Exigences de sécurité pour les Externes

1 Objectif

Ce document est établi afin de garantir contractuellement la protection des données de NRB et de ses clients dans le cadre de l'utilisation de personnel externe par NRB (notamment des consultants, des sous-traitants). Dans ce cadre, il énonce les règles applicables à toute personne externe effectuant une mission pour NRB.

2 Définitions

Externe : toute personne qui ne fait pas partie des membres du personnel de NRB, càd toute personne qui n'est pas liée par un contrat de travail. Exemple : consultant, employé de sous-traitant, ou même sous-traitant du sous-traitant (externalisation en cascade).

NRB : NRB s'entend comme étant NRB S.A., les succursales actuelles et futures de NRB en Belgique et à l'étranger.

Informations confidentielles : Sont considérées comme confidentielles toutes les informations de nature financière, juridique, commerciale, technique, informatique, administrative, personnelle ou autre hors du domaine public qui, en raison de leur nature ou des circonstances de leur divulgation, devraient être raisonnablement considérées comme confidentielles.

3 Champ d'application

Les règles énoncées dans les présentes exigences et dans les Politiques de NRB référencées au chapitre 10 s'appliquent à tous les Externes qui réalisent des prestations, directement ou indirectement, pour NRB et qui accèdent aux bâtiments, aux infrastructures informatiques et aux données de NRB et/ou de ses clients. Si des clients disposent de politiques ou procédures de sécurité concernant leur infrastructure, celles-ci seront applicables en lieu et place des présentes.

4 Principes généraux

Les informations et les ressources IT de NRB et de ses clients sont mises à disposition de l'Externe dans le cadre exclusif de sa mission.

L'Externe s'engage à :

- prendre connaissance de toutes les Politiques et procédures de NRB qui lui sont applicables dans le cadre de sa mission ;
- notifier à NRB, dans les plus brefs délais, toute violation des obligations imposées par le présent document dont il aurait connaissance ;
- contacter sans tarder le « Service Desk » de NRB s'il constate une brèche de la sécurité des données, un dysfonctionnement des outils de sécurité (e.g. anti-virus) ou s'il constate une anomalie (détection de virus, comportement bizarre, lenteur,…) ;
- enregistrer les données de NRB et de ses clients sur les emplacements de stockage adéquats mis à disposition par NRB ou ses clients. L'utilisation du disque dur local du PC est interdite car il ne fait pas l'objet de sauvegardes ;
- faire usage des services Internet (web, e-mail, collaboration,…) uniquement dans le cadre strict de sa mission, dans le respect de principes généraux et des règles propres aux divers services utilisé, ainsi que dans le respect de la législation en vigueur ;

- respecter les politiques, processus et procédures de NRB, ainsi que les bonnes pratiques en matière de sécurité de l'information, de confidentialité et de gouvernance ;
- remettre en fin de mission tout le matériel et les logiciels utilisés qui ont été mis à disposition par NRB.

5 Confidentialité

Généralités

L'Externe ayant accès à une information confidentielle de NRB ou de ses clients s'engage :

- à l'utiliser uniquement pour les besoins pour lesquels cette information est communiquée ;
- à utiliser cette information uniquement lorsque cela est nécessaire pour l'exécution de ses prestations ;
- à ne procéder à aucune duplication, sous quelque forme et quelque support que ce soit, de tout ou partie de l'information transmise sans l'autorisation écrite et préalable de NRB ;
- à prendre les mesures et précautions raisonnablement nécessaires, notamment en matière de conservation, afin de maintenir sa confidentialité.

L'information confidentielle reste, en tout état de cause, la propriété de NRB ou de ses clients et le présent document ne reconnaît et ne constitue aucun droit de propriété, que ce soit de licence, marque, modèle, copyright, droit d'auteur ou tout autre droit de propriété intellectuelle sur les informations accessibles.

L'Externe s'engage à appliquer la « Politique de classification de l'information » de NRB.

L'Externe garantit qu'il ne traitera des données à caractère personnel que conformément aux instructions transmises par NRB, dans la stricte mesure nécessaire à la réalisation de la mission prévue et en suivant les règles définies dans l'Annexe GDPR au contrat conclu entre la société contractante de l'Externe et NRB.

Divulgation

L'Externe s'engage à notifier à NRB, dans les plus brefs délais, toute violation des obligations de confidentialité imposées par les présentes exigences dont il aurait connaissance.

Exclusion

Les obligations de confidentialité ne s'appliquent pas aux informations pour lesquelles l'Externe peut démontrer :

- qu'il les a divulguées après obtention préalable de l'autorisation écrite de NRB ou que la divulgation a été réalisée par cette dernière ;
- qu'elles étaient entrées dans le domaine public préalablement à leur divulgation ou entrées dans le domaine public après leur divulgation pour autant que ce ne soit pas le résultat d'une violation de ses propres obligations de confidentialité ;
- qu'elles ont été reçues d'un tiers sans violation d'une obligation de confidentialité à l'égard de NRB.

Durée

Les obligations de confidentialité énoncées dans les présentes exigences prennent effet le jour où l'Externe commence ses prestations.
Il est entendu que les présentes obligations s'imposent à l'Externe après la fin des prestations et pour une durée indéterminée.

6 Accès aux infrastructures IT

Accès limités à la mission
L'Externe utilisera uniquement :

- les ressources IT 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 ;
- les méthodes de connexion supportées par NRB, notamment en ce qui concerne l'accès à distance.

L'accès aux données et ressources IT de NRB et de ses clients s'effectue en utilisant exclusivement le(s) compte(s) d'accès qui ont été fournis à l'Externe. Les mots de passe associés à ce(s) compte(s) doivent être de qualité, renouvelés à chaque demande et ne pas être communiqués à des tiers, conformément à la « Politique de compte et mot de passe utilisateur ». L'Externe contactera sans tarder le « Service Desk » si un de ses mots de passe est divulgué ou s'il constate une tentative de violation de ses accès.

Limitation des utilisations
Il est formellement interdit d'utiliser les ressources IT de NRB ou le(s) compte(s) d'accès qui lui a/ont été attribué(s) pour commettre des actions illégales et/ou dangereuses (hacking, pyramides financières, P2P…).

Préservation du fonctionnement des systèmes informatiques
Toute connexion de matériel quel qu'il soit appartenant et/ou géré par l'Externe ne peut en aucun cas

- perturber le fonctionnement attendu du réseau et des différents systèmes informatiques ;
- contourner les mesures de contrôles d'accès.

Il est interdit à l'Externe de provoquer des perturbations de quelque nature que ce soit, par des applications, des outils de gestion, des outils de surveillance, de capture ou d'analyse, des virus informatiques ou tout autre élément logique.

Préservation de l'intégrité des systèmes informatiques
L'Externe s'assurera que le poste de travail qu'il utilise dispose :

- d'un anti-virus actif, avec mise à jour récente des signatures ;
- d'un système d'exploitation mis à jour au niveau des correctifs de sécurité fournis par le constructeur.

Logiciels autorisés
Sur le poste de travail de NRB utilisé par l'Externe, seuls les logiciels dont NRB a préalablement acquis une licence d'utilisation sont autorisés.

Sur le matériel propre de l'Externe, il est de la responsabilité de celui-ci de s'assurer que les logiciels utilisés soient en ordre de licence.

Dans les 2 cas, 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 ;
- 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 quel que usage que ce soit.

7 Accès administrateurs

Les administrateurs sont des utilisateurs qui disposent en outre, de par leur fonction d'administrateur, d'accès privilégiés. Ces accès privilégiés sont attribués à un compte d'administration personnel et spécifique.

L'Externe disposant d'accès privilégiés s'engage à :

- n'utiliser ce compte spécifique que pour des activités strictement professionnelles et nécessitant des accès privilégiés;
- se conformer à la « Politique de compte et mot de passe administrateur » ;
- ne pas utiliser de compte privilégié générique (sauf exception autorisée dans la « Politique de compte et mot de passe administrateur ») ;
- ne pas utiliser ce compte pour se connecter à des services bureautique interne ou sur internet ;
- ne pas utiliser ce compte dans des processus automatisés.

8 Accès physique

Les Externes bénéficiant de l'accès aux bâtiments de NRB pour l'accomplissement de leur mission recevront le premier jour de celle-ci un badge leur permettant d'activer l'ouverture des barrières de parking et du sas d'entrée. Ce badge leur permet également d'accéder aux zones nécessaires pour l'accomplissement de leurs missions, à l'exclusion de toute autre zone ou bâtiment.

Règles :

- Le badge est nominatif et ne peut pas se transmettre ;
- Il est formellement interdit de forcer le passage d'une zone à laquelle le badge ne donne pas accès (par exemple par l'escalade ou le passage clandestin des speedgates) ;
- NRB se réserve tous droits en matière d'accès à un Externe ;
- Le badge doit être porté de manière visible à tout moment ;
- En cas de perte de son badge, l'Externe informera directement son responsable NRB ou l'agent G4S ;
- Si l'Externe accède aux bâtiments de NRB en dehors des heures de bureau, il informera l'agent G4S de sa présence sur le site ;
- A la fin de la mission, le badge doit être remis au poste de garde ou au responsable en charge de l'Externe.

9 Sanctions

Le non-respect des présentes exigences et/ou aux Politiques de NRB applicables constituent une faute grave dans le chef de l'Externe. Selon la gravité des faits, la société responsable de l'Externe ou l'Externe pourra faire l'objet de poursuites pénales et/ou civiles.
En outre, en cas de dommages résultant du non-respect de ces politiques, la société responsable de l'Externe ou l'Externe s'expose à rembourser l'ensemble des frais, sans limites, nécessaires au rétablissement de la situation initiale (c'est-à-dire d'avant infraction), majorée de dommages et intérêts supplémentaires auxquels NRB serait exposée vis-à-vis de ses clients, pour les perturbations/ruptures de services ou les dommages occasionnés.
En cas de non-respect des présentes exigences et/ou aux Politiques de NRB applicables, NRB se réserve le droit de bloquer l'accès, et ce, de manière temporaire ou définitive sans devoir assurer le paiement de quelque indemnité que ce soit.

10 Liste des Politiques NRB applicables aux Externes

1) Politique de classification de l'information
https://intranet.nrb.be/document/Process%20Map/QRM_Pol%20Classification%20de%20l%27information_FR.pdf

2) Politique de compte et mot de passe utilisateur
https://intranet.nrb.be/document/Process%20Map/QRM_Pol%20mdp%20user_FR.pdf

3) Politique de compte et mot de passe administrateur
https://intranet.nrb.be/document/Process%20Map/QRM_Pol%20mdp%20admin_FR.pdf

4) Politique Clean desk & Clean screen
https://intranet.nrb.be/document/Process%20Map/QRM_Pol%20Clean%20Desk%20and%20Clean%20Screen_FR.pdf