Security Requirements for External personnel

1 Objective

The purpose of this document is to contractually ensure the protection of data belonging to NRB and its customers in the context of the use of external personnel by NRB (including consultants and subcontractors). In this context, it sets out the rules applicable to any External personnel carrying out an assignment for NRB.

2 Definitions

External personnel: any person who is not part of the NRB staff, i.e. any person who is not bound by an employment contract. For example: a consultant, subcontractor's employee, or even the subcontractor of a subcontractor (cascading outsourcing).

NRB: NRB is understood to be NRB S.A., NRB's current and future branches in Belgium and abroad.

Confidential information: Confidential information is any information of a financial, legal, commercial, technical, IT, administrative, personal or other nature, outside the public domain which, by reason of its nature or the circumstances of its disclosure, should be reasonably considered confidential.

3 Scope

The rules set out in these requirements and in NRB Policies referenced in chapter 10 apply to all External personnel who provide services, directly or indirectly, for NRB and who access the buildings, IT infrastructure and data of NRB and/or its customers. If customers have security policies or procedures regarding their infrastructure, these will be applicable in place hereof.

4 General principles

The information and IT resources of NRB and its customers are made available to the External personnel in the exclusive context of his assignment.

The External party undertakes to:

- be aware of all NRB policies and procedures applicable to him in the context of his assignment;
- notify NRB, as soon as possible, of any violation of the obligations imposed by this document of which he becomes aware;
- contact the NRB Service Desk without delay if he notes a breach of data security, a malfunction of security tools (e.g. antivirus) or if he notes an anomaly (virus detection, unusual behaviour, slowness, etc.);
- record the data of NRB and its customers on the appropriate storage locations made available by NRB or its customers. The use of the PC's local hard drive is prohibited since it is not backed up;
- use internet services (websites, email, collaboration, etc.) solely within the strict framework of his assignment, in compliance with the general principles and rules specific to the various services used, as well as in compliance with the legislation in force;- respect NRB's policies, processes and procedures, as well as best practices in information security, confidentiality and governance;
- return all hardware and software used that has been made available by NRB, at the end of the assignment.

5 Confidentiality

General

The External personnel, having access to confidential information of NRB or its customers, undertakes to:

- only use it for the needs for which this information is communicated;
- use this information only when necessary for performance of his services;
- not make any duplication, in any form and on any medium whatsoever, in whole or in part, of the information transmitted, without NRB's prior written authorisation;
- take reasonably necessary measures and precautions, in particular as regards preservation, in order to maintain its confidentiality.

The confidential information remains, in any event, the property of NRB or its customers and this document does not recognize or constitute any right of ownership, whether of licence, brand, model, copyright, or any other intellectual property right on the accessible information.

The External personnel undertakes to apply NRB's "Information Classification Policy".

The External pesonnel guarantees that he will only process personal data in accordance with the instructions transmitted by NRB, within the strict limits necessary for performance of the planned assignment and following the rules defined in the GDPR Appendix to the contract concluded between the External personnel's contracting company and NRB.

Disclosure

The External personnel undertakes to notify NRB, as soon as possible, of any violation of the obligations of confidentiality imposed by these requirements of which he becomes aware.

Exclusion

The confidentiality obligations do not apply to information for which the External personnel can demonstrate that:

- he disclosed it after obtaining prior written authorization from NRB or that it was disclosed by NRB;
- it had entered the public domain prior to its disclosure or entered the public domain after its disclosure provided that this was not the result of a violation of its own confidentiality obligations;
- it was received from a third party without breaching an obligation of confidentiality with respect to NRB.

Term

The confidentiality obligations set out in these requirements take effect on the day the External personnel begins his services.
It is understood that these obligations apply to the External personnel after the end of the services and for an indefinite period.

6 Access to IT infrastructure

Access limited to the assignment

The External personnel will only use:

- the IT resources necessary for him to carry out the assignment entrusted to him;
- the access account(s) assigned to him for the said assignment;
- connection methods supported by NRB, especially with regard to remote access.

Access to data and IT resources of NRB and its customers is performed exclusively using the access account(s) provided to the External personnel. The passwords associated with this/these account(s) must be of high quality, renewed at each request and not be communicated to third parties, in accordance with the "User account and password policy". The External personnel will immediately contact the Service Desk if one of its passwords is disclosed or if he notices an attempt to violate his access.

Limitation of uses

It is strictly forbidden to use NRB's IT resources or the access account(s) assigned to it to commit illegal and/or dangerous actions (hacking, financial pyramids, P2P, etc.).

Preservation of computer system operation

Any connection of any hardware whatsoever belonging to and/or managed by the External personnel may in no case

- disrupt the expected operation of the network and the various computer systems;
- bypass access control measures.

It is forbidden for the External personnel to cause disturbances of any nature whatsoever, by applications, management tools, monitoring, capture or analysis tools, computer viruses or any other logical element.

Preserving the integrity of computer systems

The External personnel will ensure that the workstation he uses has:

- an active anti-virus, with recent signature updates;
- an operating system updated with security patches provided by the manufacturer.

Authorized software

On the NRB workstation used by the External personnel, only software for which NRB has previously acquired a licence for use are authorized.

On hardware belonging to the External personnel, it is its responsibility to ensure that the software used is properly licensed.

In either case, the following are strictly prohibited:

- software whose objectives are hacking (extended concept), spamming, the distribution and exploitation of spyware, sniffing, except for an explicit and formalized exemption;
- software allowing the exchange and sharing of files between workstations (better known as peer-to-peer or P2P);
- non-genuine copies of commercial software for any purpose.

7 Administrator access

Administrators are users who also have privileged access due to their administrator function. These privileged accesses are assigned to a personal and specific administration account.

An External personnel with privileged access undertakes to:

- only use this specific account for strictly professional activities requiring privileged access;
- comply with the "Administrator account and password policy";
- not use a generic privileged account if a personal administration account is recommended (except as authorised in the "Administrator account and password policy");
- not use this account to connect to internal business services or on the internet;
- not use this account in automated processes.

8 Physical access

External personnel benefiting from access to NRB buildings for the accomplishment of their assignment will receive a badge on the first day of this assignment allowing them to activate the parking barriers opening and the entrance lock. This badge will also provide access to the areas necessary for accomplishment of their assignment, excluding any other area or building.

Rules:

- The badge is name-based and cannot be passed on;
- It is strictly forbidden to force passage into an area where the badge does not give access (for example, by climbing or illegally passing speedgates);
- NRB reserves all rights regarding access by an External personnel;
- The badge must be worn in a visible manner at all times;
- In case of loss of their badge, the External personnel must immediately inform their NRB manager or the G4S agent;
- If the External personnel accesses NRB buildings outside of office hours, they must inform the G4S agent of their presence on the site;
- At the end of the assignment, the badge must be returned to the guardhouse or to the person in charge of the External person.

9 Penalties

Failure to comply with these requirements and/or applicable NRB Policies constitutes serious misconduct on the part of the External personnel. Depending on the seriousness of the facts, the company responsible for the External personnel or the External person may be the subject of criminal and/or civil proceedings.
In addition, in the event of damage resulting from non-compliance herewith, the company responsible for the External personnel or the External person is liable to reimburse all the costs, without limits, necessary to restore the initial situation (i.e. before the infringement), increased by additional damages to which NRB would be exposed with respect to its customers, for service disruptions or damage caused.
In the event of non-compliance with these requirements and/or the applicable NRB Policies, NRB reserves the right to block access, temporarily or permanently without having to make payment of any compensation whatsoever.

10 List of NRB Policies applicable to External personnel

1) Information Classification Policy
   https://intranet.nrb.be/document/Process%20Map/QRM Pol%20Classification%20de%20l%27information EN.pdfhttps://intranet.nrb.be/document/Process Map/QRM_Pol Classification de l'information_FR.pdf

2) User Account and Password Policy
   https://intranet.nrb.be/document/Process%20Map/QRM Pol%20mdp%20user EN.pdf

3) Administrator Account and Password Policy
   https://intranet.nrb.be/document/Process%20Map/QRM Pol%20mdp%20admin EN.pdf

4) Clean Desk & Clean Screen Policy
   https://intranet.nrb.be/document/Process%20Map/QRM Pol%20Clean%20Desk%20and%20Clean%20Screen EN.pdf