Politique relative à la divulgation coordonnée des vulnérabilités

Le présent document décrit la politique relative à la divulgation coordonnée des vulnérabilités (ci-après dénommée la "Politique") de la Société Nationale des Chemins de fer Belges (dont le siège est établi rue de France 56, à 1060 Bruxelles, et inscrite sous le numéro d'entreprise 0203.430.576) et de ses entreprises liées (**'La SNCB'**). Toute personne qui (elle-même ou par l'intermédiaire d'un tiers) détecte, recherche et/ou divulgue des vulnérabilités présentes dans les systèmes de réseaux et d'information de la SNCB (ci-après dénommé le **"Participant"**) doit le faire en stricte conformité avec la présente Politique. En cas de conflit entre la présente Politique et d'autres conventions conclues par la SNCB, ce sont les dispositions reprises dans la présente Politique qui prévalent (sauf convention écrite formelle de la SNCB stipulant qu'il peut être dérogé à l'une des dispositions de cette Politique).

1. Champ d'application de la présente Politique

1.1 La SNCB a instauré cette Politique par souci d'amélioration de la performance et de la sécurité des systèmes de réseaux et d'information de la SNCB et/ou utilisés pour le compte de celle-ci (ci-après dénommés les "Systèmes"). Ainsi, les Participants bien intentionnés peuvent détecter et identifier d'éventuelles vulnérabilités dans les systèmes de la SNCB, et transmettre à cette dernière les informations concernant ces vulnérabilités. Il s'agit des vulnérabilités de sécurité qui pourraient être exploitées à mauvais escient par des tiers ou perturber le bon fonctionnement des produits, services ou systèmes de la SNCB.

1.2 La SNCB n'accorde l'accès aux systèmes et n'autorise les Participants à y encoder (ou tenter d'y encoder) des données que dans le but de renforcer la sécurité de la SNCB et de l'informer des vulnérabilités existantes, et ce dans le strict respect des conditions stipulées dans la présente Politique.

1.3 Seuls les systèmes suivants de la SNCB relèvent du champ d'application de la présente Politique :

(a) Sites web accessibles au public ;

(b) Applications (mobiles) accessibles au public.

1.4 Tous les systèmes de la SNCB qui ne sont pas expressément identifiés à l'article 1.3 ne relèvent pas du champ d'application de la présente Politique.

1.5 En outre, les systèmes dépendant de tiers sont également exclus du champ d'application de cette Politique, sauf si ces tiers acceptent expressément cette Politique au préalable, ou si le Participant se conforme à la politique applicable de ces tiers.

1.6 Toute recherche portant sur des (parties de) systèmes qui n'ont pas expressément été identifiés à l'article 1.3, ainsi que toute autre violation de la présente Politique, peut engager la responsabilité contractuelle, extracontractuelle et/ou pénale et/ou des poursuites du Participant concerné en vertu de la législation applicable. Rien dans la présente Politique ne limite le droit de la SNCB d'intenter une action devant une juridiction compétente en vue de mesures urgentes, provisoires ou conservatoires. Le Participant préserve et indemnise la SNCB contre toute action en justice et tout dommage, au sens large du terme, résultant de, découlant de ou lié à toute violation de la présente Politique.

1.7 Cette Politique est interprétée conformément aux articles 8, 22, 23 et 30, §3, 11°, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (Loi NIS2).

2. Obligations réciproques des parties

2.1. Le Participant agit en toute bonne foi et dans le respect de l'objet de la présente Politique. Le Participant n'est pas autorisé à rechercher des systèmes ou à détecter des vulnérabilités dans des systèmes sur la base d'informations confidentielles provenant de ou concernant la SNCB qui ont été obtenues de manière illégale ou qui ont été obtenues légalement par le Participant ou par un tiers dans le cadre de tout emploi occupé à la SNCB ou de toute prestation de services fournie à la SNCB.

2.2. Le Participant s'engage à respecter scrupuleusement le principe de proportionnalité dans le cadre de toutes ses activités. Cela implique, entre autres, que le Participant ne peut pas perturber la disponibilité des services fournis par les systèmes et qu'il ne peut pas exploiter la vulnérabilité en dehors de ce qui est strictement requis pour démontrer l'existence du problème de sécurité. L'attitude du Participant doit rester proportionnelle : s'il est démontré qu'il s'agit d'un problème à petite échelle, le Participant ne peut entreprendre aucune autre action.

2.3. La présente Politique n'accorde en aucun cas au Participant le droit d'intercepter, d'observer, d'inspecter, de lire, d'enregistrer, de stocker ou de traiter de quelque manière que ce soit, de manière intentionnelle, le contenu des données de technologie de l'information, des données de communication ou des données à caractère personnel de la SNCB.

2.4. Il est interdit au Participant d'effectuer les opérations suivantes : (i) copier ou modifier des données des systèmes, ou supprimer des données des systèmes ; (ii) modifier les paramètres des systèmes ; (iii) installer des logiciels malveillants (c.-à-d. : virus, vers, chevaux de Troie, …) ou des logiciels similaires désactivant la fonctionnalité des systèmes de la SNCB ; (iv) effectuer des attaques de type "denial of service" (Distributed Denial Of Service – DDOS) ; (v) effectuer des attaques de type "social engineering" ; (vi) effectuer des attaques de phishing ; (vii) effectuer des attaques de courriers indésirables (spamming) ; (viii) procéder à un vol de mot de passe ou à des attaques de type "brute force" ; (ix) utiliser toute autre méthode destructive lors de la recherche de vulnérabilités ; (x) installer un dispositif permettant d'intercepter, de stocker ou de prendre connaissance de communications non publiques ou de communications électroniques non publiques ; (xi) intercepter, capter ou stocker intentionnellement des communications non publiques ou des communications électroniques non publiques ; (xii) utiliser, stocker, communiquer ou diffuser intentionnellement le contenu de communications non publiques ou de données d'un système, alors que le Participant aurait raisonnablement dû savoir qu'elles avaient été obtenues illégalement.

2.5. Si le Participant est assisté par un tiers dans l'exécution de sa recherche, il doit veiller - et s'assurer - que ce dernier a préalablement pris connaissance de la présente Politique et accepte d'en respecter les conditions lorsqu'il assiste le Participant.

2.6. Le Participant ne peut en aucun cas partager ou diffuser à des tiers des informations collectées dans le cadre de la présente Politique, sauf convention écrite formelle avec la SNCB et, le cas échéant, conformément à l'article 5.5 (*annonce publique*).

2.7. Il est interdit au Participant de transmettre ou de diffuser à des tiers des données sur la technologie de l'information, des données de communications ou des données à caractère personnel.

2.8. S'il existe un risque raisonnable que la vulnérabilité puisse affecter d'autres organisations en Belgique, la SNCB peut le signaler au Centre pour la Cybersécurité Belgique ("CCB") (vulnerabilityreport@cert.be), conformément à l'article2.1(d). S'il prend personnellement la décision de faire un tel signalement, le Participant doit en informer la SNCB.

2.9. Dans le chef du Participant lui-même, il ne peut être question d'aucune intention frauduleuse, ni de volonté de nuire, ni de l'intention d'exploiter ou d'endommager le système consulté ou les données qu'il contient. Cela vaut également pour les systèmes de tiers, en Belgique ou à l'étranger.

2.10. En cas de doute concernant certaines conditions de la présente Politique, le Participant prendra préalablement contact avec la SNCB par e-mail à l'adresse : disclose@belgiantrain.be, afin d'obtenir une autorisation écrite avant d'agir.

3. Traitement des Données à caractère personnel

3.1. La présente Politique n'a pas pour objet de déboucher sur un quelconque Traitement de Données à caractère personnel. Il est toutefois possible que le Participant soit amené, même de manière fortuite, à traiter des Données à caractère personnel dans le cadre de sa recherche de vulnérabilités. Si tel est le cas, les Participants traitent ces Données à caractère personnel conformément à ce qui est exposé ci-dessus.

3.2. Les définitions suivantes doivent être prises en compte :

(a) **"Législation en matière de protection des données"** désigne toute réglementation de l'Union européenne et/ou de ses États membres, y compris, mais sans s'y limiter, les lois, les directives et règlements relatifs à la protection des Données à caractère personnel, en particulier le RGPD.

(b) **"RGPD"** désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données).

3.3. Les termes **"Personne concernée"**, **"Données à caractère personnel", "Violation de données à caractère personnel"** et **"Traitement(s)"** ont la même signification que dans la législation en matière de protection des données.

3.4. Dans le cadre de la présente Politique, le Traitement effectué par le Participant et/ou ses entreprises liées et son personnel peut porter sur des données d'identification, des données techniques, des données relatives aux caractéristiques personnelles et des données concernant la relation et la profession des Personnes concernées, ainsi que tout autre type de données (sensibles) avec lesquelles le Participant peut être amené à entrer en contact, conformément à la nature des activités faisant l'objet de la présente Politique et aux fins de l'exécution de ces activités. En principe, les Personnes concernées par la présente Politique sont (i) les collaborateurs·trices ou préposés de la SNCB qui utilisent les services et (ii) les clients ou fournisseurs de la SNCB et leurs collaborateurs·trices ou préposés. Le Participant est donc autorisé à traiter les Données à caractère personnel de manière limitée et de façon continue pendant toute la durée de sa prestation de services, conformément à la présente Politique, et le Participant ne conservera ces données que pendant la durée nécessaire à la réalisation de l'objet des services décrits ci-dessus. Lors du traitement de ces données, le

Participant s'engage à respecter les obligations légales en matière de protection des Données à caractère personnel, ainsi que les dispositions de la présente Politique, en particulier :

(a) Le Participant traitera les Données à caractère personnel uniquement conformément aux instructions de la SNCB qui ont été définies dans la présente Politique, et uniquement dans le but de détecter des vulnérabilités dans les systèmes. Tout Traitement de Données à caractère personnel à toute autre fin est exclu, y compris en ce qui concerne le transfert de Données à caractère personnel vers un pays tiers ou une organisation internationale, sauf si la législation applicable l'exige ; dans un tel cas, le Participant informera la SNCB de cette obligation légale avant le Traitement, à moins que cette législation n'interdise la communication de ces informations pour des raisons d'intérêt général.
(b) Le Participant s'engage à limiter le Traitement des Données à caractère personnel à ce qui est strictement nécessaire à la détection des vulnérabilités.
(c) Le Participant veille à ce que les personnes habilitées à traiter des Données à caractère personnel se soient engagées à respecter la confidentialité ou soient tenues à une obligation légale de confidentialité appropriée.
(d) Le Participant s'engage à respecter les conditions énoncées dans la présente Politique, et en particulier à l'article 3.5, lorsqu'il fait appel à un autre sous-traitant.
(e) Le Participant prend les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque (comme par exemple le chiffrement), conformément à l'article 32 du RGPD. Cela comprend notamment, le cas échéant, (i) la pseudonymisation et le chiffrement des Données à caractère personnel, (ii) la capacité à garantir la confidentialité, l'intégrité, la disponibilité et la résilience permanentes des systèmes et services de traitement, (iii) la capacité de rétablir à temps la disponibilité et l'accès aux Données à caractère personnel en cas d'incident physique ou technique et (iv) un processus permettant de tester, d'estimer et d'évaluer l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du Traitement.
(f) Le Participant déclare comprendre les risques liés à la mise en œuvre de la présente Politique et disposer de l'expertise et de l'expérience nécessaires pour tester les systèmes de manière sûre et conformément à la loi.
(g) Le Participant s'engage, dans la mesure du possible et compte tenu de la nature du Traitement et des informations dont il dispose, à assister la SNCB dans l'exécution de ses obligations relatives à l'exercice des droits des Personnes concernées, à la sécurité du Traitement et à l'éventuelle analyse d'impact.
(h) Le Participant s'engage à informer la SNCB le plus rapidement possible après avoir pris connaissance de toute violation éventuelle de Données à caractère personnel, en la notifiant à l'adresse dataprotectionofficer@belgiantrain.be.
(i) Le Participant ne peut pas conserver les Données à caractère personnel plus longtemps que nécessaire. Durant cette période, le Participant doit assurer un niveau de sécurité proportionnel au risque (de préférence de manière cryptée). Au terme de la participation à cette Politique, ces Données à caractère personnel devront immédiatement être effacées, sauf si le Participant est obligé de les conserver en vertu de la législation européenne ou du droit national applicable.
(j) Le Participant s'engage à tenir un registre des Activités de traitement qu'il a effectuées pour le compte de la SNCB. Ce registre contient une description des mesures de sécurité prises par le Participant, conformément à l'article 30 § 2 du RGPD.
(k) Le Participant met à la disposition de la SNCB toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article 3 et apporte son entière collaboration aux audits, y compris aux inspections, réalisés par la SNCB, un autre auditeur mandaté par la SNCB et/ou toute autre autorité compétente.

3.5. Le Participant peut faire appel à des tiers pour mener sa recherche. Dans ce cas, le Participant doit veiller à ce que ce tiers soit préalablement informé de la présente Politique et qu'il s'engage à respecter, dans le cadre de l'assistance fournie, les conditions de la Politique, y compris la confidentialité, la mise en œuvre de mesures de sécurité appropriées et les principes stipulés à l'article 3.3 concernant l'étendue, la nature et la durée du Traitement. Le Participant reconnaît qu'il reste entièrement responsable vis-à-vis de la SNCB si le tiers auquel il fait confiance ne respecte pas ses obligations en matière de protection des données.

3.6. Si le Participant traite des Données à caractère personnel stockées par la SNCB et/ou traitées différemment de manière contraire à la présente Politique ou à des fins autres que la détection d'éventuelles vulnérabilités dans les systèmes, le Participant reconnaît qu'il sera considéré comme le responsable du Traitement et qu'il portera l'entière responsabilité du Traitement qu'il aura effectué dans ce cadre. Le Participant préserve la SNCB et l'indemnise entièrement contre toute action en justice d'une Personne concernée ou d'un autre tiers, ainsi que contre tout préjudice lié subi par la SNCB en rapport avec toute violation par le Participant (ou tout tiers pour lequel la responsabilité du Participant est engagée) de ses obligations en matière de Traitement des Données à caractère personnel.

4. Récompenses

4.1. La SNCB s'engage à verser une récompense au Participant aux conditions suivantes :

(a) La vulnérabilité n'est pas encore connue au sein de la SNCB ;

(b) La vulnérabilité n'a pas été signalée auparavant par une autre personne que le Participant ; et

(c) Le signalement est conforme à la présente Politique et complet.

4.2. La SNCB se réserve le droit de déterminer, à sa seule discrétion, la forme que prendra cette récompense.

4.3. Toute demande de récompense ne respectant pas ces conditions sera assimilée à une tentative illégale d'extorsion.

5. Procédure

5.1. Détection

Lorsque le Participant découvre une information relative à une vulnérabilité, il procède, dans la mesure où cela est raisonnablement possible, à des vérifications préalables afin de confirmer l'existence de la vulnérabilité et d'identifier les risques éventuels. Après cette première évaluation du risque inhérent à ces vulnérabilités, le Participant contacte la SNCB le plus rapidement possible, conformément à l'article 5.2.

5.2. Signalement

(a) Le Participant envoie toute information relative aux vulnérabilités identifiées à la SNCB à l'adresse e-mail suivante : disclose@belgiantrain.be.

(b) Le Participant suivra les directives suivantes lors de l'envoi des informations :

(i) Le Participant s'exprime en français, en néerlandais ou en anglais dans ses communications.

(ii) Le Participant utilise le formulaire figurant à l'annexe 1 (*Annexe 1 :* Rapport de vulnérabilité) et fournit toutes les informations demandées dont il dispose. Les vulnérabilités identifiées doivent être décrites de manière complète et détaillée, y compris les adresses IP, les logs, les captures d'écran, les URL concernées, etc. Il est important que la SNCB puisse retrouver elle-même la vulnérabilité afin de l'éliminer.

(iii) Le Participant confirme expressément qu'aucune information confidentielle provenant de ou sur la SNCB (obtenue de manière directe ou indirecte, légale ou illégale) n'a été utilisée lors de la détection ou de l'identification de la vulnérabilité.

(iv) Si nécessaire, le Participant fournira les informations de contact pertinentes afin que la SNCB puisse continuer à assurer le suivi du signalement avec lui.

(c) La SNCB s'engage, dès réception d'un signalement, à envoyer au Participant, dans les plus brefs délais, un accusé de réception ainsi que les étapes suivantes de la procédure.

5.3. Communication

(a) Les parties s'engagent à tout mettre en œuvre pour assurer une communication continue et efficace dans le but d'identifier et de résoudre la vulnérabilité identifiée et signalée.

(b) Si, après un délai raisonnable, aucune des parties n'a réagi, les parties peuvent faire appel au Centre pour la Cybersécurité Belgique (CCB) (vulnerabilityreport@cert.be) en tant que coordinateur (par défaut).

5.4. Recherche et objectif

(a) Lors de la phase de recherche, la SNCB reproduira l'environnement et le comportement identifié du Participant afin de vérifier les informations fournies.

(b) La SNCB tiendra le Participant régulièrement informé des résultats de cette recherche et des mesures prises à la suite de ces informations.

(c) Au cours de ce processus, les parties tiendront compte des rapports similaires ou connexes, évalueront le risque et la gravité de la vulnérabilité identifiée et identifieront d'éventuels autres produits ou systèmes affectés.

(d) La présente Politique vise à permettre le développement d'une solution pour résoudre la vulnérabilité du système avant que d'autres dommages (supplémentaires) ne soient causés.

5.5. Annonce publique

(a) La SNCB décide, après avoir entendu le Participant, de la manière dont l'existence de la vulnérabilité éventuelle sera rendue publique.

(b) En aucun cas, une annonce publique n'aura lieu avant qu'une solution ait été mise en œuvre et qu'un avis de sécurité puisse être diffusé auprès des utilisateurs concernés.

(c) Aucune divulgation n'est autorisée sans l'autorisation écrite expresse de la SNCB.

(d) Si une vulnérabilité affecte également d'autres organisations, la SNCB la signalera au CCB (vulnerabilityreport@cert.be).

6. Droit applicable

6.1. La présente Politique sera régie par le droit belge et interprétée conformément à celui-ci. Tous les litiges relatifs à la validité, à l'interprétation, à l'exécution de la présente Politique seront définitivement réglés par les tribunaux bruxellois compétents.

6.2. Le CCB (vulnerabilityreport@cert.be) peut intervenir en tant que médiateur entre la SNCB et le Participant pour des litiges relatifs à l'application de la présente Politique.

7. Durée

7.1. La présente Politique s'applique à partir du 02/04/2026 et restera en vigueur jusqu'à ce que la SNCB annonce une modification conformément à l'article 7.2.

7.2. La SNCB peut modifier ou mettre fin à la présente Politique. La SNCB annoncera toute modification matérielle de la présente Politique par voie de publication sur son site internet. Sauf mention contraire explicite de la part la SNCB, les modifications apportées à la présente Politique entreront en vigueur trente (30) jours après leur publication.

Annexe 1 : Rapport de vulnérabilité

Nom : Prénom :	
(Adresse/Pays) :	
Adresse e-mail : Numéro de téléphone :	
Description de la vulnérabilité :	
Type de vulnérabilité :	
Détails de configuration :	
Système d'exploitation :	
Opérations réalisées (logs) :	
Outils utilisés :	
Dates et heures des tests effectués :	
Adresse IP ou URL du système affecté :	
Si des Données à caractère personnel sont traitées :	• Types de Données à caractère personnel consultées/traitées : • Catégorie de Personnes concernées (client, personnel, fournisseur) : • S'agit-il d'un transfert de données à/d'accès depuis un pays hors Union européenne ou ne faisant pas partie de l'Espace économique européen (EEE) ? Si oui : - mentionnez le(s) pays(s) concerné(s) : - renvoyez l'annexe II complétée et signée.
Toute autre information pertinente :	
Annexes (captures d'écran).	
Signalement fait au CCB.	Si la vulnérabilité a également été signalée au CCB, veuillez mentionner la date du signalement.
En transmettant ces informations, je confirme expressément, en tant que Participant à la Politique de la SNCB relative à la divulgation coordonnée des vulnérabilités, que ma recherche et les informations susmentionnées obtenues dans le cadre de celle-ci ne sont en aucune manière basées, directement ou indirectement, sur des informations confidentielles provenant de ou sur la SNCB, ni ne découlent de celles-ci.	

Annexe 2 : Transfert de Données à caractère personnel en dehors de l'UE et EEE (dispositions contractuelles types)

Lorsque le Participant obtient l'autorisation de la SNCB de transférer des Données à caractère personnel de la SNCB au Participant ou à une entreprise liée au Participant (ou un transfert ultérieur), en tous les cas, lorsqu'un tel transfert serait interdit par le Règlement (EU) 2016/679 sans la protection des Données à caractère personnel transférées offerte par les clauses contractuelles types énoncées dans la Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de Données à caractère personnel vers des pays tiers en vertu du Règlement (UE) 2016/679 du Parlement européen et du Conseil, telles que modifiées ou remplacées de temps à autre par une autorité compétente en vertu de la législation et de la réglementation applicable en matière de protection des données au sein de l'EEE ("clauses contractuelles types de l'EEE"), il est expressément convenu entre la SNCB (« exportateur de données ») et le Participant ou l'une des entreprises liées (chacune en sa qualité "d'importateur de données") que le module 2 applicable des clauses contractuelles types de l'EEE ("clauses contractuelles types de l'EEE pour le transfert entre le Responsable de traitement et le Sous-traitant"), incorporées par le biais d'une référence, s'appliquera dès le début du transfert en question, et tant la SNCB que le Participant confirmeront que :

- la clause 7 (Docking) des clauses contractuelles types s'applique ;
- la clause 9 (Recours à des sous-traitants) s'applique et que le "délai" est d'un (1) moins ;
- à la clause 11(a), le texte facultatif ne s'applique pas ;
- à la clause 13(a) (Contrôle), le texte suivant est sélectionné : " *L'autorité de contrôle qui veille à ce que l'exportateur de données respecte le Règlement (UE) 2016/679 en ce qui concerne le transfert de données, comme indiqué à l'annexe I.C, agit en tant qu'autorité de contrôle compétente"* ;
- "l'option 1" prévue à la clause 17 (Droit applicable) s'applique et que l' "État membre" est la Belgique ;
- à la clause 18 (Forum et choix de la juridiction), l'État membre est la Belgique ;
- l'annexe 1 du module 2 est réputée avoir été préalablement complétée avec les informations pertinentes de l'article 3.3 de la présente Politique, les parties sont l'exportateur de données et l'importateur (ou les importateurs) de données, l'autorité de contrôle est l'*Autorité belge de protection des données* et les Traitements sont réputés être décrits dans la présente Politique ; et
- l'annexe 2 du module 2 est réputée avoir été préalablement remplie avec les informations pertinentes des articles (e) et (f) de la présente Politique.