BAŞKENT ÜNİVERSİTESİ İNTERNET KULLANIM POLİTİKASI

Günümüzde teknolojinin hızla gelişmesi sonucunda bilgi, kolay erişilebilir hale gelmiştir. Özellikle kritik sistemlerin dijitalleşmesi ile beraber siber güvenlik kavramı, kurumsal bilgi güvenliği kapsamında değerlendirilmelidir. Hem kişisel e-posta ve diğer hesaplarımız, kişisel bilgisayarlarımız hem de kurumsal bilişim sistemlerimiz sürekli siber saldırılara maruz kalabilmektedir.

Bu kapsamda Hukuk sisteminde ADLİ BİLİŞİM BİLİMİ oluşmuş ve 5237 sayılı Türk Ceza Kanununda "BİLİŞİM ALANINDA SUÇLAR" madde başlığı ile düzenleme yapılmıştır. TCK'da ve diğer kanunlarda suç olarak tanımlanan fiillerin işlenmesinde bilgisayar teknolojisi kullanılmış ise oluşan suçlar bilişim suçu olarak kabul edip, kanunda belirlenen cezalar artırıma tabi tutulmuştur (TCK, hakaret, sahtecilik, dolandırıcılık, Fikir ve Sanat Eserleri Kanununa aykırı olarak yazılımın izinsiz kullanımı, Kişisel Verilerin Korunması Kanununa aykırı olarak kişilerin şahsi ve mahrem bilgilerin kaydedilmesi veya yasaya aykırı olarak elde edilmesi, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna aykırı davranılması). Ayrıca kanunlarda kişilere ve kurumlara, verilerin güvenliğinin sağlanması hususunda büyük sorumluluklar yüklenmiştir. Bu kapsamda üniversitemiz gerekli tedbirleri alıp siber güvenlik, bilgi güvenliği politikaları ile sürdürülebilir hale getirmek için çalışmalarını yürütmektedir.
Kurum çalışanlarımızın da kişisel bilgisayarlarının kullanımında veri güvenliğinin sağlanmasına özen göstermeleri gerekmektedir.

Ülkemizdeki bütün Üniversitelerde olduğu gibi Üniversitemizin de internet erişimi TÜBİTAK-ULAKNET (Ulusal Akademik Ağ) üzerinden sağlanmaktadır. İstenmeyen ağ trafiğinin oluşmamasına yönelik önlemler başta olmak üzere siber güvenlik önlemlerinin belli bir kısmı bu kurum tarafından verilmekle beraber üniversitemizin de bu kapsamda sorumlulukları bulunmaktadır.

Üniversitemiz ağ ve internet kullanım trafiğinde son dönemlerde artışlar meydana gelmiştir. Yapılan analizlerde bu artışın büyük bir oranı istenmeyen internet erişim trafiğinden kaynaklandığı tespit edilmiştir. Bu sebeple kullanıcılarımız üniversitemiz ağ ve internet hizmetini etkin, verimli ve güvenli biçimde kullanabilmeleri için aşağıda belirtilen kurallara dikkatle uyum sağlamaları gerekmektedir.

1- Kullanıcılar, bilişim kaynaklarını sadece eğitim, bilimsel ve akademik amaçlarla kullanabilir, hiçbir şekilde ticari, siyasi, genel ahlak kurallarına aykırı reklam, duyuru, propaganda, istenmeyen iletiler (spam) vb. içeriğe sahip olan veri ve mesaj transferi amacıyla kullanmamalıdır. Film, oyun, bahis ve kumar sitelerine girilmemesine hassasiyet gösterilmelidir.
2- Herhangi bir kullanıcı ağ sistemi üzerinde DHCP, PROXY, DNS, NAT vb. servisler vermemelidir.
3- Kullanıcılar, ağ kaynağına veya servisine zarar verecek saldırı amaçlı (DOS saldırısı, port/network taraması, paket dinleme vb. uygulamalar) girişimlerde bulunmamalıdır.
4- Noktadan noktaya (Peer-to-peer P2P) dosya paylaşım programları ile indirilen film, mp3 ve lisanssız yazılımlar, telif haklarını ihlal etmekle kalmayıp, indirme esnasında yüksek bant genişliği oluşturarak ağ kaynaklarını tüketmekte ve ağ trafiğinde yavaşlamaya neden olmaktadır. Bu sebeple kullanıcılar, bilgisayarlarında bu tür yazılımlar bulundurmamalı ve dağıtımı yapmamalıdır.
5- Kullanıcılar, internet hizmeti sağlayan aktif ve/veya pasif ağ donanımlarına (ağ anahtarı (swicth), kablosuz ağ erişim cihazı (Access point), ağ kabloları, ağ prizi vb.) hiçbir şekilde müdahale etmemeli, ayarlarını değiştirmemelidir.

6- Kullanıcılar, internet hizmetini kullandıkları bilgisayardan ve bu bilgisayarla yapılan her türlü kural dışı işlemlerden sorumludur. Aynı zamanda bilgisayarlarının üçüncü kişilere kullandırılması durumunda ortaya çıkabilecek her türlü kural dışı işlemlerden kendisi sorumludur.
7- E-posta ve diğer hesap parolalarının daha güçlü olmasına, periyodik olarak değiştirilmesine, ikinci ve üçüncü şahıslarla paylaşılmamasına, parola değişimi veya kota aşımı gibi e-posta yoluyla gelen aldatıcı mesajlara hiçbir şekilde itibar edilmemelidir. Kullanıcılar parolalarının kaybedilmesinden veya izinsiz bir şekilde başka birinin kullanıcı parolasını ele geçirilmesinden kendisi sorumludur.

Belirlenen kurallara uymayanlar, kanunlarda tanımlanan suçların oluşması halinde sonuçlarından sorumlu olacakları gibi kişisel bilgisayarlarının IP adreslerinin kontrolünde belirlenen kurallara aykırı davrananlar haklarında disiplin soruşturması yoluna da başvurulabilinecektir.