

Roima SaaS Technical Service Description

1 Introduction

This document is an appendix to the SaaS Agreement between Roima and the Customer and applies specifically to Roima-hosted SaaS services.

2 Definitions

The terms used in this document are listed below. If any definition here differs from those found in the Agreement, the precedence outlined in the Agreement will apply.

Term	Definition
Continuous Delivery	Continuous Delivery is a software release practice in which updates to the SaaS are prepared, tested, and made ready for deployment on a frequent and predictable basis.
CSP	CSP is an abbreviation for cloud service provider.
Roima Application	Roima Application refers to a set of specific Software provided by the Supplier that the Customer is able to access and operate or otherwise utilize according to this Agreement (See Software in the main agreement definitions).
SaaS	SaaS (Software as a service) refers to a service provided by Roima via a data network, where the software and the related license, support service and data are delivered centrally from a managed service to the Customer
Service Package	As defined in Roima SaaS Support and Maintenance Service Description.
Service Request	Formal request from a user for something to be provided, such as access to a service, change of configuration, or information
Software	Roima's proprietary standard software and related documents, including modifications to Roima's standard software and new versions provided to the Customer by Roima.

3 General

This document describes the content of the Roima SaaS technical services provided with Roima Applications by the Supplier.

The Roima SaaS technical services consists of the following components:

- Software user management
- Service uptime
- Technical platform for SaaS
- Support for the technical platform

- Backup service
- Monitoring service
- Data security

The scope of the Roima SaaS technical services is determined by the Agreement between the Supplier and the Customer.

Scope of Deployment Model

This technical service description applies to Roima-hosted SaaS services unless otherwise explicitly agreed. Where the Service is deployed in a customer-controlled cloud environment or on customer infrastructure, infrastructure responsibility and operational boundaries are defined in a separate, customer-specific appendix.

4 Content and limitations of the SaaS

4.1 Application availability

The availability and uptime targets of the SaaS are defined in the separate Service Level Description appendix. This section describes technical prerequisites and limitations relevant to availability but does not define service level commitments.

The SaaS is generally available to the Customer within the agreed time period up to a maximum of 24/7 every day of the year, excluding planned and announced maintenance outages and possible disruptions and problems. The service uptime of the SaaS is in accordance with the separate service level description.

The Customer shall report any unplanned disruptions in the SaaS to the support channel indicated by the Supplier to the Customer.

The Customer's access to the SaaS may be restricted or prevented by the Supplier prior to written warning to the Supplier if the usability or security of the SaaS strictly requires it or the Customer's use endangers the operation of the SaaS. The access can be restricted for example because of security incident containment, abusive traffic or legal requirement. Such restrictions are applied only to the extent necessary and, where practicable, are limited to the affected customer environment.

4.2 Service interruptions

The operating systems and other components associated with the SaaS, excluding the Roima Application software, will be kept up to date with updates. For these updates, a regular service window is reserved. The service windows are presented in Roima Application specific documentation.

The Supplier reserves the right to make urgent critical updates to the technical platform without prior notice outside of the outages described above.

Updates of the Roima Applications are planned and scheduled separately together with the Customer or according to possible Continuous Delivery schedule of the Roima Application.

4.3 Service testing

The SaaS includes a test environment and test applications with which the Customer performs the Customer-specific testing.

The test environment is described more closely in Roima Application documents.

The agreed service level promises for the SaaS do not apply to the test environment.

4.4 Support for the technical platform

The maintenance and support service of the technical platform covers the resolution of problems related to the availability of the SaaS.

Support is available for the Customer's key users as follows:

- Through the service channel provided by the Supplier to the Customer

4.5 Backup service

There is a backup service for the production data of the Roima Application included in the service fee. The details of the backup service are described in a Roima Application related document.

The backup service is not responsible for the statutory archiving of the Customer's statutory or similar material added to the SaaS.

Recovery of backups required for the functionality of the SaaS will be performed as a measure included in the SaaS without separate compensation, if the need for the recovery arises from the Supplier's actions.

If the Customer's material stored in the SaaS is destroyed, lost, changed, or damaged in part or in full as a result of the Customer's action, the Supplier has the right to charge the Customer for the recovery of the data.

4.6 Monitoring service

The Supplier monitors the operation and applications of the cloud platform used to provide the SaaS with automated monitoring tools. The scope of the monitoring is on application availability.

4.7 Data security

The SaaS is operated in accordance with the Supplier's current data security policies and continuity plans.

The Supplier monitors the security of the components and software used in the SaaS and is responsible for the security of the SaaS by regularly updating and configuring the environment. The platform is aligned to CIS benchmarks / controls as applicable ([cisecurity.org](https://www.cisecurity.org)) to ensure security and reliability.

4.7.1 Reporting of Security Incidents

The Customer must report any detected or suspected information security incidents to Roima without delay. Reporting of information security incidents should be conducted via email to the address: security@roimaint.com, which creates a trackable ticket in Roima's service management system.

Roima will inform the designated contacts of the Customer about any significant security incidents that have been detected without undue delay.

4.7.2 Use of Encryption in the SaaS

All data traffic entering and leaving the SaaS is encrypted with industry-standard encryption algorithms.

The details of the encryption in the SaaS are described in a Roima Application related document.

4.7.3 Service Log Data

The SaaS records log data related to the use of the SaaS at various levels. The SaaS offers the Customer the ability to audit various changes in the system; this log data is retained in the database of the Roima Application.

The details of the logging in the SaaS are described in a Roima Application related document.

4.7.4 Data Derived from the SaaS

Data derived from the SaaS is provided only to be utilized by the Customer who owns the data in the system, except for utilizing some aggregated or anonymous operational metrics for reliability and capacity planning. However, for the explicit purpose of developing and improving the SaaS, data may be used in the development and training of artificial intelligence systems (including large language models) or artificial intelligence functionalities, as long as such data is anonymized and aggregated so that neither the Customer nor any individual person can be identified.

5 Service level

The service level of the SaaS is described in the separate appendix: “Roima Cloud Service Level Description”.

6 Responsibilities

The responsibilities of the Supplier and the Customer is described in detail in the tables of section 6.

Definition of responsibilities set out in the tables of this section (RACI):

Table 1 RACI matrix responsibility explanations

Ref	Role	Responsibility	Description
R	Responsible	The performer of the task	- Assigned to achieve the task, - Responsible to (A)
A	Accountable	Has the ultimate ownership of the task	- Is the authority who approves the work before it is effective - Does not supervise individual subtasks
C	Consulted	Provides consultancy and resources if needed in the actual work	- With whom there is mandatory two-way communication unless otherwise agreed
I	Informed	Informed about the task	- Kept up to date on progress of the task - One-way communication

Table 2 RACI matrix Pricing column explanations

Pricing	Description
T&M or Service Package	Time and Material or according to optional Service Package ordered by the Customer.
Included in the SaaS fees	No actual based invoicing for standard activity.

6.1 Application Operation Services

This section defines the scope of the Application Operation defined as follows:

- Service restoration
- Application Service Request management
- Daily scheduled operation activities
- Event, availability and capacity management
- Document management

Table 3 Responsibilities – RACI matrix of Application Operation services

Application Operation service	Supplier	Customer	Pricing
Activity			
Service restoration			
Initiate infrastructure application operations incident ticket	A,R		Included in the SaaS fees
Analyze Application Operation incident	A,R	I	Included in the SaaS fees
Coordinate incident / problem resolution with 3 rd parties (networks, devices, systems and infrastructure where Customer has responsibility)	C	A,R	T&M or Service Package
When applicable initiate a change request / ticket for service restoration activities.	A,R		Included in the SaaS fees
Approve and restore service / Supplier caused incident	Supplier: A,R CSP: R	I	Included in the SaaS fees
Approve and restore service / Customer or third party caused incident	A,R	I (C)	T&M or Service Package
Application Service Request management			
Initiate Service Request	A,R		Included in the SaaS fees
Respond to Application Operation related information requests / Initiated by the Customer	A,R	I	Included in the SaaS fees
Respond to Application Operation related information requests / Initiated by the Supplier	A,R		Included in the SaaS fees

Application Operation service	Supplier	Customer	Pricing
Activity			
Scheduled operation activities			
Perform logical DB administration	A,R		Included in the SaaS fees
Perform Application specific configurations in production environment	A,R		Included in the SaaS fees
Perform regular operations to maintain the Roima Application	A,R		Included in the SaaS fees
Deploys application fixes to production (*) See separate Appendix Roima SaaS Support and Maintenance Service Description, Table 8 for the pricing principle.	A,R	I	(*)
Define application and application data backup requirements	A,R		Included in the SaaS fees
Application specific support during application and application data restore	A, R	I	Included in the SaaS fees
Event, availability and capacity management			
Implement application specific monitoring tools	A,R		Included in the SaaS fees
Develop and maintain application monitoring procedures	A,R	I	Included in the SaaS fees
Monitoring of application capacity dependencies and reporting of capacity needs	A,R		Included in the SaaS fees
Propose changes to capacity according to reports and analysis.	A,R	I	Included in the SaaS fees
Approve/Reject proposed changes to capacity.	A,R	I	Included in the SaaS fees
Document Management			

Application Operation service	Supplier	Customer	Pricing
Activity			
Application document updates required due to changes in operations	A,R	I	Included in the SaaS fees

6.2 Database operation and support

Database operation and support is the set of services necessary to install, configure, operate and maintain, monitor and support the databases, as well as the services required to return operations to normal levels of service following an incident.

Table 4 Responsibilities – RACI matrix of 4.2 Database operation and support

Activity	Supplier	Customer	Pricing
Maintain the database software and apply database software maintenance fixes and patches;	A,R		Included in the SaaS fees
Execute recovery procedures, as required, for database subsystem resources;	A,R		Included in the SaaS fees
Provide database subsystem status, as requested;	A,R		Included in the SaaS fees

6.3 Environment and installation

Environment and installation chapter addresses the responsibilities related to customer network, workstations, software installation and security.

Table 5 Responsibilities – RACI matrix of Environment and installation

Activity	Supplier	Customer	Pricing
Customer's terminals, their software and updates, and data security such as firewall and antivirus software	C	R,A	T&M or Service Package
Network environment security inside Customer's infrastructure	C	R,A	T&M or Service Package
The security of the internal network environment of the SaaS inside the access point of the SaaS	R,A		Included in the SaaS fees
Acquiring data connection from terminals of the Customer to the SaaS access point	C	R,A	T&M or Service Package
Service interfaces to the Customer's other systems: The opposite ends and the data connection from the SaaS access point of the service to them	C	R,A	T&M or Service Package

Activity	Supplier	Customer	Pricing
Printers and other hardware and software related to the use of the SaaS inside Customer's infrastructure.	C	R,A	T&M or Service Package
Providing optional Roima Application module specific launcher software to Customer	R,A	C	T&M or Service Package
Optional Roima Application module specific launcher software installation on Customer's terminals	C	R,A	T&M or Service Package
Providing possible database client and database driver for optional database connection to the Customer	R,A	C	T&M or Service Package
Optional database client and database driver installation on the Customer's terminals	C	R,A	T&M or Service Package
Correctness of the Customer's material entered into the SaaS		R,A	N/A
Statutory or other long-term storage of Customer's material entered into the SaaS		R,A	N/A
Responsibility for the actions performed with their user IDs	R,A	R	Included in the SaaS fees
Physical security of the data center	Supplier: I, CSP: R,A	I	Included in the SaaS fees
Data center devices and their maintenance	Supplier: I, CSP: R,A	I	Included in the SaaS fees
Material encryption at rest	Supplier: I, CSP: R,A	I	Included in the SaaS fees
Infrastructure as a service platform services such as virtual machine platform, identity service, virtual networks and backup service used by the Supplier to deliver the SaaS	Supplier: I, CSP: R,A	I	Included in the SaaS fees
Two phase authentication when the SaaS is used through internet with Customer's identity service	C	R,A	T&M or Service Package

7 Termination of SaaS

Upon termination of the SaaS, the Supplier and the Customer shall separately agree on the possible transfer of the Customer's material. In accordance with the hourly rate of the agreement, the Supplier will charge the Customer for the transfer of the material from the SaaS to the location indicated by the Customer. If the transfer also incurs other costs for the Supplier, they will also be charged to the Customer.

The Customer's materials will be permanently deleted within 31 days of the termination of the SaaS. A longer period needs to be agreed separately. Deletion occurs by destroying resources containing the Customer's materials, such as the database. However, this does not apply to backups included in the SaaS, from which the Customer's materials will be removed in accordance with the respective retention period for each backup. Backups will be permanently deleted after the last retention period has expired as described in 4.5.