

CampusNet Server Service

Table of Content

- [Service Level Agreement](#)
 - [Name of Service](#)
 - [Service Description](#)
 - [Service Products](#)
 - [Service Customer](#)
 - [Service User](#)
 - [Server Administrator](#)
 - [Service Continuity](#)
 - [Service Availability](#)
 - [Service Reliability](#)
 - [Service Charging](#)
 - [Service Customer Responsibility](#)
 - [Service User Responsibility](#)
 - [Server Administrator Responsibility](#)
 - [Service Support](#)
 - [Support Extent](#)
 - [Support Channels](#)
 - [Support Availability](#)
 - [Service Workflows](#)
 - [Application Support](#)
 - [Incidents](#)
 - [Requests](#)
 - [Backup Configuration](#)
 - [Key Performance Indicators](#)
- [Measurements of Key Performance Indicators](#)
- [Live System Status](#)
- [Additional Links](#)

Service Level Agreement

Name of Service

CampusNet Server Service, short name "campusnetserv".

Service Description

The service provides network access and hardware maintenance for the business administration application "CampusNet".

Service Products

The following servers are provided for the production environment:

Server	Role
SCNAPP01	application server
SCNSQL01	database server
SCNWEB01	web server

The following servers are provided for the staging environment:

Server	Role
SCNTST01	testing application and web server
SCNTST02	testing database server
SCNTST03	recovery server

Hardware maintenance is performed upon incident or request. The servers are virtualized.

All systems are running Microsoft Windows Server operating system.

Air condition, power supply, uninterruptible power supply, and network access is provided.

The windows servers are members of the Windows domain JACOBS.

The servers are included in IRC-IT's monitoring and reporting system. (see below)

The servers are included in IRC-IT's backup system. (see below)

The recovery server is usually switched off and only activated upon request by the [Service User](#) or [Service Customer](#). Requests follow the Service Support as detailed below.

Service Customer

CampusNet Team: Ulrike Jeschke, Detlef Haubold, Evans Bekoe.

This SLA has not explicitly agreed upon, but the service is being used by the Service Customer for months, hence constituting an implicit acceptance.

Service User

Company Datenlotsen.

Server Administrator

Server administrator is IRC-IT, operating on instructions from [Service Customer](#) and [Service User](#).

Service Continuity

The service is provided until end of June 2010.

Service Availability

The service is available 24/7. Technical support and incident response is provided as described below.

All servers are located in a dedicated VPN 950 "campusnet". Routing into that network is restricted.

HTTPS service of SCNWEB01 is available from Jacobs' network and from the public Internet. RDP service of all servers is available from Jacobs' admin network.

Full network access is provided for the service user via [VPN Access](#). The VPN account `datenlotsen` is provided.

A local account `Datenlotsen` has been setup on all systems, the password been issued to the [Service User](#), and the account has been added to the group `Local Admins`.

Service Reliability

The HTTPS service is 99% reliable, calculated per month.

Service Charging

No internal costs for service provisioning is charged to the [Service Customer](#) or [Service User](#).

Costs resulting from maintenance or changing hardware, software, or external service contracts are charged to the service customer's cost center.

Service Customer Responsibility

The [Service User](#) is responsible for any content stored on or published by the server. IRC and Jacobs University policies, German and International laws apply. This specifically include data protection and telecommunication laws.

Service User Responsibility

The [Service User](#) has to regularly and timely direct the [Server Administrator](#) of updates to install, which are required to ensure secure operation of the system and applications.

The [Service User](#) is responsible for technical soundness of non-standard application services.

Server Administrator Responsibility

The server administrator is responsible for technical soundness of the server regarding operating system and standard applications, as far as covered by Microsoft update services.

The Server Administrator has to:

- prevent abuse of the system by enforcing adequate system, application and data security and integrity,
- update the system and all installed standard services.

If the [Service User](#) has not issued instructions for updates as quoted above, and the [Server Administrator](#) deems updates necessary to comply with obligations as stated here, then

1. the [Server Administrator](#) will inform the [Service Customer](#) and [Service User](#) about updates deemed necessary,
2. will issue a deadline for feedback to the effect of preventing specific updates for ensuring continued service operation,
3. taking this feedback into consideration will update the systems as deemed required,
4. inform [Service User](#) and [Service Customer](#) about the measures taken.

Service Support

Support Extent

The [Service Desk for Faculty and Staff](#) ensures availability of the service products to the extent of this [Service Level Agreement](#).

Support Channels

Service support can be reached by employing the [Service Desk for Faculty and Staff](#) contact channels.

Support Availability

Incident response is available during business hours.

Configuration and extension requests, and other inquiries should follow the procedures and contact channels for [Service Desk for Faculty and Staff](#).

Service Workflows

Application Support

Application support is provided by the service customer by sending email to campus.net@jacobs-university.de.

Incidents

Upon incidents detected by IRC-IT's monitoring system and not resolvable locally to the extent of this [Service Level Agreement](#), the service user and service customer will be informed.

After resolving the incident, the service customer or service user must inform [Service Desk for Faculty and Staff](#) about the taken measures, configuration changes and results.


If after serious failure any of the servers has to be reinstalled, IRC-IT will restore the systems from the last known good backup. The [Service User](#) has then to accommodate the provided restored system to revert to the previous configuration and security level. The [Service Customer](#) has to ensure re-entering of data as is necessary to reach the same data state as was before system failure.

Requests

Requests and inquiries should follow the procedures and contact channels for [Service Desk for Faculty and Staff](#).

Backup Configuration


Fill according to status quo.

 Filling these directories with data to be saved is not performed by IRC-IT.

Restoring data from backup should follow the procedure for incident response. Data will be restored to directories on a server into directories as discussed during the incident response workflow.

Key Performance Indicators

Monthly availability numbers of the HTTPS service as reported by IRC-IT's monitoring system.

 Please note, that the server process implementing the monitored and measured KPI is not maintained by IRC-IT!

Measurements of Key Performance Indicators

Availability of services:

Service	Last Month	Last Seven Days
CampusNet Web Server	snmp	snmp
CampusNet Application Server	snmp	snmp
CampusNet DB	snmp	snmp

Live System Status

The live status of the host systems implementing the service can be seen:

Host
SCNWEB01
SCNAPP01
SCNSQL01

Additional Links

IRC-IT policies can be found at [Policies](#). A non-exhaustive collection of relevant German laws can be found at [Legal](#).

The web service on the web production server can be accessed at <https://campusnet.jacobs-university.de/>. The link is also included for convenience on the page [Link Collection](#).