



Policy for the coordinated disclosure of vulnerabilities

This document describes the policy for the coordinated disclosure of vulnerabilities (hereinafter: "the Policy") of the National Railway Company of Belgium (with registered office at Rue de France 56, 1060 Brussels, and company number 0203.430.576) and its affiliated companies, (hereinafter: "**SNCB-NMBS**"). Any person who (themselves or via a third party) detects, investigates and/or discloses vulnerabilities in the network and information systems of SNCB-NMBS (hereinafter: "**the Participant**") must do so strictly in accordance with this Policy. In the event that this Policy conflicts with other agreements entered into by SNCB-NMBS, the provisions of this Policy shall prevail (unless SNCB-NMBS has expressly agreed in writing that a derogation from any part of this Policy is permitted).

1. Scope of application of this Policy

1.1. SNCB-NMBS implemented this Policy out of a concern to improve the performance and security of the network and information systems of SNCB-NMBS and/or used on behalf of, SNCB-NMBS (hereinafter: "the Systems"). Participants with good intentions may detect and identify potential vulnerabilities in SNCB-NMBS's systems, and provide information about vulnerabilities to SNCB-NMBS. These concern security vulnerabilities that may be exploited by third parties or that may disrupt the proper functioning of the products, services or systems of SNCB-NMBS.

1.2. SNCB-NMBS only grants access to the systems and only allows Participants to enter (or attempt to enter) data into the systems for the purpose of enhancing the security of SNCB-NMBS and informing SNCB-NMBS of existing vulnerabilities, strictly in accordance with the terms of this Policy.

1.3. Only the following systems of SNCB-NMBS are included within the scope of this Policy:

- (a) Public accessible websites;
- (b) Public accessible (mobile) applications.

1.4. All SNCB-NMBS systems not explicitly identified in Article 1.2 are not included within the scope of this Policy.

1.5. In addition, systems that rely on third parties are also outside the scope of this Policy unless those third parties expressly agree to this Policy in advance or the Participant complies with the applicable policies of those third parties.

1.6. Any investigation regarding systems (or parts of systems) not expressly identified in Article 1.2, and any other violation of this Policy may result in contractual, extra-contractual and/or criminal liability and/or in the prosecution of the Participant concerned under applicable law. Nothing in this Policy shall limit the right of SNCB-NMBS to seek injunctive, provisional or protective relief in a court of competent jurisdiction. The Participant shall indemnify and hold SNCB-NMBS harmless in respect of any claim and all damage or losses in the broadest sense, arising out of, as a result of or in connection with any violation of this Policy.



1.7. This Policy shall be interpreted in accordance with Articles 8, 22, 23 and 30 §3, 11° of the Act of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security (the NIS2 Act).

2. Mutual obligations of the parties

2.1. The Participant shall act in good faith and within the purpose of this Policy. The Participant is prohibited from investigating systems and detecting vulnerabilities in systems based on confidential information of or about SNCB-NMBS that is obtained unlawfully or lawfully by the Participant or by any third party, pursuant to any employment with or provision of services to SNCB-NMBS.

2.2. The Participant undertakes to scrupulously observe the principle of proportionality in all its activities. Amongst other things, this means that the Participant must not disrupt the availability of the services provided by the systems and that the Participant must not exploit the vulnerability beyond what is strictly necessary to demonstrate the security problem. The Participant's attitude must remain proportionate: if it has been demonstrated that the scale of the problem is small, the Participant should take no further action.

2.3. This Policy in no way grants the Participant the right to intentionally intercept, observe, inspect, read, record, store or otherwise process the content of information technology data, communications data or personal data belonging to SNCB-NMBS.

2.4. The Participant is not allowed to perform the following actions: (i) to copy or modify data from the systems or delete data from the systems; (ii) to change the settings of the systems; (iii) to install malware (i.e.: viruses, worms, Trojan horses, etc.) or similar software that disables the functionality of the SNCB-NMBS systems; (iv) to carry out "denial of service" attacks (Distributed Denial Of Service - DDOS); (v) to carry out "social engineering" attacks; (vi) to carry out phishing attacks; (vii) to carry out junk mail attacks (spamming); (viii) to carry out password theft or "brute force" attacks; (ix) to use any other destructive method in searching for vulnerabilities; (x) to install a device that allows the interception, storage or knowledge of non-publicly available communications or electronic communications; (xi) to intentionally intercept, intercept or store non-publicly available communications or electronic communications; (xii) to intentionally use, store, communicate or distribute the content of communications that is not publicly available or data from a system that the Participant should have reasonably known were obtained illegally.

2.5. If the Participant is assisted by a third party while carrying out its investigation, the Participant must ensure and affirm that the third party has prior knowledge of this Policy and agrees to comply with these terms when assisting the Participant.

2.6. Under no circumstances shall the Participant share with or distribute to third parties any information collected under this Policy, except where expressly agreed in writing with SNCB-NMBS and, where relevant, in accordance with Article 5.5 (*public announcement*).

2.7. The Participant is not allowed to transmit or distribute information technology data, communications data or personal data to third parties.

2.8. If the vulnerability could reasonably affect other organisations in Belgium, SNCB-NMBS can report it to the Centre for Cyber Security Belgium (CCB) (vulnerabilityreport@cert.be), in accordance with Article 1.1(d). If the Participant decides to carry out such reporting themselves, the Participant shall inform SNCB-NMBS of this.



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

2.10. In case of doubt about certain terms of this Policy, the Participant shall contact SNCB-NMBS in advance by email at the address disclose@belgiantrain.be and obtain written permission before acting.

3. Processing of personal data

3.1. This Policy is not intended to result in any Processing of Personal Data. However, the Participant may, even accidentally, need to Process Personal Data as part of its investigation into vulnerabilities. If so, Participants shall Process such Personal Data in accordance with what is set forth below.

3.2. The following definitions must be observed:

(a) **"Data Protection Legislation"** means any legal regulation of the European Union and/or its Member States, including, but not limited to, laws, Directives and Regulations, for the protection of Personal Data, in particular the GDPR.

(b) **"GDPR"** means 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 (General Data Protection Regulation).

3.3. The terms **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"** and **"Processing"** have the same meaning as in the Data Protection legislation.

3.4. In the context of this Policy, Processing by the Participant and/or its affiliates and employees may include identification data, technical data, data on personal characteristics and data relating to the relationship and occupation of the Data Subjects, as well as any other type of (sensitive) data with which the Participant may come into contact in accordance with the nature of the activities that are the subject of this Policy and for the purpose of carrying out those activities. In principle, the Data Subjects covered by this Policy are (i) SNCB-NMBS employees or appointees using the services and (ii) customers or suppliers of SNCB-NMBS and their employees or appointees. The Participant is therefore allowed to process Personal Data in a limited and ongoing manner for the duration of the services performed by the Participant in accordance with this Policy, and the Participant shall retain such data only for as long as is necessary to fulfil the purpose of the services described above. When processing such data, the Participant undertakes to comply with the legal obligations regarding the protection of Personal Data, as well as the provisions of this Policy, in particular:

(a) The Participant shall Process Personal Data only in accordance with the instructions from SNCB-NMBS specified in this Policy, and only for the purpose of detecting vulnerabilities in the systems. Any Processing of Personal Data for any other purpose is excluded, including with regard to the transfer of Personal Data to a third country or an international organisation, unless required by the applicable legislation; in such a case, the Participant shall inform SNCB-NMBS of this legal



obligation prior to the Processing, unless such law prohibits it being informed of this on the grounds of public interest.

(b) The Participant undertakes to limit the Processing of Personal Data to what is strictly necessary in order to detect vulnerabilities.

(c) The Participant shall ensure that those authorised to Process Personal Data have undertaken to uphold confidentiality or are bound by an appropriate statutory obligation to uphold confidentiality.

(d) The Participant undertakes to comply with the conditions set forth in this Policy and in particular in Article 3.5 when engaging another processor.

(e) The Participant shall take appropriate technical and organisational measures to ensure a level of security appropriate to the risk (such as, for example, encryption), in accordance with Article 32 of the GDPR. This shall include, where applicable, (i) the pseudonymisation and encryption of Personal Data, (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (iii) the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident, and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure that Processing is carried out securely.

(f) The Participant declares that it understands the risks associated with the implementation of this Policy and that it has the expertise and experience necessary to test the systems in a safe and legally compliant manner.

(g) To the extent possible and taking into account the nature of the Processing and the information available to it, the Participant undertakes to assist SNCB-NMBS in the performance of its obligations with regard to the exercise of the rights of Data Subjects, the security of the Processing and any impact analysis.

(h) The Participant undertakes to inform SNCB-NMBS by email at dataprotectionofficer@belgiantrain.be as soon as possible after becoming aware of a possible Personal Data breach.

(i) The Participant is not allowed to retain Personal Data for longer than necessary. During this period, the Participant must provide a level of security that is commensurate with the risk (preferably encrypted). Upon termination of participation in this Policy, the Personal Data concerned must be deleted immediately, unless the Participant is required to retain them under applicable European Union or national law.

(j) The Participant undertakes to keep a register of the Processing activities it has carried out on behalf of SNCB-NMBS. That register shall contain a description of the security measures taken by the Participant, in accordance with Article 30 §2 of the GDPR.

(k) The Participant shall make available to SNCB-NMBS all information necessary to demonstrate compliance with the obligations of this Article 3 and shall cooperate with audits, including inspections, conducted by SNCB-NMBS, by another auditor commissioned by SNCB-NMBS and/or by any competent authority.



3.5. The Participant may have recourse to third parties in order to carry out its investigation. In such cases, the Participant shall ensure that such third party has prior knowledge of this Policy and agrees to comply with the terms of the Policy when providing assistance, including confidentiality, the implementation of appropriate security measures and the principles set forth in Article 3.4 regarding the scope, nature and duration of Processing. The Participant acknowledges that it remains fully liable to SNCB-NMBS if the third party on which it relies fails to meet its data protection obligations.

3.6. If the Participant processes Personal Data stored and/or otherwise processed by SNCB-NMBS in a manner contrary to this Policy or for purposes other than detecting possible vulnerabilities in the systems, the Participant acknowledges that it will be considered to be the controller of the Processing and will be fully liable for the Processing performed by it in that context. The Participant shall indemnify and fully hold SNCB-NMBS harmless against any claim by a Data Subject or other third party and all related damage or losses incurred by SNCB-NMBS in relation to any breach by the Participant (or by any third party for which the Participant is responsible) of its obligations with regard to the Processing Personal Data.

4. Rewards

4.1. SNCB-NMBS undertakes to grant a reward to the Participant under the following conditions:

- (a) The vulnerability was not yet known within SNCB-NMBS;
- (b) The vulnerability had not previously been reported by a person other than the Participant;
- (c) The notification was complete and was made in accordance with this Policy.

4.2. SNCB-NMBS reserves the right to determine the form of such rewards at its discretion.

4.3. Any request for a reward beyond these terms shall be treated as an illegal attempt at extortion.



5. Procedure

5.1. Discovery

Whenever the Participant discovers information about a vulnerability, the Participant shall, to an extent that is reasonably practicable, perform prior checks to confirm the existence of the vulnerability and identify any risks. After carrying out this initial assessment of the inherent risk posed by these vulnerabilities, the Participant shall contact SNCB-NMBS as soon as reasonably possible in accordance with Article 5.2.

5.2. Notification

- (a) The Participant shall send any information about identified vulnerabilities to SNCB-NMBS at the address disclose@belgiantrain.be.
- (b) The Participant shall follow the following guidelines when forwarding information:
 - (i) The Participant shall communicate in Dutch, French or English.
 - (ii) The Participant shall use the form included in 0 (*Annex 1: Vulnerability Report*) and shall provide all information in its possession that is requested therein. The vulnerabilities identified shall be described fully and in detail, including IP addresses, logs, screenshots, affected URLs, etc. It is important that SNCB-NMBS can find the vulnerability itself in order to eliminate it.
 - (iii) The Participant expressly confirms that no confidential information (whether obtained directly or indirectly, lawfully or unlawfully) from or about SNCB was used when detecting or determining the vulnerability.
 - (iv) The Participant shall provide relevant contact information if requested so that SNCB-NMBS can follow up the report with the Participant in more detail.
- (c) On receiving a notification, SNCB-NMBS undertakes to send a confirmation of receipt to the Participant as soon as possible, together with details of the next steps of the procedure.

5.3. Communication

- (a) The parties undertake to make every effort to ensure continuous and effective communication for the purpose of identifying and resolving the vulnerability that was identified and reported.
- (b) If no response from either party is forthcoming after a reasonable period of time, the parties may have recourse to the Centre for Cybersecurity Belgium (CCB) (vulnerabilityreport@cert.be) in its capacity as the (standard) coordinator.

5.4. Investigation and objective

- (a) During the investigation phase, SNCB-NMBS shall reproduce the Participant's environment and identified behaviour in order to verify the information provided.
- (b) SNCB-NMBS shall keep the Participant informed on a regular basis of the results of this survey and of the actions taken as a result of that information.
- (c) During that process, the parties shall take similar or related reports into account, assess the risk and severity of the identified vulnerability and identify any other products or systems affected.



(d) This Policy aims to enable the development of a solution in order to resolve system vulnerabilities before (further) damage is done.

5.5. Public announcement

- (a) SNCB-NMBS shall decide, after hearing the views of the Participant, how the existence of any vulnerability will be disclosed.
- (b) In no case shall a public announcement be made before a solution has been implemented and a security notice can be distributed to affected users.
- (c) No disclosure whatsoever is permitted without the express written permission of SNCB-NMBS.
- (d) If a vulnerability also affects other organisations, SNCB-NMBS shall report it to the CCB (vulnerabilityreport@cert.be).

6. Applicable law

6.1. This Policy shall be governed by and interpreted in accordance with Belgian law. All disputes concerning the validity, interpretation or implementation of this Policy shall be finally settled by the competent courts of Brussels.

6.2. The CCB (vulnerabilityreport@cert.be) may act as a mediator between SNCB-NMBS and the Participant in the event of disputes relating to the application of this Policy.

7. Duration

7.1. This Policy shall enter into force from 02/04/2026 onwards and will remain in effect until SNCB-NMBS announces a change in accordance with Article 0.

7.2. SNCB-NMBS is entitled to modify or terminate this Policy. SNCB-NMBS shall announce material changes to this Policy by publication on the SNCB-NMBS website. Unless otherwise expressly stated by SNCB-NMBS, amendments to this Policy shall become effective thirty (30) days after publication.



Annex 1: Vulnerability Report

Surname:	
First name:	
(Address/Country):	
Email address:	
Phone number:	
Description of vulnerability:	
Type of vulnerability:	
Configuration details:	
Operating system:	
Operations performed (logs):	
Tools used:	
Dates and times of testing:	
IP address or URL of the affected system:	
If personal data is processed:	• Types of Personal Data consulted/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: - indicate the country or countries involved: - return the completed and signed Annex II.
Any other relevant information:	
Attachments (screenshots).	
Reported to the CCB	If the vulnerability has also been reported to the CCB, please provide the date of reporting.
By transmitting this information, as a Participant in SNCB-NMBS's Policy for the Coordinated Disclosure of Vulnerabilities, I expressly confirm that my investigation and the above information obtained as a result of my research are in no way, either directly or indirectly, based on or the result of confidential information from or about SNCB-NMBS.	



Annex 2: Transfer of Personal Data outside the EU and the EEA (Modal contractual provisions).

When the Participant is authorised by SNCB-NMBS to transfer Personal Data from SNCB-NMBS to the Participant or an affiliate of the Participant (or any further transfer), in any case, where such transfer would be prohibited by Regulation (EU) 2016/679 without the protection for the Personal Data transferred provided by the standard contractual clauses set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by any competent authority under applicable data protection laws and regulations in the EEA ("EEA Standard Contractual Clauses"), it is hereby expressly agreed between SNCB-NMBS (hereinafter: "the Data Exporter") and the Participant or any of the Participant's affiliates (each in the capacity of "Data Importer") that the applicable Module 2 of the EEA Standard Contractual Clauses ("EEA Standard Contractual Clauses for Transfers Between Controller and Processor"), which are hereby incorporated by reference, shall apply from the commencement of the relevant transfer, and both SNCB-NMBS and the Participant confirm that:

- Clause 7 (Docking) of the standard contractual clauses shall apply;
- Clause 9 (Use of sub-processors) shall apply and the "time period" shall be 1 month;
- In Clause 11(a) (Redress), the optional text shall not apply;
- Under Clause 13(a) (Supervision), the following text is selected: *"The supervisory authority that supervises the data exporter's compliance with Regulation (EU) 2016/679 with respect to data transfers, as indicated in Annex I.C, shall act as the competent supervisory authority"*;
- "Option 1" under Clause 17 (Applicable law) shall apply and the "Member State" shall be Belgium;
- In Clause 18 (Choice of forum and jurisdiction), the Member State Shall be Belgium;
- Annex 1 to Module 2 shall be deemed to have been pre-completed with the relevant information of Article 3.4 from this Policy; the parties shall be the data exporter and the data importer(s), the supervisory authority shall be the Belgian *Data Protection Authority*, and the Processing operations shall be deemed to have been described in this Policy; and
- Annex 2 of Module 2 shall be deemed to have been pre-completed with the relevant information from Articles 0 and 0 of this Policy.