1. AMAÇ

Bu politika, Hakkari Üniversitesi ağ altyapısının güvenli, verimli ve kesintisiz bir şekilde yönetilmesini sağlamak amacıyla oluşturulmuştur.

2. KAPSAM

Bu politika, Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında Hakkari Üniversitesi'nin tüm ağ bileşenlerini, cihazlarını, kullanıcılarını ve bu ağ üzerinden sunulan hizmetleri kapsamaktadır.

3. TANIMLAR VE KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi'nin kısaltmasıdır.

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

Ağ: İki veya daha fazla cihazın (bilgisayar, sunucu, yazıcı, vb.) birbirleriyle veri alışverişi yapabilmesi için oluşturulan bağlantılar bütünüdür.

4. SORUMLULUKLAR

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

Bilgi İşlem Daire Başkanı: Politikanın kontrolü ve uygulanabilirliğinin sağlanmasından sorumludur.

Rektör: Politikanın onaylanması ve yürürlüğe konulmasından sorumludur.

İlgili Personel: Politika içinde belirtilen faaliyetlerin gerçekleştirilmesinden sorumludur.

5. UYGULAMA

a) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedekli ekipman bulundurulmalı veya bakım anlaşmaları yapılmalıdır.

b) Ağ ekipmanları sadece yetkilendirilmiş kişiler tarafından erişilebilir ve yönetilebilir olmalıdır. Yetkisiz erişime karşı korunmalıdır.

c) İletişim ağları üzerinde bulunan tüm Üniversite kaynaklarına erişim, kullanıcı adı ve parola olmak üzere kimlik doğrulama yöntemleri kullanılmalıdır.

d) Ağ hizmetlerinden faydalanan her kullanıcı, erişiminin iş amaçları için verildiğini hatırlayarak iş amaçları dışında kullanımı asgari düzeyde tutarak ağ kaynaklarının etkin kullanımına katkı sağlar.

e) Üniversite ağına sadece Üniversite bilgisayarları bağlanmalıdır. Üniversite dışında bir bilgisayar bağlanacak ise yetkili kişinin izni ve gözetiminde izin süreci nasıl oluyor? bağlanmalıdır.

f) Personeller Üniversitenin faaliyet göstermiş olduğu alanlardaki ağları dinlemeye yönelik herhangi bir uygulamayı, programı bilgisayarına kurmamalı ve bulundurmamalıdır.

g) Ağ bağlantıları düzenli olarak **Ağ ve Sistem Hizmetleri Şubesi** tarafından takip ve kontrol edilmelidir.

h) 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da belirtilen trafik izlerinin kaydedilmesi ve belirtilen sürelere göre saklanması sağlanmalıdır.

i) Üniversite internet ağına misafirler alınmamalıdır.

j) Kamera, kablosuz ağ ve kullanıcı ağları birbirinden ayrı olmalıdır.

k) Uzaktan bağlantı için kullanılacak portların güvenliği **Ağ ve Sistem Hizmetleri Şubesi** tarafından sağlanmalıdır.

l) Dış ağlara yapılan bağlantılarda Üniversite ağları ile ilgili bilgilerin sızmasını önleyecek tasarımlar yapılır.

m) Ağ üzerinde kullanıcılar her yöne erişememeli ve erişimleri **Ağ ve Sistem Hizmetleri Şubesi** tarafından kısıtlanmalıdır.

n) Ağ cihazları yılda en az 1 defa Bilgi İşlem Daire Başkanı'nın belirlediği tarihte açıklık tarama testlerinden geçirilerek güvenli hale getirilmelidir.

o) Ağ ve güvenlik cihazları üzerinde yapılan değişiklikler için için **BLG-PR- Değişiklik Yönetimi Prosedürü** işletilmelidir.

p) Ağ cihazlarının konfigürasyonları her değişiklikten sonra yedeği alınarak saklanmalıdır.

q) Politika ihlali disiplin kurallarına tabi olmanıza neden olabilir ve yasal sonuçlar doğabilir.