NRB Online Services Terms & Conditions of Use

1 Purpose

This document has been drawn up to define the terms and conditions of use of the online services provided by NRB to its Clients.

These terms and conditions govern the use of NRB Online Services by the Client and the obligations of the Client and NRB concerning the processing and security of Client Data and Personal Data.
The Client's general terms and conditions of purchase for online services are explicitly excluded from the use of NRB Online Services unless NRB gives prior written consent.

2 Definitions

Client: means any entity that has entered into a contract with NRB for the performance of NRB Online Services.

Client Data: means all data, including but not limited to text, sound, video or image files and software provided to NRB by or on behalf of the Client in connection with the use of NRB Online Services.

Personal Data: any information relating to an identified or identifiable natural person (hereafter referred to as "data subject"). "Identifiable natural person" means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, identification number, location data, online identifier, or to one or more elements specific to their physical, physiological, genetic, psychic, economic, cultural or social identity.

DPO: Data Protection Officer.

Security Incident: a breach of security resulting in accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to Client Data or Personal Data.

NRB: NRB means NRB s.a., the present and future branches of NRB in Belgium and abroad.

NRB Online Services: Any online service made available by NRB to its Clients under a contract.

User: means any natural or legal person under the control of the Client who has access to NRB Online Services. A computer or robotic equipment accessing the service may also be considered a "User" for some services.

3 Scope of application

The stated terms and conditions apply to all NRB Online Services. These include (non-exhaustive list):

- The NECS 4 service, of which the various applications are accessible via the NECS portal
- The SIEM/SOC Service based on Splunk

4 Compliance with laws and regulations

NRB commits to comply with all laws and regulations applicable to the provision of NRB Online Services, including legislation relating to the notification of security breaches and Personal Data protection obligations. However, NRB is not responsible for compliance with any laws or regulations applicable to the Client or the Client's industry that would not generally apply to digital service providers. NRB does not determine whether the Client Data includes information subject to a specific law or regulation. All Security Incidents are subject to the Security Incident Notification (NIS) provisions below.

The Client must comply with all laws and regulations applicable to its use of NRB Online Services, including laws concerning the confidentiality of communications, the GDPR, and the Personal Data protection obligations of the GDPR. It is the Client's responsibility to determine whether NRB Online Services are appropriate for the storage and processing of information subject to any specific laws or regulations and to use NRB Online Services in a manner consistent with the Client's legal and regulatory obligations.

It is the Client's responsibility to respond to any request by a third party concerning the Client's use of an NRB Online Service, such as a request for access to the Content made by a Belgian judicial authority.

5 Use of NRB Online Services

The Client is authorised to use NRB Online Services according to its contract and these terms of use. NRB reserves the right to make commercially reasonable changes to each NRB Online Service.

5.1 Client Responsibilities

Use of NRB Online Services
The Client is responsible for its operations and the use it makes, or its users make, of NRB Online Services. The Client must ensure that this use of NRB Online Services is made according to the contract and within these Terms of Use. The Client is responsible for ensuring that the purpose, scope and characteristics of NRB Online Services meet the prerequisites and needs expressed in their specifications/RFP.

Users
The Client is responsible for identifying and authenticating its Users, approving access by such users to NRB Online Services, controlling unauthorised access and maintaining the confidentiality of user names, passwords and account information. NRB is not responsible for damages caused by the Client

and Users, including persons who have not been authorised to access NRB Online Services. The Client is solely responsible for the use of NRB Online Services by its Users or any person using its user accounts.
In the event that NRB technically manages the Users, the Client is obliged to notify NRB as soon as it becomes aware of any changes concerning its Users (departure, mobility or other).

Security obligations
The Client is solely responsible for independently determining whether the technical and organisational measures of an NRB Online Service meet the Client's requirements, including its security obligations under the applicable Personal Data protection obligations. The Client acknowledges and agrees that (taking into account the current state of knowledge, implementation costs and the nature, scope, context and purposes of the processing of their Personal Data as well as the risks for individuals), the security practices and policies implemented and maintained by NRB ensure a level of security appropriate to the risk concerning its Personal Data. The Client is entirely responsible for implementing and maintaining security and Personal Data protection measures for the components that the Client provides or controls (such as a virtual machine or application that it uses on the NECS platform).

5.2 Rules of good use

Neither the Client nor anyone accessing an NRB Online Service through the Client is authorised to use an NRB Online Service:

- in violation of laws, ordinances or regulations, or violation of the rights of others;
- to attempt to gain unauthorised access to or disrupt access to services, devices, data, accounts or networks;
- to send spam or distribute malicious software (malware);
- in a manner that may impair NRB Online Services or disrupt the use of it by another user;
- in any use or situation where the failure of NRB Online Services could result in death or serious bodily injury to any person, serious physical or environmental damage, or
- to assist or encourage anyone to perform any of the above actions.

Violating these rules of good use may result in the suspension of NRB Online Services. NRB will notify the Client before any suspension of an NRB Online Service for the reasons mentioned above unless NRB considers an immediate suspension necessary.

5.3 Technical restrictions

The Client must respect and not circumvent the technical restrictions applicable to an NRB Online Service that only allow it to be used in a certain way.

5.4 Availability

The availability of each NRB Online Service and its functionalities are not guaranteed unless one or more levels of availability have been expressly stipulated in the current contract between NRB and the Client.

6 Data protection and security

NRB commits to take all reasonable steps to provide an adequate level of security regarding the provision of NRB Online Services. As such, NRB develops and maintains a documented Information Security Management System (ISMS) based on the ISO27001:2013 standard.

The Annex "Standard Technical and Organisational Security measures" describes the technical and organisational security measures applicable to NRB Online Services in more detail. This annex is available on the Client Documentation Portal, which comprises documentation intended for the Client.

The Client commits to notify NRB as soon as possible of a security incident affecting NRB Online Services or the Client's data hosted by NRB.

7 Notification of security incidents

If NRB becomes aware of a security incident during NRB's processing of Client Data or Personal Data, NRB shall act promptly and as quickly as reasonably possible to:
(1) notify the Client of the security incident;
(2) investigate the security incident and provide the Client with information about the security incident; and
(3) take reasonable measures to mitigate the effects and minimise the adverse consequences of the security incident.

Notifications concerning security incidents will be forwarded to one or more of the Client's administrators by any means chosen by NRB, including by email. Notifications relating to security incidents concerning Personal Data will also be transmitted to the Client's DPO by any means chosen by NRB, including by email.

It is the Client's sole responsibility to ensure that updates to the contact details of its administrators and the DPO are communicated to NRB. The Client is solely responsible for compliance with its obligations under the Client's incident notification laws and any third-party notification obligations related to any security incident.

NRB shall make reasonable efforts to assist the Client in fulfilling its obligation to inform the competent authorities and the persons concerned of this security incident under Article 33 of the GDPR or any other applicable law or regulation.

NRB's response to, or notification of, a security incident under this Article shall not constitute an acknowledgement by NRB of any fault or liability concerning the security incident.

The Client must promptly notify NRB of any potential misuse of its accounts or credentials or any security incident related to an NRB Online Service.

8 Specific Terms & Conditions applicable to selected NRB Online Services

8.1 NECS 4 Service

Definitions:

- **CMP:** Cloud Management Platform. This software is the cloud's core building block. It consists of two parts: one is the web interface that presents the service catalogue, and the other is the workflow engine that sequences automatic actions and validates them step by step. It interfaces and drives the various infrastructure components to provide the service that you ordered.
- **Tenant:** refers to the container in which your systems and data are stored. Each Client has its own container, its own Tenant, completely isolated from other Clients.

License management and unauthorised use or Content

If the Client installs or uses applications/software on the infrastructure provided by NRB, the Client must comply with the provisions of the Software Licensing Management Services policy, available at www.nrb.be, which are incorporated into the contract.

Use of unsupported components

If the Client installs or uses components not supported by third-party providers on the infrastructure provided by NRB (for example, an OS that the provider no longer supports), the Client assumes full responsibility and releases NRB from all its obligations regarding compliance with SLAs, quality or security.

Access to Personal Data

Within the CMP, within the same Tenant, all users have access to the following Personal Data of other Tenant users: Last Name, First Name, Email and Business Phone Number. It is the responsibility of the Client owner of the Tenant to ensure that this provision complies with its privacy policy and that of its suppliers.

Configuration of Dual-Homed systems

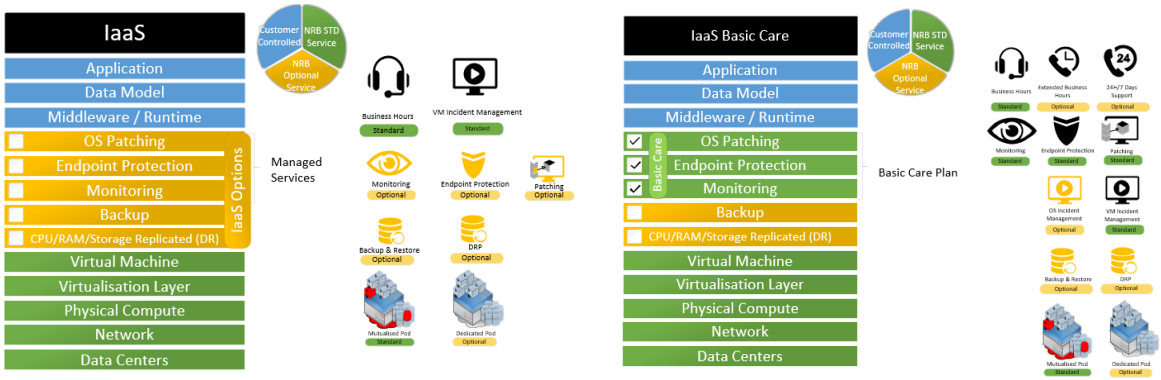
The Client can configure Dual-Homed systems within their Tenant, meaning having several network cards connected to different network segments. This type of configuration can potentially allow network traffic between network segments with different security levels without passing through the Tenant firewall. If the Client uses this type of configuration, the Client assumes full responsibility for this situation and clears NRB of all its obligations in terms of compliance with SLAs, quality or security.

System management on a public cloud

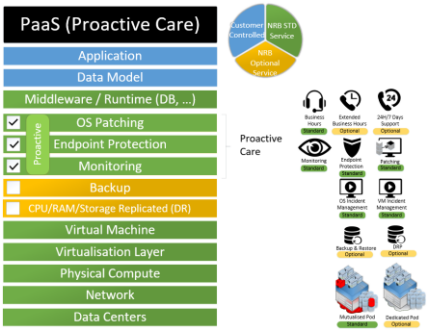
Using the CMP, the Customer can create and manage resources on a public Cloud other than the NRB Cloud (Microsoft Azure and Amazon Web Services). For these resources hosted on a public Cloud, the contracts, conditions of use and SLAs specific to the corresponding public Cloud apply, and not NRB's contracts, conditions of use and SLAs. It is therefore the Customer's responsibility to ensure that use of the Public Cloud via the CMP complies with the laws and regulations applicable to the Customer.

Shared responsibilities between the Customer and NRB

The roles and responsibilities of each party depend on the level of service ordered by the customer, and are summarized in the following diagrams:



If NRB is in charge of OS Patching, Endpoint protection and/or Monitoring, any impact on the 'Customer Controlled' layers is not supported free of charge by NRB.



In addition, the customer is fully responsible for managing the following elements:

- User management in the Cloud Management Portal.
- Management of Patching periods in the 'Tenant Master Data & Networks' tile.
- Management of all containers on a Red Hat OpenShift cluster created by the Customer.
- Management of Load Balancers (F5 BIG-IP VE) & Centralized Management (BIG-IQ) created by the customer.
- Management of security policies for tenant VLANs via the 'Firewall Rules & Configuration' tile, if the customer requires read/write access.