"OSTİM TECHNICAL UNIVERSITY WIRELESS NETWORK USAGE POLICY"

OSTİM TECHNICAL UNIVERSITY WIRELESS NETWORK USAGE POLICY

The wireless network service provided by our university is intended to serve the educational and research purposes of our students and staff.
Personal use should never hinder the primary purposes of other individuals. In line with this, within the scope of the Information Security Management System (ISMS), the rules to be followed and prohibited activities regarding the use of network resources are outlined below.

1. All access over the wireless network service is recorded in accordance with Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications.
2. Access to the categories specified in Article 8 of Law No. 5651 and the Computer Research and Application Center Information Security Policy is blocked.

   a. Incitement to suicide
   b. Sexual abuse of children
   c. Facilitation of drug or stimulant use
   d. Supply of substances dangerous to health
   e. Obscenity
   f. Prostitution
   g. Providing places and opportunities for gambling
   h. Crimes specified in Law No. 5816 dated 25/7/1951 on Crimes Committed Against Atatürk.

3. The use of Peer-to-Peer (P2P) file-sharing programs is prohibited.
4. The use of VPN (Virtual Private Network) programs is prohibited.
5. Access to websites categorized as Malware, Hacking, Phishing, and Command and Control (C&C) is prohibited.
6. Access to all gaming platforms categorized under Games is prohibited.
7. The use of wireless network resources for personal gain or profit is prohibited.
8. Sending mass emails (mass mailing, mail bombing, spam) using wireless network resources and enabling third parties to do so is prohibited.
9. Hosting server-like computers (web hosting services, email services, etc.) using the wireless network connection is prohibited.
10. Any activity that may cause university network resources to be used from outside the university or that allows individuals or computers outside the university to present themselves as if they are inside the university (proxy, relay, IP sharer, NAT, etc.) is prohibited.

11. Engaging in activities that threaten network security (DoS attacks, port/network scanning, etc.) is prohibited.
12. Every student and/or staff member benefiting from the wireless network service is primarily responsible for the use and security of the resources allocated to them by the university (network connection, user code, on/off-campus access, etc.) and for any prohibited activities that may arise from the conscious or unconscious use of these resources by third parties.
13. In the event that a violation of the above rules is detected, one or more of the following penalties may be applied:

    a. Restriction of on-campus and/or off-campus network access
    b. Termination of on-campus and/or off-campus network access
    c. Initiation of university investigation mechanisms
    d. Initiation of judicial mechanisms

14. Students and staff found to be in violation of the rules will be notified through the relevant administrative unit.
15. These rules are effective as of the date of publication. Changes may be made to the text as deemed necessary. The current version of the rules can be accessed at this web address.