

# **İstanbul Üniversitesi Bilgisayar ve İnternet Kullanım Talimatnamesi**

Üniversitemizde bilgisayar kullanan tüm personelin, aşağıda açıklanan kurallarla birlikte, Rektörlüğümüzün imzaladığı ve web sayfamızda yayınlanan "**Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) Kullanım Politikası Sözleşmesi**"ndeki diğer hükümlere de titizlikle uymaları, internet hizmetlerinin aksamadan yürütülmesi bakımından büyük önem taşımaktadır.

Sistem ve Ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. İstanbul Üniversitesi Rektörlüğü bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç olduğundan şüphelenilirse yasa uygulayıcı ile işbirliği yapar.

## **1) Bilgisayar Ağı ve İnternet Kullanım Kuralları:**

Rektörlüğümüzün imzalamış olduğu "Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) Kullanım Politikası Sözleşmesi" kapsamında, Üniversitemizde bilgisayar ağı ve internet kullanan tüm personelin uyması gereken kuralları tanımlamak üzere hazırlanmıştır.

- Üniversitemizin bilgisayar ağı (İÜNet), Ulusal Akademik Ağ (ULAKNET) üzerinden sınırlı kaynaklarla internet hizmeti almaktadır ve akademik, idari, eğitim ile araştırma birincil amaçlarına hizmet etmek üzere yapılmıştır. Ağ üzerindeki kişisel kullanımlar hiçbir zaman diğer kullanıcıların birincil ağ erişim gereksinimlerini (akademik, idari, eğitim, araştırma) yerine getirmelerine engel olmamalıdır.
- Üniversitemizin farklı birimlerinde yürütülen internet uygulamaları, bilgi sistemleri alanına giren her konuda akademik ve idari birimlerin gereksinim duyduğu her türlü alt yapı, donanım, vb. hizmetleri Bilgisayar Bilimleri Uygulama ve Araştırma Merkezi (BUYAMER) tarafından yürütülmektedir.>
- BUYAMER gerekli görüldüğü durumlarda kurallar üzerinde değişiklik yapabilir. Son değişiklikler <http://buyamer.istanbul.edu.tr> adresinden takip edilebilir.
- Peer-to-peer dosya paylaşım programları, film, lisanssız yazılımlar telif haklarını ihlal etmekle kalmayıp yüksek bant genişliği tutarak ağ kullanımına kaynak bırakmamakta ve trafikte yavaşlamaya neden olmaktadır. Bu sebeple bu tür yazılımlar bulundurulmamalı ve dağıtımı yapılmamalıdır.
- Telif hakları yasasına aykırı olarak dosya transferi, kopyalanması ve dağıtımı yapılmamalıdır.
- Ağ kaynaklarının şahsi kazanç ve kar amacı ile kullanılması yasaktır.
- İÜNet olanakları hiçbir şekilde ticari, siyasi, genel ahlak kurallarına aykırı reklam, duyuru, propaganda (Spam iletiler) ve bunlar gibi içeriği olan veri, mesaj transferi amacıyla kullanılmamalıdır.
- Üniversite ağ kaynaklarının üniversite dışından kullanılmasına sebep olabilecek ya da üniversite dışındaki kişi ya da bilgisayarların kendilerini üniversite içindeymiş gibi tanıtılmalarını sağlayacak her tür faaliyet (DHCP, DNS, proxy, relay, IP sharer, NAT vb.) yasaktır.
- Kullanıcı ağ kaynağına veya servisine saldırı amaçlı (DOS saldırısı, port/network taraması, paket dinleme v.b. uygulamalar ile) zarar verecek girişimlerde bulunmamalıdır.
- Kullanıcılar İÜNet hizmetinin verilmesini sağlayan donanıma (switch'ler, kablolar, duvar prizlerine, v.b) hiç bir şekilde müdahale edemez, ayarlarını değiştiremezler. Birimimizin bilgisi olmadan switch ya da hub dahil edemezler.
- Başka bir kullanıcının posta adresi, o kullanıcının açık izni olmadan mesaj gönderme amacıyla kullanılmamalıdır.
- Kullanıcılar ağa bağlantı yaptıkları cihazdan ve bu cihazlarla yapılan her türlü kural dışı işlemlerden sorumludur. Bu kaynakların üçüncü kişilere kullanılması durumunda ortaya çıkabilecek her türlü kural dışı hareketlerden birinci derecede sorumludur.
- Yurt odasında, her öğrencinin adına kayıtlı bilgisayarların problemleri (bozuk ağ kartı, bozuk işletim sistemi v.b) kullanıcının sorumluluğu altındadır.

- Kullanıcılar ağa bağlantı yaptıkları bilgisayarlara bir antivirüs programı yüklemek, işletim sistemi ve içindeki programların yamalarını yapmakla yükümlüdürler.
- Mecbur kalınmadıkça bilgisayarlar ağda paylaşım açılmamalıdır. Eğer açılması gerekiyorsa, şu andaki virüsler tek karakterli şifreleri geçebildikleri için mutlaka en az 4-6 karakterli bir şifre ile korunmaya alınmalıdır.
- Web sitelerinden virüs bulaşmasına engel olmak için Internet Explorer, Firefox, vb. browserların güvenlik ayarları orta düzeyin üzerinde tutulmalıdır.
- Güvenli olmadığı bilinen sitelere (bedava mp3, program vb.) girilmesi kesinlikle yasaktır.
- İnternette bedava dağıtılan her programa güvenilmemeli ve virüs taraması yapılmadan bilgisayara yüklenmemelidir.
- ftp, web, vb. çeşitli amaçlarla sunucu kurmak ve yönetmek isteyen tüm birimlerin, <http://buyamer.istanbul.edu.tr> adresinde yer alan "Sunucu Yönetim Talep Formu"nu eksiksiz doldurarak BUYAMER'e başvurmaları gereklidir.
- Web sayfalarını Üniveristemiz web sunucusunda yayınlamak isteyen tüm birimlerin, <http://buyamer.istanbul.edu.tr> adresinde yer alan "Web Alanı Talep Formu"nu eksiksiz doldurarak BUYAMER'e başvurmaları gereklidir.
- Yukarıda belirtilen kurallara uyulmadığı takdirde aşağıdaki yaptırımlardan bir ya da birkaçı uygulanabilir;  
Kampus içi ve/veya kampus dışı ağ erişiminin sınırlandırılması,  
Kampus içi ve/veya kampus dışı ağ erişiminin kapatılması,  
Sunucu sistemler üzerindeki kullanıcı kodunun kapatılması,  
Üniversite bünyesindeki soruşturma mekanizmalarının harekete geçirilmesi,  
Adli yargı mekanizmalarının harekete geçirilmesi.

## II) Bilgisayar Kullanım Kuralları:

### A) Donanım

- Üniversite işleri için personelin kullanıma verilen bilgisayarlar kuruma ait olup özenle kullanılmalıdır.
- Bilgisayarların kasaları mutlaka yerden yukarıda mümkünse masa üzerinde olmalıdır. Bilgisayarlar toz , nem ve sığağa karşı korunmalıdır.
- Yazıcılar ve monitör de dahil olmak üzere tüm parçalar direk güneş ışığına maruz bırakılmamalı, kalorifer peteklerine uzak tutulmalıdır.
- Bilgisayar masası üzerinde yiyecek ve içecek bulundurulmamalıdır. Eğer klavye üzerine sıvı bir madde dökülürse klavye hemen ters çevrilmeli, kurumaya bırakılmamalıdır.
- Kasa, klavye ve fare haftada bir kez hafif nemli bir bez (kolonyalı mendil vb.) ile temizlenmelidir. Monitörün ekran temizliği mutlaka kuru bez ile yapılmalıdır. Aksi takdirde ekranda lekeler oluşmaktadır.
- Bilgisayarların çalışabilmesi için gereken elektriğin sağlıklı olması şarttır. Kullanıcılar sahip oldukları bilgisayarlarını en yakın prize takmadan önce prizleri kontrol ettirmelidir, mümkünse topraklı priz kullanılmalıdır. Eğer binada Kesintisiz Güç Kaynağı (UPS) var ise UPS kullanılmalıdır.
- Bilgisayara ait elektrik, data ve Internet kabloları kesinlikle çalışma sahası içinde yerde olmamalı ve ezilmemelidir. Kablo bağlantıları bu kurala dikkat edilerek yapılmalıdır.

### B) Yazılım

- İşletim sistemi, ofis programları sadece İ.Ü. Bilgi Teknolojileri Ofisi tarafından yüklenebilir.

- Antivirüs yazılımı olarak İ.Ü. Bilgi Teknolojileri Ofisi tarafından merkezi olarak dağıtımı yapılan ve yönetilen yazılım kullanılabilir. Yazılımla ilgili soru ve sorunlar için İ.Ü. Bilgi Teknolojileri Ofisi ile temasa geçilmelidir.
- Mevcut programların üst versiyonlarını yüklemek bilgisayarınızın kaynaklarını zorlayacağından tavsiye edilmez. Yüklenen tüm programlar bilgisayarınızın hafıza ve işlemcisinde yük oluştururlar. Bu nedenle ihtiyaçlar doğrultusunda İ.Ü. Bilgi Teknolojileri Ofisi danışılarak karar verilmelidir. Bilgisayarınızı, hiç bir ek özelliğini kullanmayacağınız Office 2003, XP yada Windows 2000 yüklemek veya XP ye yükseltmek, bilgisayarın yavaş çalışmasına hatta kilitlenmelere sebep olacaktır.
- Her kullanıcı bilgisayarının dış temizliğinde olduğu kadar iç temizliğinde de duyarlı olmalıdır. Sistem kaynaklarını sömüren gereksiz hiç bir program kurulmamalıdır. (Oyun, haber vericiler, ilave güvenlik duvarı (firewal) vb.)
- Bilgisayarda yazılımsal sorunlar yaşamaya başlanması en son yüklediğiniz yada tam olarak kaldıramadığınız programlarla ilgilidir. Bu nedenle içeriği ve tam olarak nasıl çalıştığı bilinmeden herhangi bir program bilgisayara yüklenmemelidir.
- Sürekli tekrarlanan arızalarda, büyük bir olasılıkla kullanıcı kusuru sözkonusudur. Bu konuda ısrar edilmesi halinde, kullanıcıya yaptırımlar uygulanabilecektir.
- Kullanıcının tanımadığı kişilerden gelen ve özellikle eki (attachment) olan elektronik postaları (e-mail) açmadan silinmelidir. Postalarınız merkezi olarak antivirüs yazılımı ile kontrolden geçmekle birlikte, tam güvenlik için bu uygulama gereklidir.

#### **C) Güvenlik ve virüslerden korunmak için uygulanabilecek bazı önlemler:**

- İşletim sistemi her zaman en son yama (patch) lar ile güncel tutmaya çalışılmalıdır.
- Mecbur kalınmadıkça bilgisayarlar ağda paylaşım açılmamalıdır. Eğer açılması gerekirse, mutlaka en az 4-6 karakterli bir şifre ile korumaya alınmalıdır. Şu andaki virüsler tek karakterli şifreleri geçebilmektedirler.
- Virüsler web sitelerinden de bulaşabilmektedir. Bu nedenle Internet Explorer, yada hangi program kullanıyorsa güvenlik ayarlar orta düzeyinin üzerinde tutulmalıdır. Bu en azından bazı scriptler ve ActiveX kodlar ile bulaşabilecek virüsleri engelleyebilmektedir.
- Güvenli olmadığı bilinen sitelere (bedava mp3, program yada porno) girilmesi kesinlikle yasaktır.
- Bilgisayarınıza yüklediğiniz bazı programlar da sisteminize zarar verebilir. Bu nedenle Internet'te görülen her programa güvenilmemeli ve bilgisayarınıza yüklenmemelidir. Denetim Masasında Program Ekle/Kaldır başlığı altında sisteminizdeki programları görebilmek ve buradan bilinmeyen ve kullanmayan programları kaldırabilmek mümkündür.
- Mutlaka bir antivirüs programı edinilmelidir. Kişisel bir antivirüs programı kullanılmıyor ise merkezi antivirüs programı yüklenmelidir.
- Antivirüs programının kişisel olması durumunda sürekli güncel tutulmasına özen gösterilmelidir.
- Bilgisayar sistemi zaman zaman taranmalıdır.
- Virüs uyarısı ile karşılanması halinde, virüs programı tarafından temizlenmeli veya karantınaya alınmalıdır.
- Bilgisayarın çökmesi sürekli karşılaşılabilecek bir sorundur. Bu nedenle bilgilerinizin bir yedeği bulundurulmalıdır.