rotronic
MEASUREMENT SOLUTIONS

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.

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. Cloud Service Information

3.1. 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.

4. Data Center

4.1. Which tier level does the data center support?

Rotronic works with an Interxion tier 4 data centre.

4.2. Is a two-factor authentication for access to the data center required?

Yes .

4.3. Where are the data centers located?

Primary data center: Zurich.

Secondary data center: 80km outside of Zurich.

4.4. Can the data center 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.

4.5. How far apart are the relevant data centers?

Over 80km apart.

5. Server Security

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

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

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

Yes (only http and https).

6. Are the hosts secured by the following general hardening techniques?

- Hardened operation systems.
- Deactivation of unnecessary services.

7. 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.

8. Network security

8.1. What security measures are in place against malware?

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

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

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

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

Yes.

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

- SSL.
- VPN.

8.5. Is the communication between the data center and the cloud user encrypted?

Yes.

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

Yes.

8.7. How is the protection against DDoS attacks done?

IPS.

9. Data security

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

Tagging.

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

Yes.

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

No.

9.4. Is stored customer data encrypted?

Yes.

9.5. Is backup data encrypted?

No.

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

Yes.

9.7. Which algorithm is used for deletion?

As of today, no data wiping after deletion.

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

- IP ranges.
- Isolated partitions.

10. ID and Rights Management

10.1. Which authentication protocols are supported?

Password.

10.2. Are role-based access controls used?

Yes.

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

Yes.

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

Yes.

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

Yes.

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

Yes.

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

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

10.8. IS a 2-factor authentication for the management of the cloud service used?

Yes.

11. Monitoring, Logging and Security Incident Management

11.1. 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.

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

Yes.

11.3. Are administrators activities logged and monitored?

Yes.

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

No.

12. Emergency management

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

Yes.

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

Annually.

13. SLA, Portability and Interoperability

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

Yes.

13.2. 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.

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

Yes.

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

Yes, via the RMS software.

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

See the Rotronic SaaS SLA contract.

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

See the Rotronic SaaS SLA contract.

13.7. 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.

14. Security Certification and Audit

14.1. By which certification is the provided service covered for all relevant data centers?

ISO27001.

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

None for the moment.

14.3. Are regular penetration tests carried out?

No.

14.4. Are regular penetration tests for subcontractors carried out?

No.

14.5. Which independent security audit reports are provided?

None for the moment.

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

No.

15. Transparency

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

Data center: Interxion

IT service provider: 4NET

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

New / discontinued functions.

Please see the Rotronic SaaS SLA contract for more details.

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

Rotronic has a contract with 4NET, the subcontractor.

15.4. 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.

16. Data Protection

16.1. 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.

16.2. How is data protection ensured?

EU directive 95/46/EG §17 (3).

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

16.3. Is “privacy by design” or “privacy by default” used for the design and implementation of the service?

Yes.

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

No.

17. Licensing

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

No.

18. Service Description

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

Yes.

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

No.

18.3. Does the service require a local installation at the client’s site?

No.

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

No, DLP is not yet in use, but it is possible to set this up.

19. Legal

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

The customer.

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

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