USKUDAR UNIVERSITY’S INFORMATION SOURCES USAGE POLICY

In case of using the university's wireless or cable network by using computers, computer laboratories or their own laptops which are open to the use of the students, the following rules must be observed.

- In computers, all kinds of games, including bridge, movies in all kinds of environments (CD, Web, etc.)to listen to music in an audible way and to enter betting sites not allowed.

- Other users who do not comply with the community's general moral rules are disturbing content should not be entered on web pages that can contain content, other users are uncomfortable it should not be.

- Do not use mobile phone to disturb other users, mobile phone negotiations should be held outside the laboratory.

- Computer laboratories are not allowed to consume food and beverages.

- It is a criminal offense to log in to computers with user code other than user code or someone else's code.

- If each user is using his / her personal computer, he / she is responsible for his /it is obliged to protect usernames and passwords given by the university.

- Quiet and calm work environment in the lab and library it should not be spoken loudly.

- Users are responsible for ensuring the healthy functioning of the laboratories they have to obey their directions. There should be no discussion with the staff, and when necessary, suggestions and complaints mechanisms should be used.

- By registering software that threatens information security with the right to write, use, attempt to install and harm computers and software and hardware it constitutes a crime.

- Using laboratory network infrastructure, laptop computers and so on. with network access devices unauthorized internet access is not allowed.

- Peer-to-peer (P2P) point-to-point file sharing programs in addition to violating their licenses, for high-bandwidth purposes it does not leave resources for network use. For this reason, the following the use of all "peer-peer" file sharing tools not limited not provided.

- iMesh, eDonkey2000, Gnutella, Napster, Aimster, Madster, FastTrack, Audiogalaxy, MFTP, eMule, Overnet, neomodus, Direct Connect, Acquisition, BearShare, Gnucleus, gtkgnutell LimeWire, Mactell, Morpheus, Phex, Qtell, Shareaza, Xolox, opennap, WinMX, DC ++, BitTorrent, DC ++, such as programs used, even though your own laptop .

- University network investments, determined by Üsküdar University using resources to serve the primary purposes of academic, administrative, educational and research. Personal use on the wireless network will never use other users' primary network access requirements (academic, administrative, training,interrogation).

- Wireless network resources can not be used for personal gain and profit purposes.

- In wireless or wired networks, it is forbidden to sniff peripheral computers.(rest of the traffic)

- Using wireless network resources, mass mailing, mail bombing, spam, and sending third parties are not allowed.

- Using a wireless network connection (web hosting service, e-mail service etc.).

- The university is responsible for all kinds of activities (proxy, relay, IP sharer, NAT etc.) which could cause the network resources to be used from outside the university, or to let the outside people or the computers introduce themselves as if they are in the university.

- Do activities that threaten network security (DoS attack, portnetwork etc.) constitute a crime.

- If the hardware address (MAC address) of the wireless network interface is changed, the Data Processing Department must be notified. (The system does not allow wireless network access without being introduced to the new address authentication system.)

- Every user who makes use of the wireless network service the resources allocated (network connection, user code, on-campus / off-campus access, etc.) use, safety and security of these resources consciously or unconsciously third prohibited activities that may occur if the it is the first responsibility.

Punishment Sanstions

If one of the above rules are not followed one or more of the following punishments can be applied.

- Limitation of on-campus and / or off-campus network access,

- Closing campus and / or off campus network access,

- Server inter-system code shutdown,

- Activation of interrogation mechanisms within the university,

- Activation of judicial mechanisms.

  Notifications are made with the administrative unit of the students and members who do not comply with the rules. These rules apply from the date of publication. Text can be changed.

  Uskudar University Directorate of Information and Information does not accept responsibility for risks arising from the use of wired and wireless networks. All responsibility belongs to the user.