Conditions d'utilisation des Services en ligne NRB

1 Objectif

Ce document est établi afin de définir les conditions d'utilisation des services en ligne fournis par NRB à ses Clients.

Les présentes conditions régissent l'utilisation des Services en ligne NRB par le Client ainsi que les obligations du Client et de NRB en ce qui concerne le traitement et la sécurité des Données Client et des Données à Caractère Personnel.
Les conditions générales d'achat du Client concernant des services en ligne sont explicitement exclues pour l'utilisation des Services en ligne NRB, sauf accord préalable écrit donné par NRB.

2 Définitions

Client : désigne toute entité ayant passé un contrat avec NRB pour l'exécution des Services en ligne NRB.

Données Client : désigne toutes les données, notamment les fichiers de texte, son, vidéo ou image et les logiciels fournis à NRB par le Client ou en son nom dans le cadre de l'utilisation des Services en ligne NRB.

Données à Caractère Personnel : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »). Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

DPO : Data Protection Officer.

Incident de sécurité : violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non-autorisée de Données Client ou de Données à Caractère Personnel, ou l'accès non autorisé à celles-ci, de manière accidentelle ou illicite.

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

Services en ligne NRB : tout service en ligne mis à disposition par NRB à ses Clients dans le cadre d'un contrat.

Utilisateur : désigne toute personne physique ou morale relevant du Client ayant accès aux Services en ligne NRB. Dans le cadre de certains services, un ordinateur, ou un matériel robotisé accédant au service peut également être considéré comme un « Utilisateur ».

3 Champ d'application

Les conditions énoncées s'appliquent à tous les Services en ligne NRB. Il s'agit notamment de (liste non limitative) :

- Le service NECS 4 dont les différents applicatifs sont accessible via le portail NECS.
- Le service SIEM/SOC basé sur l'application Splunk.

4 Conformité aux lois et règlementations

NRB s'engage à se conformer à toutes les lois et réglementations applicables à la fourniture des Services en ligne NRB, y compris à la législation relative à la notification des violations de sécurité et aux obligations de protection des Données à Caractère Personnel. Cependant, NRB n'est pas responsable du respect de toute loi ou réglementation applicable au Client ou au secteur d'activité du Client qui ne serait pas généralement applicable aux prestataires de services informatiques. NRB ne détermine pas si les Données Client incluent des informations soumises à une loi ou réglementation spécifique. Tous les Incidents de sécurité sont soumis aux dispositions ci-dessous relatives aux Notifications d'Incidents de sécurité (NIS).

Le Client est tenu de se conformer à toutes les lois et réglementations applicables à son utilisation des Services en ligne NRB, y compris aux lois concernant la confidentialité des communications, au RGPD, ainsi qu'aux obligations de protection des Données à Caractère Personnel du RGPD. Il incombe au Client de déterminer si les Services en ligne NRB sont appropriés au stockage et au traitement d'informations soumises à toute loi ou réglementation spécifique et d'utiliser les Services en ligne NRB d'une manière compatible avec les obligations légales et réglementaires du Client.

Il incombe au Client de répondre à toute demande formulée par un tiers concernant l'utilisation d'un Service en ligne NRB par le Client, telle qu'une demande d'accès aux contenus formulée par une autorité judiciaire belge.

5 Utilisation des Services en ligne NRB

Le Client est autorisé à utiliser les Services en ligne NRB conformément à son contrat et aux présentes conditions d'utilisation. NRB se réserve le droit d'apporter des modifications commercialement raisonnables à chaque Service en ligne NRB.

5.1 Responsabilités du Client

Utilisation des Services en ligne NRB
Le Client est responsable de ses opérations et de l'utilisation qu'il fait, ou que ses utilisateurs font, des Services en ligne NRB. Le Client doit s'assurer que cette utilisation des Services en ligne NRB soit faite en conformité avec le contrat et avec les présentes Conditions d'utilisation. Il est responsable de s'assurer que l'objet, le périmètre et les caractéristiques des Services en ligne NRB, rencontrent les prérequis et besoins qu'il a exprimés dans son cahier des charges/RFP.

Utilisateurs
Le Client est chargé d'identifier et d'authentifier ses Utilisateurs, d'approuver l'accès par ces Utilisateurs aux Services en ligne NRB, de contrôler les accès non autorisés et de préserver la confidentialité des noms d'utilisateur, mots de passe et informations de compte. NRB n'est pas responsable des dommages causés par le Client et les Utilisateurs, y compris les personnes qui n'ont pas été autorisées à avoir accès aux Services en ligne NRB. Le Client est seul responsable de l'utilisation faite des Services en ligne NRB par ses Utilisateurs ou toute personnes utilisant ses comptes d'utilisateurs.
Dans le cas où les Utilisateurs sont techniquement gérés par NRB, le Client est tenu de notifier à NRB, dès qu'il en a connaissance, de tout changement concernant ses Utilisateurs (départ, mobilité ou autre).

Obligations de sécurité
Le Client est seul responsable pour déterminer de façon indépendante si les mesures techniques et organisationnelles d'un Service en Ligne NRB répondent aux exigences du Client, y compris ses obligations en matière de sécurité en vertu des obligations de protection des Données à Caractère Personnel applicables. Le Client reconnaît et accepte que (compte-tenu de l'état actuel des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement de ses Données à Caractère Personnel ainsi que des risques pour les personnes) les pratiques et stratégies de sécurité mises en œuvre et maintenues par NRB garantissent un niveau de sécurité adapté au risque en ce qui concerne ses Données à Caractère Personnel. Le Client est entièrement responsable de la mise en œuvre et du maintien de mesures de sécurité et de protection des Données à Caractère Personnel pour les composants que le Client fournit ou contrôle (comme une machine virtuelle ou une application qu'il utilise sur la plateforme NECS).

5.2 Règles de bon usage

Ni le Client, ni quiconque accédant à un Service en ligne NRB par l'intermédiaire du Client n'est autorisé à utiliser un Service en ligne NRB :

- en violation des lois, ordonnances ou règlements, ou en violation de droits d'autrui ;
- pour tenter d'accéder de façon non autorisée à des services, des appareils, des données, des comptes ou des réseaux ou d'en perturber l'accès ;
- pour envoyer des courriers indésirables ou distribuer des programmes malveillants ;
- d'une façon qui peut porter atteinte au Service en ligne NRB ou en perturber l'utilisation par un autre utilisateur ;

- dans toute application ou situation où la défaillance du Service en ligne NRB pourrait entraîner la mort ou de graves blessures corporelles de toute personne, ou de graves dommages physiques ou environnementaux ; ou
- pour aider ou encourager toute personne à effectuer une des actions qui précèdent.

La violation de ces règles de bon usage peut entraîner la suspension du Service en ligne NRB. NRB avertira le Client avant toute suspension d'un Service en ligne NRB pour les raisons mentionnées ci-dessus, excepté si NRB estime qu'une suspension immédiate est nécessaire.

5.3 Restrictions techniques

Le Client doit respecter et ne pas contourner les restrictions techniques applicables à un Service en ligne NRB qui lui permettent de ne l'utiliser que d'une certaine façon.

5.4 Disponibilité

La disponibilité de chaque Service en ligne NRB et de ses fonctionnalités ne sont pas garanties, sauf si un(des) niveau(x) de disponibilité ont été expressément stipulé(s) dans le contrat en vigueur entre NRB et le Client.

6 Protection des données et sécurité

NRB s'engage à prendre toutes les mesures raisonnables pour fournir un niveau adéquat de sécurité dans le cadre de la fourniture des Services en ligne NRB. A ce titre, NRB développe et maintient un système de gestion de la sécurité de l'information (SMSI) documenté et basé sur la norme ISO27001:2013.

L'Annexe 'Mesures standards techniques et organisationnelles de sécurité' décrit de manière plus précise les mesures techniques et organisationnelles de sécurité applicables aux Services en ligne de NRB. Cette annexe est disponible sur le portail regroupant la documentation à destination du Client.

Le Client s'engage à prévenir NRB, dans les meilleurs délais, d'un Incident de sécurité affectant les Services en ligne NRB ou les données du Client hébergées par NRB.

7 Notification des Incidents de sécurité

Si NRB a connaissance d'un Incident de sécurité pendant le traitement par NRB de Données Client ou de Données à Caractère Personnel, NRB devra rapidement et dans les meilleurs délais :
(1) aviser le Client de l'Incident de sécurité ;
(2) enquêter sur l'Incident de sécurité et fournir au Client des informations concernant ce dernier ; et
(3) prendre des mesures raisonnables pour atténuer les effets et minimiser les conséquences préjudiciables de l'Incident de sécurité.

Les notifications relatives aux Incidents de sécurité seront transmises à un ou plusieurs administrateurs du Client, par tout moyen choisi par NRB, y compris par courrier électronique. Les notifications relatives aux Incidents de sécurité liés aux Données à Caractère Personnel seront également transmises au DPO du Client, par tout moyen choisi par NRB, y compris par courrier électronique.

Il incombe au Client et à lui seul de veiller à ce que les mises à jour des coordonnées de ses administrateurs et du DPO soient communiquées à NRB. Il incombe au Client et à lui seul de respecter ses obligations en vertu des lois sur la notification des incidents applicables au Client et de s'acquitter de toute obligation de notification à un tiers liée à tout Incident de sécurité.

NRB devra consentir des efforts raisonnables pour aider le Client à s'acquitter de son obligation d'informer les autorités compétentes et les personnes concernées de cet Incident de sécurité, en vertu de l'Article 33 du RGPD ou d'une autre loi ou réglementation applicable.

La réponse de NRB à un Incident de sécurité ou la notification de NRB à ce sujet en vertu du présent article ne constitue pas une reconnaissance par NRB de quelque faute ou responsabilité que ce soit en ce qui concerne l'Incident de sécurité.

Le Client doit avertir rapidement NRB en cas de mauvaise utilisation potentielle de ses comptes ou informations d'identification, ou de tout Incident de sécurité lié à un Service en ligne NRB.

8 Conditions spécifiques pour certains Services en ligne NRB

8.1 Service NECS 4

Définitions :

- **CMP :** Cloud Management Platform. Ce logiciel est la brique centrale du cloud. Il se compose de deux parties : l'une est l'interface web qui présente le catalogue de services et l'autre est le moteur de workflow qui séquence les actions automatiques et les valide étape par étape. C'est lui qui interface et pilote les divers composants d'infrastructure pour fournir le service que vous avez commandé.
- **Tenant :** Désigne la bulle dans laquelle vos systèmes et données sont stockés. Ainsi chaque Client possède sa propre bulle, son propre Tenant complètement isolé des autres Clients.

Gestion des licences et usage ou contenu non autorisé

Si le Client installe ou utilise sur l'infrastructure fournie par NRB des applications/logiciels, le Client doit respecter les dispositions de la Politique de gestion de licences de Software (Software Licensing Management Services), disponible à l'adresse www.nrb.be, qui sont incorporées au contrat.

Utilisation de composants non-supportés

Si le Client installe ou utilise sur l'infrastructure fournie par NRB des composants non-supportés par des fournisseurs tiers (exemple un OS dont le support n'est plus assuré par le fournisseur), le Client en assume l'entière responsabilité et dédouane NRB de toutes ses obligations en matière de respect des SLA, de qualité ou de sécurité.

Accès aux données personnelles

Au sein du CMP, dans un même Tenant, tous les utilisateurs ont accès aux données personnelles suivantes des autres utilisateurs du Tenant : nom, prénom, e-mail et numéro de téléphone professionnel. Il est de la responsabilité du Client propriétaire du Tenant de s'assurer que cette disposition est conforme avec sa politique vie privée et celle de ses fournisseurs.

Configuration de systèmes Dual-Homed

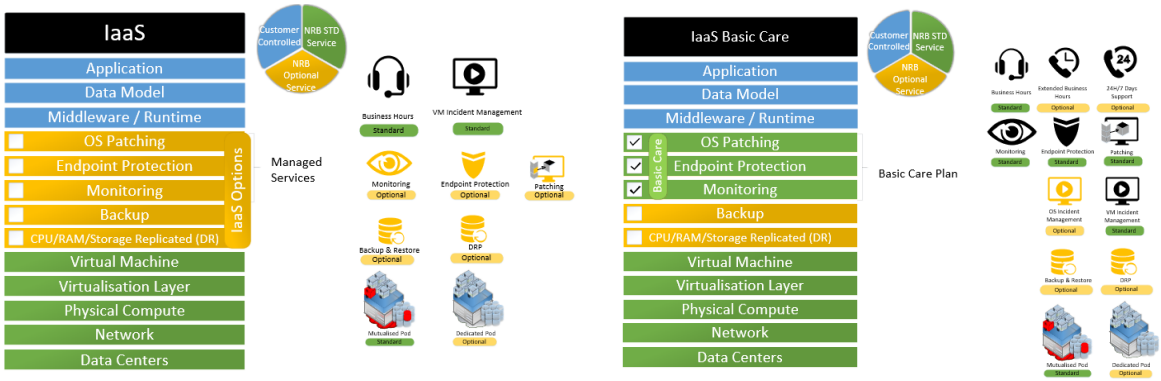
Au sein de son Tenant, le Client a la possibilité de configurer des systèmes Dual-Homed, c'est-à-dire ayant plusieurs cartes réseau connectées sur des segments réseau différents. Ce type de configuration peut potentiellement permettre du trafic réseau entre segments réseau ayant des niveaux de sécurité différents sans passer par le firewall du Tenant. En cas d'utilisation de ce type de configuration par le Client, celui-ci en assume l'entière responsabilité et dédouane NRB de toutes ses obligations en matière de respect des SLA, de qualité ou de sécurité.

Gestion de systèmes sur un Cloud public

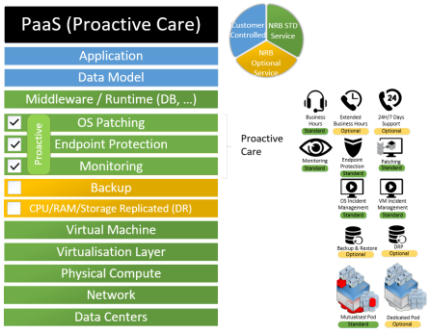
Via l'utilisation du CMP, le Client a la possibilité de créer et gérer des ressources sur un Cloud public différent du Cloud NRB (Microsoft Azure et Amazon Web Services). Pour ces ressources hébergées sur un Cloud public, ce sont les contrats, les conditions d'utilisation et les SLA spécifiques du Cloud public correspondant qui s'appliquent, et non les contrats, les conditions d'utilisation et les SLA de NRB. Il est donc du ressort du Client de s'assurer que l'utilisation du Cloud public via le CMP est conforme aux lois et règlementations en vigueur applicables au Client.

Partage de responsabilités entre le Client et NRB

Les rôles et responsabilités de chacun sont dépendants du niveau de service commandé par le client et résumés dans les schémas suivants :



Dans le cas où NRB est en charge de l'OS Patching, Endpoint protection et/ou Monitoring, tout impact sur les couches 'Customer Controlled' ne sont pas pris en charge gratuitement par NRB.



De plus, le Client est totalement responsable de la gestion des éléments suivants :

- La gestion des utilisateurs dans le Cloud Management Portal.
- La gestion des périodes de Patching dans la tuile 'Tenant Master Data & Networks'.
- La gestion de tous les containers sur un cluster Red Hat OpenShift créé par le Client.
- La gestion des Load Balancers (F5 BIG-IP VE) & Centralized Management (BIG-IQ) créé par le Client.
- La gestion des Security Policies des VLANs du tenant via la tuile 'Firewall Rules & Configuration' si le Client désire un accès en lecture/écriture.