LANCOM Management Cloud (Public) Data Protection and Data Security

Where is the LANCOM Management Cloud (Public) hosted and operated?

The LANCOM Management Cloud (Public) is hosted by the German service provider SysEleven GmbH (https://www.syseleven.de/) with two geo-redundant data centers in Berlin (master) and Frankfurt am Main.

Both data centers observe the latest standards for modern, secure, and highly available data centers

- → Centralized uninterruptible power supply (UPS) with multiple supply lines
- → Batteries and backup generators
- → Fire protection
- → Protection against water ingress
- → Burglary protection including access concept
- → Access control system
- → Building management system connected to a security center
- → Network feeder from three points of the compass with disjunctive, redundant carrier design

What certifications does the hosting service provider have?

SysEleven GmbH received its first IT-Grundschutz (basic protection) certificate BSI-IGZ-0197-2015 from the BSI (German Federal Office for Information Security) on March 9, 2015. This was supplemented by a native ISO 27001 certification PER-27-2015-001-V from August 4, 2015. To synchronize the audit dates of the two certifications, the native ISO 27001 recertification with PER-27-2018-003 was completed on July 11, 2018, while the BSI IT-Grundschutz certification BSI-IGZ-0333-2018 was issued on August 29, 2018.

Irrespective of this, our data-center operator for the Berlin sites obtained their own native ISO 27001 certification on October 28, 2016, which was successfully re-certified on December 16, 2019. Our data-center operator for the Frankfurt site also received its own certification in accordance with ISO 27001 on December 17, 2017 on the basis of IT-Grundschutz and was successfully re-certified on December 17, 2020.

SysEleven GmbH operates its cloud infrastructure exclusively in security-certified data centers. All of these data centers have at least one ISO 27001 certification. Furthermore,

the sites are aligned with the internationally recognized EN 50600 standard. DIN EN 50600 provides comprehensive specifications for the planning and operation of data centers. The TÜV NORD Group, as the master of the Trusted Site Infrastructure criteria catalog, has also aligned it with the international EN 50600 standard in the form of the new TSI.50600 certification.

Which certifications does the LANCOM Management Cloud (Public) have?

As a hosted application, the LANCOM Management Cloud (Public) does not have its own certification as such. Irrespective of this, the issues of security and trustworthiness are at the heart of the strategic orientation of LANCOM Systems GmbH: Our solution itself and the communication between the devices and the cloud are regularly checked by independent penetration testers. Our portfolio has also been certified by the BSI (German Federal Office for Information Security) (www.lancom-systems.com/bsi-security-certification) and we guarantee that our entire portfolio is free of backdoors (www.lancom-systems.de/pdf/company/LANCOM_Declaration_of_Trustworthiness.pdf).

What are the safeguards against interruptions to availability in terms of business continuity management?

All essential databases are fully replicated and maintained at both geo-redundant data centers at the Berlin and Frankfurt am Main sites, so that in the event of a data center failure, all systems are fully operational again within a maximum of four hours. A failure of this type affects only the traffic of configuration and monitoring data. All devices managed via the LANCOM Management Cloud remain fully up and running at all times, regardless of any connection to the cloud.

Furthermore, daily off-site backups of all configuration data are made to a separate, local instance in the LANCOM Systems data center. The backup data is encrypted.

Which personal data and which business-related data are queried or stored in the LANCOM Management Cloud?

Like all processes in which personal data is processed—and this includes, for example, IP addresses and MAC addresses that are collected and used for network management—network management from the cloud is also fundamentally subject to the GDPR. Exactly which data are collected is listed in our Contract Data Processing Agreement.

Are the data centers of the LANCOM Management Cloud operated on the basis of renewable energies?

In addition to maintaining data protection and data security, the aspects of sustainability and the reduction of GHG emissions are becoming increasingly significant when it

comes to evaluating a cloud service. The data centers of the LANCOM Management Cloud not only offer numerous technologies and processes to ensure high security and availability, but are also characterized by the fact that they are powered 100% by electricity from renewable sources.

How are the data and information sets of the various tenants kept separate?

Each tenant is managed in a strictly separate project. Projects correspond to the customers served by the partner. In other words: You create a project for each customer, and this is where all of the customer data is stored along with global, cross-site settings. There is no connection between individual projects.

How and with what measures are data and applications protected against unauthorized viewing and unauthorized manipulation?

Regular penetration tests carried out by external experts simulate attacks on the LANCOM Management Cloud in order to detect and fix security vulnerabilities. This is supplemented by security audits by renowned major corporations, extensive internal security measures, and the certifications from our hosting service provider as listed.

How is the data protected from unauthorized access and modification when being transported within the LANCOM Management Cloud and when being transported over the Internet?

All data transfers are encrypted via certificate-based SSL.

Where is the transmitted data decrypted?

The decryption takes place exclusively in the LANCOM Management Cloud and the devices managed by it.

What options are available to LANCOM to access which data?

We as LANCOM Systems can only view the configuration data of a tenant if we are expressly invited to be a member of the relevant project.

What options are available to LANCOM's hosting service provider to access data?

The hosting service provider has no access to configuration and customer data.

What availability and what confidentiality does LANCOM grant according to its contracts?

The above parameters are granted.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Germany
info@lancom.de
www.lancom-systems.com