1.AMAÇ

Bu politika; Hakkari Üniversitesinde sunulan internet hizmetinin uygun olmayan kullanımını engelleyerek; Hakkari Üniversitesinin yasal yükümlülüklerini, internet güvenliğini, kapasite kullanımını ve kurumsal imajını korumak için gerekli kuralları tanımlamak amacıyla oluşturulmuştur.

2.KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında Hakkari Üniversitesi akademik/idari personelleri, öğrencileri ve dış paydaşlarını kapsar.

3.TANIMLAR VE KISALTMALAR

3.1.Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, risk yaklaşımına dayalı yönetim sistemidir.

3.2.Bilgi: Hakkari Üniversitesi süreçlerinin devamlılığı için gerekli olan ve bu nedenle değeri olan, dolayısı ile uygun şekilde korunması gereken bir veridir.

3.3.Bilgi varlıkları: TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi dâhilinde Hakkari Üniversitesi'nde bulunan ve bilgi güvenliği için anlam taşıyan tüm varlıklar.

3.4.Üniversite: Hakkari Üniversitesi

3.5.Rektör: Hakkari Üniversitesi Rektörü.

3.6.Kalite Yönetim Temsilcisi: Kalite Yönetim Sistemi şartlarını, gerekli proseslerin oluşturulmasını, uygulanmasını ve sürekliliğini sağlayarak, Hakkari Üniversitesi Kalite Yönetim Sisteminin performansı ve iyileştirme için fırsatlar ile ilgili üst yönetime rapor sunan, Hakkari Üniversitesinde, müşteri şartlarının bilincinde olunmasını tüm çalışanlarda sağlayan, Hakkari Üniversitesi Kalite Yönetim Sistemindeki değişiklikleri planlayan ve uygulayan, kalite yönetim sisteminin bütünlüğünü güvence altına alan Hakkari Üniversitesi çalışanı.

3.7.Daire Başkanı: Hakkari Üniversitesi Bilgi İşlem Daire Başkanı

3.8.VPN (Virtual Private Network-Sanal Özel Ağ): İnternet üzerinden güvenli ve şifreli bir bağlantı sağlayarak verilerinizi koruyan ve gizliliğinizi artıran bir ağ teknolojisidir.

3.9.DNS: Domain Name System kısaltmasıdır. Alan adlarını IP adreslerine çevirerek internet üzerindeki cihazlar

ve sunucular arasında iletişimi sağlayan sistemdir.

3.10.İnternet : Bilgisayarlar ve diğer dijital cihazlar arasında bilgi paylaşımı, iletişim ve etkileşim sağlayan küresel ağdır.

3.11.Erişim : İnternet içeriklerine bağlanılmasıdır.

3.12.E-Posta: Elektronik posta anlamına gelir ve internet üzerinden elektronik olarak gönderilen ve alınan iletileri ifade eder.

3.13.Proxy: İnternet trafiğinizi başka bir sunucu üzerinden yönlendirerek IP adresinizi gizleyen ve bağlantınızı anonim hale getiren bir ara sunucudur.

3.14.Sunucu (Server): İstemcilere veri, hizmet veya kaynak sağlayan ve genellikle ağ üzerinden erişilen bir bilgisayar veya yazılım sistemidir.

3.15.ULAKNET: TUBİTAK Ulusal Akademik Ağ ve Bilgi Merkezi

4.SORUMLULAR

4.1.Bilgi Güvenliği Yönetim Sistemi Komisyonu: Bu politikanın hazırlanmasından ve güncellenmesinden sorumludur.

4.2.Rektör: Politika onaylanması ve yürürlüğe konulmasından sorumludur.

4.3.Kalite Yönetim Temsilcisi: Politikanın KYT-PRD-01 Dokümanların Kontrolü Prosedürü'ne göre kontrol edilmesinden, politikaya doküman kodu verilmesinden, politika revizyona uğrarsa takibinden ve revizyon numarasının verilmesinden, prosedürün güncel doküman listesine eklenmesinden ve listenin takibinden sorumludur.

4.4.Daire Başkanı: Politika kontrolü ve uygulanabilirliğinin sağlanmasından sorumludur.

4.5.Kullanıcı: Politika içinde belirtilen faaliyetlerin uygulanmasından sorumludur.

5.UYGULAMA

5.1.Üniversitenin İnternet Erişim Hizmeti; idari/akademik personellere ve öğrencilere yönelik verilen kablolu ve kablosuz ağ erişim hizmetidir. Bu hizmet Türkiye Cumhuriyeti ilgili mevzuatlar ve politikalar çerçevesinde, üniversiteler ve araştırma kurumları arasında araştırma ve eğitim amaçlı ağlar kuran, işleten, bu ağların yurtiçi

ve yurtdışındaki ağlarla bağlantısını sağlayan TUBİTAK ULAKNET tarafından sağlanmaktadır.

5.2. Üniversite, ULAKNET ile Üniversite internetini, kullanıcılara ULAKNET Kullanım Politikasında belirlenen hükümler çerçevesinde kullandırma hak ve sorumluluğuna sahiptir.

5.3. Kullanıcılar Üniversitenin internet hizmetini kullanırken kimlik doğrulama yöntemine tabi tutulmaktadır.

5.4. Kullanıcılar Üniversite internetini, eğitim, öğretim, bilimsel ve teknolojik araştırma ve geliştirme, bilimsel, teknolojik ve kültürel bilginin yayılması veya erişilmesi amaçları için kullanmalıdır.

5.5. Kullanıcılar; internet ağı hizmetinin verilmesini sağlayan yazılım veya donanıma (ağ anahtarı, kablosuz ağ erişim cihazı, ağ kabloları, ağ prizi vb.) hiç bir şekilde müdahale etmemeli, ayarlarını değiştirmemelidir.

5.6. Üniversite misafirlerini internet erişimleri için BLG-PRD-XXX-Ağ Güvenliği ve Yönetimi Prosedüründe belirtilen hükümler uygulanır.

5.7. İnternet üzerinden erişilen tüm web siteleri ve hedef sistemlerle ilgili olarak, erişimi gerçekleştiren kullanıcı sorumludur.

5.8. Kullanıcı, internette gezinirken karşılaşabileceği (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olmalı ve bunlara tıklamamalıdır.

5.9. Kullanıcının internet üzerinde yapacağı kişisel işlemlerde (banka, alışveriş, mail vb.) oluşacak olumsuzluklardan Üniversite sorumlu değildir.

5.10. İnternet Erişim Hizmeti aşağıda belirtilen şekilde kesinlikle kullanılamaz;

- Doğrudan veya dolaylı olarak ticari amaçlarla kullanılamaz.
- İstenilmeyen siteler (pornografi, oyun, kumar, şiddet içeren vs.) için kullanılamaz.
- Kullanıcı, Üniversite faaliyetleri için kullanmakta olduğu parolaları, kritik kurum bilgilerini, kullanıcı adlarını, kurumsal e-posta adreslerini; kişisel sosyal medya hesaplarında,e-ticaret sitelerinde, forum sitelerinde vb. kişiye özel faaliyetleri için hiçbir şekilde kullanamaz,

- Diğer kullanıcıların İnternet kullanımını ve/veya ağ üzerindeki kaynaklara erişimini engellemeye çalışamaz,
- Ağ üzerindeki nesnelere yönelik saldırıları gerçekleştiremez,
- Ağ üzerindeki herhangi bir kaynağa yetki olmadan erişmek ve/veya başkasına ait trafiğin/bilgilerin izlenmesi, araştırılması veya kaydedilmesini sağlayamaz,
- İnternet kullanım kapasitesini (Bant genişliğini) diğer kullanıcıları olumsuz etkileyecek şekilde kullanamaz,
- Genel ahlak ilkelerine aykırı materyal üretemez, barındıramaz, iletemez,
- Siyasi propaganda yapamaz,
- Rastgele ve alıcının istemi dışında mesaj (Spam iletiler) gönderemez,
- VPN, Proxy ve DNS değişiklikleri yapılarak internete bağlanamaz,
- Türkiye Cumhuriyeti yasalarına ve Üniversite iç mevzuatlarına aykırı faaliyetlerde bulunamaz,

5.11. Üniversite internet kullanıcıları iş bu politikadaki bir veya daha fazla kurala uymamaları halinde söz konusu aykırılığa bağlı olarak aşağıdaki hükümler uygulanır;

- Kullanıcılar yazılı olarak uyarılır,
- Kullanıcının Üniversite internet erişimi sınırlı veya sınırsız süre ile kapatılır,
- Üniversite bünyesindeki akademik/idari soruşturma mekanizmaları harekete geçirilir,
- Bu belgenin yetersiz kaldığı durumlar Üniversite makamlarınca değerlendirilir.
- Üniversite internet erişim ve kullanımından kaynaklanabilecek her türlü bilgi güvenliği ihlali ile ilgili olarak BLG-PRD-XXX-Bilgi Güvenliği İhlal Olayları Prosedürü, BLG-PRD-XXX Ağ Güvenliği ve Yönetimi, BLG-PRD-XXX Risk Yönetimi Prosedürü ile BLG-PRD-XXX Tehdit İstihbarat Prosedürü uygulanır ve gerekli görülmesi durumunda mevcut disiplin süreçleri işletilir. 5651 sayılı kanun gereği, adli yargı mekanizmaları harekete geçirilebilir.

6.İLGİLİ DÖKÜMANLAR

6.1.BLG-PRD-XXX-Ağ Güvenliği ve Yönetimi Prosedürü

6.2.BLG-PRD-XXX-Bilgi Güvenliği İhlal Olayları Prosedürü

6.3.BLG-PRD-XXX Risk Yönetimi Prosedürü

6.4.BLG-PRD-XXX Tehdit İstihbarat Prosedürü