Internet and Network Service Usage Rules

- All users are expected to benefit from network services in accordance with BAUN IT Resources Usage Policy.
- Our university's computer network receives internet service with limited resources through the National Academic Network (ULAKNET) and serves its primary purposes of academic, administrative, education and research. It is expected that personal uses on the network will never prevent other users from fulfilling their primary network access requirements (academic, administrative, educational, research, etc.).
- According to Article 5 of the "Regulation on the procedures and principles regarding the collection of public losses", "Public officials in accordance with the relevant articles of the Public Financial Management and Control Law No. 5018; They are responsible for taking the necessary precautions to ensure that public resources are obtained, managed, used, protected, abused, and made available for service at all times, effectively, economically, efficiently and in accordance with the law."
- In accordance with the Law on Intellectual and Artistic Works No. 5846, copyrighted files should not be transferred, copied or distributed. You can share movies, unlicensed software, etc. through file sharing (Peer-to-peer) programs. File sharing not only violates copyrights, but also consumes high bandwidth, leaving no resources for network usage and slowing down traffic. For this reason, such software should not be used.
- It is prohibited to use network resources for personal gain or profit.
- Any activity (DHCP, DNS, proxy, relay, NAT, etc.) that may cause university network resources to be used outside the university or allow people or computers outside the university to identify themselves as being within the university is prohibited. If deemed necessary, these applications will be carried out only by CC system administrators.
- Users must respect the personal rights of other users on the network and must not take actions that threaten the security of their personal information (for example, eavesdropping on packets in network traffic, etc.).
- Users cannot intervene in the hardware that provides network service (switches, cables, wall sockets, etc.) or change their settings in any way. If deemed necessary, these applications will be carried out only by CC network management officers.
- Users cannot add active devices (for example, switch, hub, modem or wireless access point) to the network without the knowledge of CC network management managers.
- It is forbidden to install or put into service software or hardware that provides service over the network (for example, any server software, software that allows computer sharing, software that transmits viruses / Trojan horses, etc.).
- Anyone who sees any violation of these rules is responsible for warning the relevant authorities.
- Users are obliged to install a licensed antivirus program on their personal devices (notebook, tablet, smartphone, etc.) that they connect to the network and to patch the operating system and its programs.
- Users must use licensed antivirus software provided by our University on computers provided by the institution (see Antivirus Policy).
- Computers should not be shared on the network unless necessary. If it must be opened, it must be protected with a password in accordance with the "Password Security Policy".

- To prevent virus infection from websites, the security settings of Internet Browsers (Internet Explorer, Chrome, Firefox, etc.) should be kept above medium level.

Note: This document was created using the Istanbul University Network Usage Policy (Web Address).