

General security requirements

1 December 2019

Contents

| | |
|---|----|
| List of abbreviations used | 3 |
| Validation | 4 |
| 1. General security requirements..... | 6 |
| 1.1 Performance obligation on the successful bidder and its staff before and during performance of the contract | 6 |
| 1.2 Staff screening..... | 7 |
| 1.3 Access to SNCB premises or sites | 8 |
| 1.4 SNCB badges/keys | 8 |
| 1.5 Theft prevention | 9 |
| 1.6 Internal emergency number | 9 |
| 1.7 Confidentiality..... | 10 |
| 1.8 Failure to comply and sanctions/remedies concerning this annex..... | 10 |
| 1.9 Contact details: Corporate Security Service | 11 |





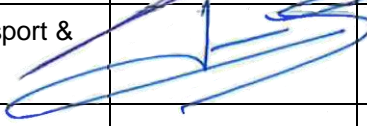
List of abbreviations used

| | |
|-------------|--|
| B-FI | Finance Department |
| B-MS | Marketing & Sales Department |
| B-PT | Passenger Transport & Security Department |
| B-ST | Stations Department |
| CSS | Corporate Security Service (B-PT.3) |
| DPO | Data Protection Officer |
| SOC | Security Operations Center |
| SUM | Service Unit Manager |



Validation

| | | | |
|---|--|------------------|-------------|
| Applicable to | All SNCB specifications/contracts with external parties | | |
| Date of publication and entry into force | 01/12/2019 | | |
| Author | Role and department | Signature | Date |
| M. DE LANGHE | Management unit consultant B-PT.301 | | 30/10/2019 |
| Reviewed by | Role and department | Signature | Date |
| H. BOCKX | Specialist Management B-ST.004 | | 07/11/2019 |
| J. DE MAET | Expert – Coordinator B-PT.301 | | 30/10/2019 |
| A. SENGAKIESE MAKAMZILE | Sourcing Development Center Manager – B-FI.5 | | 14/11/2019 |
| C. VAN USSEL | B-HR.21 HR BP B-TC Coordination | | 18/11/2019 |
| Approved by | Role and department | Signature | Date |
| D. BEATSE | Legal Security Policies Expert B-PT.002 | | 18/11/2019 |
| T. CORYN | Head of Department B-PT.7 | | 19/11/19 |
| S. DEMEDTS | SUM Operational & Service Procurement B-FI.55 | | 20/11/19 |
| T. VERDICKT | Data Protection Officer (DPO) B-SL.21 | | 21/11/2019 |
| G. EEVERS | Senior Legal Counsel B-SL. 231 | | 21/11/2019 |
| M. HAUMONT | Head of Exploitation & Construction – B-ST | | 8/11/2019 |

| | | | |
|-----------------|---|--|-------------------------------------|
| S. JONCKHEERE | Head of Domestic Commercial Operations – B-MS.1 |  | 15/12/19 |
| Y. OUAMA | Head of Department HR BP B-TC |  | 28/2/20 |
| K. BERGS | Deputy Business Director Procurement |  | 03/03/20 |
| H. VANDERKIMPEN | G.M. Passenger Transport & Security |  | 12/03/20 |
| Version | Page | Date | Description of adaptation(s) |
| | | | |
| | | | |



1. General security requirements

In connection with provision of its services, works and/or products at the premises or sites of the contracting authority, the successful bidder declares that it will observe the security requirements set out below.

1.1 Performance obligation on the successful bidder and its staff before and during performance of the contract

Before providing the contract services, the successful bidder must send the contracting authority the following information for the relevant staff:

1. Identity card

A copy of the identity card of each relevant staff member must be sent to the contracting authority.

2. Self-declaration; criminal record disclosure (basic level)¹

The successful bidder declares that none of the following situations apply to it and its staff performing the work:²

1. They are not subject to the grounds for exclusion provided for in Article 67 of the Law on Public Procurement – 17 June 2016.³
2. They are not subject to one of the following grounds for exclusion:
 - a. Being sentenced, even as a suspended sentence or a suspended sentence with probation:
 - To a prison sentence for an offence in the Penal Code;
 - Under the Law of 24 February 1921 on the movement of poisonous, soporific, narcotic, psychotropic, disinfecting or antiseptic substances and its implementing decrees;
 - Under the Law of 8 June 2006 (Weapons Act) regulating commercial and personal activity in relation to weapons, and its implementing decrees;
 - The Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data;
 - The Law of 30 July 1981 criminalising certain racist or xenophobic acts.
 - b. Receiving an alternative penalty for a breach of the Law of 24 February 1921 is not considered to be a cause for exclusion.

¹ The contracting authority may also require the vetting level for regulated activities, i.e. for activities where there is legislation or a regulation setting requirements for access or for those performing the role (e.g. security professions, transport of passengers or goods, tax professions).

² Exception for social projects where (ex-)detainees are reintegrated into employment.

³ Only applicable to representatives of the company itself, not members of its staff.



The successful bidder shall ensure that sufficient evidence is available at all times to substantiate its declaration.

The successful bidder must renew all criminal record checks annually. They confirm that no member of staff involved in performing the contract falls under the above-mentioned grounds for exclusion. If the successful bidder is aware of (criminal) activities falling within the scope of the grounds for exclusion, it must immediately inform the contracting authority of this. Having reviewed the content of this disclosure, the contracting authority may refuse the successful bidder or a member of its staff carrying out the work access to its buildings.

The contracting authority may ask the successful bidder to provide the results of criminal record checks on its employees involved in performing the contract for a maximum of six (6) months in order to be able to review this and check that the declaration was accurate. If the criminal records information is not received in response to a written request from SNCB, action may be taken under the Royal Decree of 14 January 2016⁴.

Having reviewed the content of this disclosure, the contracting authority may refuse the successful bidder or a member of its staff carrying out the work access to its buildings. The contracting authority shall not retain any copies of the criminal record information and shall not save the results in its files.

1.2 Staff screening

The Law of 11 December 1998 and the Royal Decree of 8 May 2018 relating to security classification and security clearances, certificates and advisory opinions shall apply.

⁴ The Royal Decree of 14 January 2013 laying down the general rules of public procurement and public works concessions, as amended by the Royal Decree of 22 June 2017 (Belgian Official Gazette 17 March 2017, entry into force on 30 June 2017).



1.3 Access to SNCB premises or sites

1. The contracting authority shall provide the successful bidder with badges and, if necessary, keys for its staff present on SNCB premises or sites. Badges shall be distributed in compliance with SNCB guidelines.
2. When providing the contract services, the successful bidder and its relevant staff shall only have access to premises and sites within the limits and on the routes indicated by the project leader/contract manager or their representatives.
3. Entry and exit checks are permitted under the Law of 2 October 2017 regulating private and special security.

Subject to justification, the contracting authority shall have the right to refuse access to all or part of the premises/sites.

1.4 SNCB badges/keys

Each member of staff who receives a badge and, if applicable, one or more SNCB keys, must exercise due care when looking after them.

It is strictly forbidden to:

1. Lend SNCB badges or keys to anyone else;
2. Copy keys or badges provided by SNCB;
3. Grant access to someone who does not have a valid badge or key.

SNCB badges must always be worn visibly throughout the time a staff member is present on SNCB premises or sites.

If a member of staff does not have an access badge, they must report to local security/security staff or the project leader/contract manager or their representative, who will give them access subject to approval.

The Corporate Security Service will unilaterally deactivate SNCB badges that have not been used for a period of one (1) year. A deactivated badge cannot be reactivated. The project leader/contract manager can request a new badge via "Badger"⁵.

⁵ Badger is the central system for managing SNCB access badges.



The Corporate Security Service has the right to review access rights that have been granted at any time.

If an SNCB badge is lost/stolen or if it stops working, the project leader/contract manager must deactivate the badge via "Badger". A deactivated badge cannot be reactivated. The project leader/contract manager can request a new badge via "Badger".

The successful bidder shall reimburse the costs incurred by the contracting authority for replacing badges or keys in the event that they are lost/stolen or stop working. This fee is EUR 100 per badge or key⁶. A formal notice may be drawn up for each failure to observe this obligation. The general rules governing the performance of public contracts shall apply here.

1.5 Theft prevention

When a staff member involved in performing the contract is found to be stealing food, drink, data or equipment belonging to SNCB, a member of SNCB staff, a third party, the successful bidder or a passenger, this is considered a breach of contract. The staff member concerned shall immediately be refused access to all SNCB buildings. The contracting authority may report the theft to the relevant police service.

1.6 Internal emergency number

Members of staff who see anything suspicious must inform the SOC.⁷

⁶ The price of badges and keys may change over time.

⁷ See 1.9, "Contact details: Corporate Security Service".



1.7 Confidentiality

Without prejudice to the provisions of this specification, the following clauses shall apply to the contract.

1. The successful bidder's staff may under no circumstances consult, read or copy SNCB information, nor take photos of documents/buildings/sites, etc., unless this is necessary to enable performance of the initial contract.
2. The contracting authority may also require that the successful bidder's staff sign a confidentiality statement, depending on the services or supplies to be delivered or the work to be carried out. This privacy statement shall be provided by the contracting authority to the successful bidder.

1.8 Failure to perform and sanctions/remedies concerning this annex

To be able to check whether current members of the successful bidder's staff are actually on the list of authorised workers, the project leader/contract manager or their representative may carry out spot ID checks to ensure that the successful bidder is acting in accordance with the specification.

Access to the building or site may be denied if there is uncertainty about the identity of the staff carrying out the work. A formal notice may then be sent to the successful bidder and the actions provided for in the Royal Decree of 14 January 2013⁸ may be imposed (sanctions, automatic measures).

The following persons may carry out checks on compliance with these security requirements:

1. Security officers and security guards from the Corporate Security Service or their representatives/private security companies conducting these ID checks.⁹
2. The project leader/contract manager or their representatives, regarding strict compliance with the contract.

⁸ The Royal Decree of 14 January 2013 laying down the general rules for public procurement contracts and concessions for public works, as amended by the Royal Decree of 22 June 2017 (Belgian Official Gazette 17 March 2017, entry into force 30 June 2017).

⁹ In accordance with the Law of 2 October 2017 regulating private and special security.



The purpose of any monitoring is to check:

1. Identity data by security and security officers of the Corporate Security Service/private security companies in places that are not accessible to the public, to check IDs and the list of names;
2. Identity data by the project leader/contract manager or their representatives for places that are not accessible to the public, in order to check IDs and the list of names;
3. That SNCB badges are being worn correctly, both in places that are and are not accessible to the public;
4. That SNCB badges are being presented correctly, both in places that are and are not accessible to the public;
5. Badge movements – as part of access control – with SNCB badges, following an official complaint to the CSS department.

The points listed above are not exhaustive.

1.9 Contact details: Corporate Security Service

Corporate Security Service (CSS) is the department within SNCB that acts as a point of contact for security-related issues. This department is responsible for the coordination and implementation of security activities and patrols (Securail and B-Security) on the railways.

Security Operations Center (SOC)

| Role | Telephone | Departmental email |
|--|--------------------|--|
| National point of contact for any security issues and suspicious activity on the railways. ⇒ Please call the SOC if contracted staff notice or display any suspicious behaviour. | 0800 30 230 | securityoperationscenter@b-rail.be For your information, emails are not treated as urgent. |

