Network policy of Christian-Albrechts-Universität zu Kiel

C A U
Christian-Albrechts-Universität zu Kiel
Rechenzentrum

July 2023

In the event of violations of this policy, the data center (RZ) reserves the right to suspend operations of the respective devices.

§1 Infrastructure and operations

§1.1 Active network devices (exceptions: notebooks, PCs) may not be connected to the campus network and operated without an operating agreement with the data center.

§1.2 Office switches (unmanaged switches) must be reported in writing to technik@rz.uni-kiel.de prior to commissioning, stating the installation location and model.

§1.3 Managed switches may only be installed, configured and operated by data center staff.

§1.4 Network cabinets may only be opened and maintained by data center personnel or in consultation with them.

§1.5 Only the operation of centrally managed network hardware is permitted in network cabinets.

§1.6 Radio networks may only be operated by the data center.

§2 Networks

§2.1 Only work devices may be operated in employee networks (desktop PCs, notebooks, printers, peripheral devices). Servers and similar devices may only be operated in service networks. For devices outside of these categories, the data center reserves the right of acceptance and the requirement of an operating agreement.

§2.2 Service networks may only be operated on the premises of the data center. Exceptions require an operating agreement.

§2.3 Static IP addressing is only permitted in service networks. DHCP must be used in employee networks.

§2.4 Basic network and network configuration services may only be operated by the data center (DHCP, DNS, RADIUS, VPN, etc.).

§2.5 Regular access to networks from outside the university network is only permitted via the VPN operated by the RZ. Access to dedicated employee networks requires an application.

§2.6 The use of remote maintenance services (Teamviewer, AnyDesk, etc.) is only permitted temporarily for user support and not as a permanent access option.

§2.7 The use of so-called network scanners is only permitted by authorized persons and exclusively within sub-networks of the own institution temporarily for administration purposes. Any further analysis, monitoring or filtering of network activities is prohibited.

§2.8 Both client and service networks are only intended for devices for which current updates can be regularly installed by the system administrators (regardless of whether they are in the data center or decentralized). Systems for which software updates are no longer provided by the manufacturer must be disconnected from the network or operated in specially designated networks. The devices must be reported accordingly and require an operating agreement.

Explanations

1 Office switches
Office switches are layer 2 switches without configuration options and do not support layer 2 virtualization, layer 3 routing or spanning tree protocols. However, they are fundamentally different from hubs (layer 1 operation).

2 Employee networks
Employee networks are the networks operated on facility premises for the facility's usual work equipment. Routes from outside into employee networks are granted only via VPN. Routes out of the network are limited to service networks and the Internet.

3 Service networks
Service networks are intended for network hosts that are to provide resources for multiple users. Accordingly, this includes virtual and physical servers, appliances, and related categories of devices.

4 Static IP Addresses vs. DHCP
A static IP address is an IP address that is permanently assigned to an end device or service, e.g., by manual entry. In employee networks with constantly changing end devices, on the other hand, we use dynamic IP addresses that are temporarily assigned automatically by a designated service via DHCP (Dynamic Host Configuration Protocol) each time the end device logs in again.

5 Network Cabinets
Network cabinets in facility rooms are operating locations for data center hardware and, accordingly, are not intended to house resources that seek to provisionally replace data center

services such as computing and storage. Tampering with equipment and/or cabling is accordingly prohibited.

6 Radio networks
The radio networks are generally the eduroam WLAN. Parallel operation of WLAN infrastructures has a disruptive effect on the primary infrastructure and represents a security risk, which is why operation is prohibited. Furthermore, devices that emit their own WLANs for administrative or usage purposes (e.g. printers, smart screens, etc.) must be deactivated.

7 An operating agreement within the meaning of this network guideline is a document that defines the operating parameters for the objects in question and regulates their operation. It also defines the rights and obligations of the operator and the data center.