Politique de sécurité et d'accès aux infrastructures informatiques de NRB

Security and access policy for NRB's IT infrastructure

Read the English version below

1 CHAMP D'APPLICATION

Les infrastructures informatiques et/ou données soumises aux présentes dispositions sont celles de NRB et/ou de son client. Si ce dernier dispose de procédures de sécurité, celles-ci seront applicables en lieu et place des présentes en ce qui concerne les infrastructures du client.

Par NRB, on entend NRB s.a. ses filiales, ses succursales et Trasys International.

2 EXPOSITION DES FAITS

Le consultant/sous-traitant chargé de la réalisation d'une mission ou d'une tâche peut se connecter aux infrastructures informatiques précitées, à un poste de travail qui lui appartient et qu'il gère exclusivement ou non pour les besoins de la mission.

Des normes d'accès ont été établies afin de réduire les risques existants au niveau de la sécurité informatique et de protéger l'infrastructure informatique, celles-ci sont contraignantes pour tous les consultants/sous-traitants.

Le contrat reprendra, le cas échéant, outre le nom du consultant/sous-traitant, la description de la mission et des besoins pour la réaliser, les accès aux serveurs qui s'avèrent nécessaires, les protocoles à utiliser, les besoins spécifiques, etc.

3 OBLIGATIONS

3.1 Accès limités à la mission

Le consultant/sous-traitant utilisera uniquement :

- les ressources qui lui sont nécessaires pour mener à bien la mission qui lui a été confiée ;
- le(s) compte(s) d'accès qui lui a/ont été attribué(s) pour ladite mission ;
- l'adresse IP qui lui a été attribuée sans jamais modifier la configuration réseau du poste de travail.

3.2 Préservation du fonctionnement des systèmes informatiques

Toute connexion de matériel quel qu'il soit appartenant et/ou géré par le consultant/sous-traitant ne peut en aucun cas perturber le fonctionnement attendu du réseau et des différents systèmes informatiques.

Il est interdit au consultant/sous-traitant d'introduire sur le réseau informatique des perturbations de quelque nature que ce soit, par des applications, des outils de gestions, des outils de surveillance, de capture ou d'analyse, des virus informatiques ou tout autre élément logique.

3.3 Préservation de l'intégrité des systèmes informatiques

Le consultant/sous-traitant s'assurera que le poste de travail qu'il souhaite connecter au réseau informatique dispose :

- d'un anti-virus et d'un antispyware actifs, avec mise à jour récente des signatures et dont l'écart entre la date de connexion et la date de mise à jour de l'anti-virus et de l'antispyware est en permanence inférieure à 24 heures ;
- d'un système d'exploitation mis à jour au niveau des correctifs des « vulnérabilités systèmes » fournis par le constructeur.

3.4 Connexion au réseau

Toute connexion réseau filaire ou Wifi (modem, routeur ADSL, modem câble, …) vers l'extérieur (Internet ou autre) est interdite.

3.5 Logiciels autorisés

Seule la présence de logiciels dont le consultant/sous-traitant a préalablement acquis une licence d'utilisation est autorisée sur les postes de travail connectés au réseau informatique.

Sont strictement interdits :

- les logiciels dont les objectifs sont le hacking (notion étendue), le spamming, la diffusion et l'exploitation de spyware, le sniffing, sauf dérogation explicite et formalisée de la Cellule Sécurité de NRB ;
- les logiciels permettant l'échange et le partage de fichiers entre postes de travail (mieux connus sous le nom de peer-to-peer ou P2P);
- les copies non authentiques de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par les dispositions relatives aux droits de propriété intellectuelle.

3.6 Limitation des utilisations

Il est formellement interdit d'utiliser le poste de travail pour commettre des actions illégales et/ou dangereuses (hacking, pyramides financières, P2P …).

3.7 Propriété protégée

Toutes les informations susmentionnées et leurs dérivées restent la propriété de NRB ou de son client. Rien dans cette convention ne sera interprété comme étant un transfert de droit de licence ou transfert de l'octroi ou tout autre transfert de droits de propriété intellectuelle ou industrielle.

4 SANCTION

En cas de non-respect des présentes règles, NRB et/ou son Client se réserve(nt) le droit de refuser l'accès ou de limiter totalement ou partiellement ceux-ci à leurs infrastructures, et ce, de manière définitive ou temporaire sans devoir assurer le paiement de quelque indemnité que ce soit.

Le non-respect des dites règles constituent une faute grave dans le chef du consultant/sous-traitant.

Outre le fait que le contrat pourrait être résilié sans délai ni indemnité, en cas de dommages résultant du non-respect des présentes règles, le consultant/sous-traitant s'expose à rembourser l'ensemble des frais, sans limites, nécessaires au rétablissement de la situation initiale (c'est-à-dire d'avant mission), majorée de dommages et intérêts supplémentaires auxquels NRB seraient redevables vis-à-vis de ses Clients, pour les ruptures de services ou les dommages occasionnées à leurs infrastructures informatiques.

USAGE RULES OF THE IT-INFRASTRUCTURE

1. SCOPE OF APPLICATION

The IT infrastructures and/or data subject to these provisions are those of NRB and/or its client. If the latter has security procedures in place, they will be applicable instead of these in respect of the client's infrastructure.

NRB means NRB s.a. its subsidiaries, branches and Trasys International.

2. BACKGROUND

The consultant/subcontractor responsible for carrying out a mission or task may connect to the aforementioned IT infrastructures, to a workstation belonging to him/her and which he/she manages exclusively or not for the needs of the mission.

Access standards have been established to reduce existing IT security risks and protect the IT infrastructure, which are binding on all consultants/subcontractors.

The contract will include, where applicable, in addition to the name of the consultant/subcontractor, a description of the mission and the needs to carry it out, access to the servers that are necessary, the protocols to be used, the specific needs, etc.

3. OBLIGATIONS

3.1. Access restricted to the mission

The consultant/subcontractor will only use:

- the resources required to carry out the mission it was given;
- the access account(s) assigned to him/her for the said mission;
- the IP address assigned to it without ever changing the network configuration of the workstation.

3.2. Preservation of the functioning of IT-systems

Any connection of any equipment whatsoever owned and/or managed by the consultant/subcontractor may not under any circumstances disrupt the expected operation of the network and the various computer systems.

The consultant/subcontractor is prohibited from introducing disruptions of any kind into the computer network, through applications, management tools, monitoring, capture or analysis tools, computer viruses or any other logical element.

3.3. Preservation of the integrity of the IT-systems

The consultant/subcontractor will ensure that the workstation he wishes to connect to the computer network has:

- an active anti-virus and antispyware, with recent signature updates and whose difference between the connection date and the update date of the anti-virus and antispyware is permanently less than 24 hours;
- an operating system updated with fixes to "system vulnerabilities" provided by the manufacturer.

3.4. Network connection

Any wired or Wifi network connection (modem, ADSL router, cable modem,...) to the outside (Internet or other) is prohibited.

3.5. Authorized software

Only the presence of software for which the consultant/subcontractor has previously acquired a user license is authorized on workstations connected to the computer network.

The following are strictly prohibited:

- software whose objectives are hacking (extended notion), spamming, dissemination and exploitation of spyware, sniffing, unless explicitly and formally exempted by the NRB Security Unit;
- software allowing the exchange and sharing of files between workstations (better known as peer-to-peer or P2P);
- inauthentic copies of commercial software for any purpose whatsoever, except for a backup copy under the conditions provided for by the provisions relating to intellectual property rights.

3.6. Limitation of uses

It is strictly forbidden to use the workstation to commit illegal and/or dangerous actions (hacking, financial pyramids, P2P ...).

3.7. Protected property

All the above-mentioned information and its derivatives remain the property of NRB or its client. Nothing in this Agreement shall be construed as a transfer of licensing rights or transfer of the grant or any other transfer of intellectual or industrial property rights.

4. SANCTIONS

In the event of non-compliance with these rules, NRB and/or its Client reserves the right to refuse access or to limit totally or partially access to their infrastructures, either permanently or temporarily, without having to ensure payment of any compensation whatsoever.

Failure to comply with these rules constitutes serious misconduct on the part of the consultant/subcontractor.

In addition to the fact that the contract could be terminated without delay or compensation, in the event of damage resulting from non-compliance with these rules, the consultant/subcontractor is liable to reimburse all costs, without limit, necessary to restore the initial situation (i.e. before the mission), plus additional damages to which NRB would be liable to its clients, for disruptions of services or damage to their IT infrastructure.