see Telecom

Coordinated Vulnerability Disclosure Policy

1 SCOPE OF THE POLICY

To improve the performance and security of our networks and information systems, we have chosen to adopt a coordinated vulnerability disclosure policy. This policy allows participants to search, in good faith, for potential vulnerabilities in our organisation's systems, equipment and products, or to provide us with any information discovered regarding a vulnerability.

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

Our policy covers 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 authorised to enter or attempt to enter data into our IT system, in accordance with the purposes and conditions set out in this policy.

This applies to all SEE Telecom products and services.

Systems operated by third parties are excluded from the scope of this policy, unless such third parties have explicitly and previously agreed to these rules.

Any searches carried out by the participant on information systems not explicitly covered by this policy may result in legal proceedings being brought against them.

2 THE MUTUAL OBLIGATIONS OF THE PARTIES

2.1 PROPORTIONALITY

The participant undertakes, in all their actions, to scrupulously respect the principle of proportionality not to disrupt the availability of the services provided by the system and not to exploit the vulnerability beyond what is strictly necessary to demonstrate the security flaw. Their approach 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 permit the intentional disclosure of the content of computer data, communications data or personal data, and such disclosure may only occur incidentally during vulnerability research.

2.2 PROHIBITED ACTIONS

Participants must not engage in the following actions:

- copying, modifying or deleting data from the computer system;
- altering the settings of the computer system;
- installing malicious software (malware): viruses, worms, Trojan horses or other;
- distributed denial-of-service (DDOS) attacks;
- social engineering attacks;
- phishing attacks;
- spam attacks;
- the theft of passwords or brute-force attacks;
- the installation of devices enabling the interception, monitoring or recording of communications not accessible to the public or of electronic communications;
- the interception, recording or intentional access to non-public communications or electronic communications;
- the intentional use, possession, disclosure or dissemination of the content of non-public communications or data from a computer system, where the participant cannot reasonably be unaware that such content or data has been obtained unlawfully;

If a participant wishes to seek assistance from a third party in carrying out their research, they must ensure that the third party has read this policy in advance and, by offering their assistance, agrees to comply with its terms.

2.3 CONFIDENTIALITY

Participants must strictly refrain from sharing or disclosing to third parties any information gathered under our policy without our prior and explicit consent.

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

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

2.4 ACTION IN GOOD FAITH

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

The participant must have no fraudulent intent, no intention to cause harm, and no desire to use or cause damage to the system visited or its data. This also applies to third-party systems located in Belgium or abroad.

In the event of any doubt regarding any of the terms of our policy, the participant must first consult our point of contact and obtain their written consent before taking any action.

The participant may work with a third party to carry out their research. The participant must ensure that the third party has read this policy in advance and, by offering their assistance, agrees to comply with its terms, including confidentiality and the implementation of appropriate security measures. The participant acknowledges that they remain fully liable to our organisation should the third party they have engaged fail to fulfil their 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 identification of potential vulnerabilities in our organisation's systems, products and equipment, the participant acknowledges that they will be regarded as a data controller and will assume full responsibility for the processing carried out in that capacity.

3 HOW TO REPORT SECURITY VULNERABILITIES?

3.1 POINT OF CONTACT

Whether anonymously or not, you must submit any information discovered exclusively via the 'Vulnerability Report' page on the website www.seetelecom.com.

3.2 INFORMATION TO BE PROVIDED

As soon as possible after discovery, please send us details of your findings using the web form provided on the web site www.seetelecom.com.

4 THE PROCEDURE

4.1 DISCOVERY

When a participant discovers information relating to a potential vulnerability, they should, where possible, first carry out checks to confirm the existence of the vulnerability and identify any potential risks involved

4.2 NOTIFICATION

The participant undertakes to notify the contact point, as set out in point 3.1 of this policy, of any technical information regarding potential vulnerabilities as soon as possible. The participant must use the designated secure communication channels.

Upon receiving a notification, our organisation undertakes to send the participant, as soon as possible, an acknowledgement of receipt, including, where possible, its internal reference number, a reminder of the main obligations under the CVDP and the next steps in the procedure.

4.3 COMMUNICATION

The parties undertake to do their utmost to ensure continuous and effective communication. The information provided by the participant may, in fact, prove very useful in identifying the vulnerability and resolving it.

The processing of personal data[1]

The purpose of a CVDP is not to intentionally process personal data, but it is possible that a participant may, even inadvertently, process personal data during their vulnerability research.

However, the processing of personal data is broad in scope and includes the storage, modification, retrieval, consultation, use or disclosure of any information relating to an identified or identifiable natural person. Whether a person is 'identifiable' does not depend on the mere intention of the data controller to identify them, but on the possibility of identifying the person, directly or indirectly, using such data (for example: an email address, identification number, online identifier, IP address or location data).

It is therefore possible that the participant may process personal data to a limited extent. If such data is processed, 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 our organisation's instructions, as set out in this policy, and exclusively for the purpose of identifying vulnerabilities in our organisation's systems, equipment or products. Any processing of personal data for any other purpose is prohibited.
- The participant undertakes to limit the processing of personal data to what is necessary for the purpose of vulnerability research.
- The participant shall ensure that persons authorised to process personal data undertake to maintain confidentiality or are subject to an appropriate legal duty of confidentiality.
- The participant shall implement appropriate technical and organisational measures to ensure a level of security commensurate with the risk (e.g. encryption). The participant declares that they understand the risks associated with the implementation of this policy and that they possess 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 considering the nature of the processing and the information available to the participant, in fulfilling our obligations regarding the exercise of data subjects' rights, the security of processing and any impact assessments.
- The participant undertakes to inform us, as soon as possible after becoming aware of it, of any potential personal data breach[2] at the address [to be completed by the responsible organisation].
- The participant may not retain any personal data processed for longer than is necessary. During this period, the participant must ensure that such data is stored in a manner that guarantees a level of security appropriate to the risks involved (preferably in encrypted form). Upon the participant's withdrawal from the scheme, such data must be deleted immediately.
- The participant undertakes to maintain a record of the categories of processing activities carried out on behalf of our organisation, including a description of the security measures they have implemented, in accordance with Article 30(2) of the GDPR.

[1] EU Regulation 2016/679 of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (GDPR – General Data Protection Regulation).

[2] A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

If neither party to the CVDP responds within a reasonable timeframe, the parties may call upon the Belgian Cybersecurity Centre (CBB) (vulnerabilityreport@cert.be) to act as coordinator (by default).

a) Investigation

The investigation phase will enable our organisation to replicate the reported environment and behaviour to verify the information provided.

Our organisation undertakes to keep the participant regularly informed of the results of the investigations and the action taken in response to their report.

During this process, the parties will ensure that they cross-reference similar or related notifications, assess the risk and severity of the vulnerability, and identify any other products or systems that may be affected.

b) Development of a solution

The aim 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.

Considering the current state of knowledge, implementation costs, the severity of the risks faced by users and technical constraints, our organisation will endeavour to develop a solution within 90 calendar days at the latest.

During this phase, our organisation and its partners undertake to carry out, on the one hand, positive tests to verify that the solution works correctly and, on the other hand, negative tests to ensure that the solution does not disrupt the proper functioning of other existing features.

c) Possible public disclosure

Our organisation will decide, in consultation with the participant, on the procedures for any public disclosure of the vulnerability. Such public disclosure must take place, at the earliest, at the same time as the deployment of a solution and the issuance of a security advisory to users.

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

Our organisation also undertakes to gather user feedback on the deployment of the solution and to take the necessary corrective measures to resolve any issues arising from the solution, particularly those relating to compatibility with other products or services.

5 GOVERNING LAW

Belgian law shall apply to any disputes arising from the application of this policy.

The CCB (vulnerabilityreport@cert.be) may act as a mediator to attempt to reconcile our organisation and the participant regarding issues arising from the application of this policy.

6 EFFECTIVE DATE AND DURATION

The rules of this policy shall apply from June 1st, 2026, until they are amended or repealed by our organisation. Any such amendments or repeals will be published on our organisation's website and shall automatically come into effect 30 days after their publication.

Date: May 11th, 2026

Place: Baulers, Belgium

Signature

Guy Spillebeen
C.E.O.

Danny Larbouillat
C.I.S.O.