Rotronic Monitoring System
-
Technical paper
-
SaaS - IT Compliance

Index

1. Scope

This document is designed to clarify all IT questions concerning the Rotronic SaaS solution. Based upon the details from this document, the IT manager should be able to define if RMS is compliant to the internal IT requirements.

There are three parties involved when purchasing a SaaS solution from Rotronic AG:

1) Rotronic AG: RMS Supplier.
2) 4Net AG: Virtual Server Hosting.
3) Interxion: Data Center.

The document is only relevant for the standard SaaS solution. If a customer requires an exclusive cloud solution, then must contact Rotronic AG.

2. Outline

This document covers all IT views of the SaaS solution that Rotronic offers from the services, the security, data integrity, external partners as well as relevant information around how the service is secured so that no data is lost.

The document is setup in a question answer format.

3. ISO Certifications & Compliance:

Rotronic AG:

- ISO 9001
- ISO 17025

4Net AG:

- ISO 9001
- ISO 27001

Interxion:

- ISO 27001
- ISO 22301
- SOC1
- SOC2
- FINMA RS18/3
- PCI DSS

4. Cloud Service Information

4.1. What is the name of the cloud service provider and what is the name of the cloud service?

Cloud service provider: Rotronic AG.

Cloud service: Rotronic Monitoring System.

5. Data Centre

5.1. Which tier level does the data centre support?

Rotronic works with an Interxion tier 4 data centre: https://www.interxion.com/ch/unsere-standorte/zurich-campus.

5.2. Where are the data centres located?

Primary data centre: Zurich, Switzerland

Backup (Storage): Saint Gallen, Switzerland, no failover location.

With the standard SaaS solution, the backup is only done in the primary data centre. When using the Exclusive SaaS solution, the client has the possibility to choose if the backup is only done in the primary data centre or if the backup should be carried out in the secondary data centre.

5.3. How far apart are the relevant data centres?

Over 80km apart.

5.4. Can the data centre location be changed without any further approval by the customer?

Yes, if Rotronic deems necessary to change, then the change will occur and all customers will be duly informed.

5.5. Please provide a description of the security at the physical location:

- The data centre is monitored 24x7 by CCTV and security patrols,
- There are multiple access barriers, including mantraps, contactless key cards and biometric readers.

5.6. Is a two-factor authentication for access to the data centre required?

Yes.

6. Availability

6.1. What is the software availability?

The RMS software is available to the customer without interruption 24 hours a day, 365 days a year. An uptime of 99.9% per calendar year is guaranteed.

Excepted from the uptime is announced maintenance work. Service interruptions during announced scheduled maintenance periods are excluded from the calculation of the uptime.

Availability is defined as follows:

- The resources of the data centre are available.
- The RMS software is accessible from the internet.

6.2. When does service and maintenance work take place?

Scheduled maintenance is needed to service and maintain the hardware and software and to back up data. Customers will be advised of this at least seven weekdays in advance.

IMPORTANT: The recipient of this information is the user declared in the SLA.

Maintenance periods required:

- Major maintenance period: up to 4 times per year, up to 8 hours
- Minor maintenance period: up to 4 times per year, up to 4 hours
- RMS maintenance: up to 4 times per year, up to 2 hours

The maintenance period defines a time period in which service interruptions may take place. The service interruptions in these maintenance periods typically last between a few seconds and 2 hours.

In very urgent cases, (should the security or stability of the systems be at risk) Rotronic AG will implement maintenance periods at short notice.

The maintenance periods are kept as short as possible. The aforementioned maintenance periods and service interruptions are subject to any and every exception. Rotronic AG may change the definition of the maintenance periods and service interruptions in the interests of service quality and security at any time.

6.3. Are your systems regularly patched at the operating system for security weaknesses?

Yes, the datacentre infrastructure and RMS infrastructure are regularly patched.

6.4. What is the response time in case of an error?

The response time is the maximum time between the occurrence of an error and the point in time at which Rotronic AG deals with the error. The response time only applies during the service time.

Rotronic AG shall endeavour to keep the response time as short as possible, but it is not possible in all cases to keep to the response time. A transgression of the response time does not justify a financial penalty or claim for compensation.

6.5. When are new versions of the RMS software released?

Rotronic installs software upgrades during scheduled maintenance periods. New functions can be seen online on the login page or via https://www.rotronic.com/rms.

Rotronic Public SaaS customers are informed 7 days prior to the update, that the update will occur. The change logs for the software will also be delivered.

IMPORTANT: RMS Exclusive SaaS customers are informed of new releases. Software updates are, however, only implemented on the customer’s written request.

6.6. Is the system monitored by Rotronic?

The following parameters are monitored continuously:

- CPU and memory usage of the server
- Availability of the RMS web service and web page
- Availability of the database
- Performance of the e-mail alarm function

6.7. When are backups carried out?

- A backup of the database is created every 2 hours.
- Backups are stored in various time intervals up to a maximum of 2 months.

7. Security

7.1. Which of the following technical measures for the host protection are used?

- Host Firewall.
- Regular integrity checks.
- Host-based intrusion detection.

7.2. Does the host firewall run with only the minimum ports necessary to support the services within the virtual instance?

Yes (only http and https). Only the ports needed for operation of RMS are open (80 and 443).

7.3. What security is setup

- TLS 1.2 for encrypted browser connection.
- HTTP2 for the http protocol version 2.
- Activated HSTS for the specific key agreement protocols that gives assurances the session keys will not be compromised even if the private key of the server is compromised.
- A-Rating (www.ssllabs.com) security setting rating
- A-Rating for HTTP-Headers (https://observatory.mozilla.org) security rating

8. What generall hardening techniques are used to secure the hosts?

- Hardened operation systems.
- Deactivation of unnecessary services.

9. Are certified hypervisors used (common criteria at least EAL 4)?

No, EAL 4 is only valid till VMware vSphere 5. The affected infrastructure in use is running on vSphere 6.0 with the latest patch.

10. Network security

10.1. What security measures are in place against malware?

- Virus detection.
- Trojan detection.
- Spam detection.

10.2. What security measures are in place against net-based attacks?

- IPS / IDS systems.
- Firewall.
- Application Layer Gateway.

10.3. Are the management network and data network isolated from each other?

- Yes.

10.4. Which methods are used to secure communication channels for remote administration?

- SSL.
- VPN.

10.5. Is the communication between the data centre and the cloud user encrypted?

- Yes.

10.6. Is the communication between the cloud computing sites and third party service providers encrypted?

- Yes.

10.7. How is the protection against DDoS attacks done?

- IPS.

10.8. Are there Web Application Firewalls (WAF) in-place to monitor the traffic and allow only secured connections?

- No

11. Data security

11.1. How is the secure insulation of customer data carried out?

Tagging.

11.2. Is a state of the art encryption PKI infrastructure used?

Yes.

11.3. Is it possible to use solely the customers PKI to encrypt customer data?

No.

11.4. Is stored customer data encrypted?

Yes.

11.5. Is backup data encrypted?

No.

11.6. Is customer data completely and reliably removed on customer's request?

Yes.

11.7. Which algorithm is used for deletion?

As of today, no data wiping after deletion.

11.8. How can you restrict access to your service for non Rotronic devices?

- IP ranges.
- Isolated partitions.

12. ID and Rights Management within the Rotronic Monitoring Software

The Rotronic Monitoring System is a GAMP©5[1] category 4 software[2] combined with category 1 hardware[3], helping users monitor their GxP[4] compliant applications, looking into the critical quality attributes and monitoring critical process parameters, helping focus on patient safety, product quality and data integrity and compliant to EudraLex Annex 11[5] and FDA 21 CFR Part 11[6].

12.1. Which authentication protocols are supported?

When logging into the Rotronic Public SaaS the user has to add:

- Company Name.
- User Name.
- Password.

The password security can be defined within the Rotronic System Settings:

- Do not reuse passwords.
- Change password after x days.
- Minimum password length.
- Password strength:
  - Upper and lower case letters.
  - Number and special character.

The passwords are stored hashed within the database.

12.2. Are role-based access controls used?

Yes.

[1] GAMP©5 guidelines for a risk-based approach to compliant GxP computerised systems.
[2] Category 4 software: Configurable software package.
[3] Category 1 hardware: Standard hardware components.
[4] GxP guidelines are designed to ensure that products are safe, meet their intended use and in regulated industries such as drugs, foods, medical devices and cosmetics, adhere to quality processes during manufacturing, control, storage and distribution.
[5] EudraLex is the collection of rules and regulations governing medicinal products in Europe. Annex 11 is part of the European GMP guidelines and defines the terms of reference for computerised systems used by organisations in the pharmaceutical industry. Amongst other things, Annex 11 defines the criteria under which electronic records and electronic signatures are considered to be managed.
[6] FDA is the Food and Drug Administration that is responsible for protecting the public health by ensuring the safety, efficacy and security of human and veterinary drugs, biological products and medical devices; and by ensuring the safety of the USA's food supply, cosmetics and products that emit radiation. The CFR 21 part 11 established the RDA regulations on electronic records and electronic signatures (ERES).

12.3. Does Rotronic do a regular review of roles and rights of their employees?

Yes.

12.4. Are administration controls provided to the customer and can these be used to assign read and write privileges to other users?

Yes.

12.5. Can the system enforce various password policies (minimum number of characters, upper- and lowercase, numbers and regular change of x days)?

Yes.

12.6. Can the system provide a report of granted access rights to the system users?

Yes.

12.7. Can the system allow to connect the identity management with the cloud service?

No, the Public SaaS solution won't allow users to use their active directory.

However, active directory is possible with an exclusive SaaS solution.

13. Monitoring, Logging and Security Incident Management

13.1. Does the system maintain a verifiably accurate Network Time Protocol (NTP) time source?

Yes, the system used with default configuration from Windows and synchronises the time with time.windows.com.

13.2. Is a 2-factor authentication for the management of the cloud service used?

Yes.

13.3. Is a comprehensive 24/7 monitoring of cloud services regarding security and availability Issues, as well as prompt reaction to attacks and security incidents setup?

Yes.

13.4. Are reports on security incidents or information on security incidents that could affect the customers available?

Yes.

13.5. Are administrators activities logged and monitored?

Yes.

13.6. Is this log file Information provided to the customer for access of these administrators to customer data?

No.

14. Emergency management

14.1. Is an IT service continuity plan setup for all provided services?

Yes.

14.2. How often is the IT service continuity plan tested?

Annually.

15. SLA, Portability and Interoperability

15.1. Is there an exit agreement with guaranteed formats while retaining all logical relations?

Yes.

15.2. Are there documented procedures and standard interfaces for exporting data from the cloud?

No, exporting data from the cloud is done with the RMS software.

With the exclusive SaaS solution more options are possible.

15.3. Are interoperable export formats for all data stored within the cloud provided?

Yes, in PDF format via the RMS software.

15.4. Can customers perform their own data extraction without involvement of the provider?

Yes, via the RMS software.

15.5. What guarantees on maximum available resources within a minimum period are offered?

See the Rotronic SaaS SLA contract.

15.6. What guarantees on the availability of supplementary resources within a minimum period are offered?

See the Rotronic SaaS SLA contract.

15.7. Is the operation or provision of data ensured in the event of insolvency of the cloud service provider, in accordance with confidentiality undertakings and data protection requirements?

See the Rotronic SaaS SLA contract: exit scenario.

16. Security Certification and Audit

16.1. By which certification is the provided service covered for all relevant data centres?

ISO27001.

16.2. Which reports are provided to customers on a regular basis?

None.

A monitoring of the cloud can be provided for exclusive SaaS customers on demand.

16.3. Are regular penetration tests carried out?

Yes, on a yearly basis.

16.4. Are regular penetration tests for subcontractors carried out?

No.

16.5. Which independent security audit reports are provided?

None.

16.6. Are regular and independent security audits of subcontractors carried out?

No.

17. Transparency

17.1. What subcontractors who are key to supply the cloud service are used:

Data centre: Interxion

IT service provider : 4NET

17.2. What kind of regular information on changes are provided?

New / discontinued functions.

Please see the Rotronic SaaS SLA contract for more details.

17.3. How are the security policy and controls applied (contractually) with third party providers?

Rotronic has a hosting contract with 4NET, the subcontractor.

17.4. What is the legal relationships and ownership situation of Rotronic?

Rotronic is a private company wholly owned by Process Sensing Technologies, a UK based business.

18. Data Protection

18.1. Where is the storing and processing of personal data taking place?

Outside the member states of the EU or the contract states of the EWR. Zurich, Switzerland.

18.2. How is data protection ensured?

EU directive 95/46/EG §17 (3).

Since May 2018, the EU General Protection Regulation (EU DSGVO / GDPR).

18.3. Is "privacy by design" or "privacy by default" used for the design and implementation of the service?

Yes.

18.4. Are there capabilities for authorities or intelligence services to access data without approval by Rotronic?

No.

19. Licensing

19.1. Does the customer need to consider licenses other than that offered by Rotronic for this service?

No.

20. Service Description

20.1. Does the service support storing files in the cloud?

Yes.

20.2. Does the service has any limitation to the file storage?

No, however, there is a time limitation that can be extended if required*. The standard offering is a 12 month data availability, older data is deleted automatically.

Return of the data: the customer must export the data.

All data is deleted irretrievably 3 months after termination of a contract together with all customer data.

* Depending on account and options.

20.3. Does the service require a local installation at the client's site?

No.

20.4. Is DLP (data leakage prevention) supported for the service?

No, DLP is not yet in use.

21. Legal

21.1. Who has the IP ownership of data uploaded or generated?

The customer.

21.2. Is it legally ensured that the customer’s data will be handed over in case of a service termination?

No, the customer needs to download the data.

However, for an exclusive cloud, the latest back up will be supplied to the customer.