Conditions for Connecting to the SU network

Version 1.2 | Date of inception : 15 June 2018
These conditions, as included in this document, have to be read with, and are subject to the Electronic Communications Policy (ECP) of Stellenbosch University. Should there be any requests or enquiries they can be addressed to the Director: Information Technology User Services at student@sun.ac.za

Devices:

• Only registered devices with Stellenbosch University's Information Technology Department's (hereafter "IT") approved IP addresses may be connected to the SU network. No static IP addresses are allowed.
• Devices with Microsoft® operating systems must be updated by WSUS automatic updating system with the latest Microsoft updates. Approved antivirus software must be installed and up to date on all Microsoft devices.
• No servers or network services as DHCP, DNS, “File sharing Hubs”, or any other similar equipment which can have a negative influence on the functionality of the network, may be connected to the network or activated on your device without prior written consent by IT.

Network:

• You may only connect equipment to a network connection it was registered for.
• Network connections may not be lengthened or extended for use by more than one device.
• The cost of repairs for any damage to Stellenbosch University's equipment or network points will be for your account. This is not limited to physical damage, but includes any damage to configurations and other services.
• University equipment or the network may not be used for supplying business equipment or services.
• No Wi-Fi hotspots are allowed on the SU network.
• No internet sharing, for example Connectify, Apple and Android hotspots, etc. is permitted on the SU network.
• No routers are permitted on the SU network.
• Only a single network connection is allowed, no sharing with any other device/s.

Passwords:

• You may only use your own password.
• Your personal password may not be made known to anybody else. You will remain responsible for any actions and/or misuse that may be caused by the use of your password and more specifically any costs that may be incurred by the other party by using your password. Should you suspect that your password may be known to somebody else, change it immediately.
• The security, availability and integrity of the network and/or computer systems may under no circumstances be undermined by, for example, trying to access passwords or limited systems.

Data:

• The purpose of the network is intended for official and academic communication. Therefore, data, games, movies, music or illegal “File sharing Hubs” which can swamp the network will not be allowed. Network trafficking between residences will not be allowed.
• The use of pseudonyms, false usernames and anonymous email to and from SU systems are not allowed.
• Do not harass other users with uncivil, slanderous or indecent messages.
• Data or software for which you do not have the necessary licensing, may not be sent over the network or made available via “File sharing” services as DC, KaZaA, etc. Violation of copyright is a serious offence and in some cases a criminal offence.

This document may be amended by the publishing of an updated version, which version will take effect from the date of publication. If a user does not comply with above mentioned conditions, his/her network access may be terminated temporarily or permanently, together with the sanctions as stipulated in the ECP. The matter can also be reported to the concerned authorities (University or SA Police service) according to the seriousness of infringement.

Related articles

- SafeCom Printer setup for MacOS Sonoma
- How to reset your password
- ICT Charges (ICT Student services)
- Graduation Checklist
- FAQs Register & Connecting to Eduroam