 - Possible public disclosure

Our organisation will decide, in coordination with the participant, how to make the existence of the vulnerability public.
This public disclosure should take place at the earliest possible time, at the same time as 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 organisation responsible must inform the Centre for Cybersecurity Belgium (vulnerabilityreport@cert.be) in any event, even if it does not wish the vulnerability to be disclosed publicly.

Our organisation also undertakes to gather feedback from users on the deployment of the solution and to take the necessary corrective measures to resolve any problems posed by the solution, particularly in terms of compatibility with other products or services.

3.6 - Applicable law

Belgian law is applicable to disputes arising from the application of this policy.
The CCB (vulnerabilityreport@cert.be) may act as an intermediary to try to reconcile our organisation and the participant for problems relating to the application of this policy.

4 - Implementation

To support our Coordinated Vulnerability Disclosure Policy (CVDP), a dedicated web page will be made available on our website.
This page will present a simplified version of the policy, written in accessible language to help researchers and third parties understand the essential guidelines.
The full version of the policy will be available for download in PDF format directly from this page.

In addition, the page may include a Wall of Fame, listing contributors who have responsibly reported vulnerabilities, subject to their prior consent.

To further facilitate communication and ensure visibility for security researchers, we will also configure and publish a security.txt file at the root of our main domain.
This file will contain our contact information and a link to the dedicated page.