1. AMAÇ

Bu politikanın amacı, zararlı yazılımların Hakkari Üniversitesine ait ve/veya Hakkari Üniversitesi tarafından yönetilen kullanıcı uç nokta cihazları ile altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engellemek için antivirüs kullanım esaslarının tanımlanmasıdır.

2.KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında olan, zararlı yazılımların tehdidine maruz kalabilecek tüm Hakkari Üniversitesinin bilgi varlıklarını kapsamaktadır.

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.Kullanıcı: Hakkari Üniversitesi akademik/idari personelleri ve öğrencileri

3.9.AntiVirüs: Bilgisayar sistemlerini zararlı yazılımlardan korumak için tasarlanmış bir yazılım türüdür.

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

oluşturulan bağlantılar bütünüdür.

3.11. HUBİS: Hakkari Üniversitesi Bilgi Sistemleri

4. SORUMLULAR

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

4.2. Rektör: Politikanın onaylanması ve yürürlüğe konulmasından sorumludur.

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

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

4.5. Kullanıcı: Politika içinde belirtilen faaliyetlerin uygulanmasından sorumludur.

5. UYGULAMA

5.1. Akademik personel/idari personel, öğrenciler ve misafir?? Kullanıcı olup, bu politikanın hükümlerini uygulamakla yükümlüdür.

5.2. Üniversite bünyesinde bulunan tüm kullanıcı uç nokta cihazları ve alt yapı bileşenlerinde (bilgisayar, sunucu .. vb) antivirüs yazılımı yüklü olmalıdır.

5.3. Antivirüs yazılımı otomatik olarak antivirüs sunucusu ile güncellenmelidir.

5.4. Antivirüs yazılımı yüklü olmayan veya güncel olmayan sistemler Üniversite ağına bağlanamaz. Ağın güvenliği ile ilgili BLG-PRD-XXX Ağ Güvenliği ve Yönetimi Prosedürü adımları uygulanmaktadır.

5.5. Hiçbir kullanıcı **Ağ ve Sistem Hizmetleri Şubesi** onayı olmadan herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz veya durduramaz.

5.6. Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta ve ekleri virüs içerebilir. Kesinlikle açılmamalıdır. Bu tür özelliklere sahip bir mesaj alındığında hemen **Ağ ve Sistem Hizmetleri Şubesi'ne** HUBİS üzerinden BLG-FRM-XXX Ağ ve Sistem Talep Formu ile talep gönderilmeli ve yetkili kişiler müdahale edene kadar e-

postanın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.

5.7. Zararlı programları (virüsler, solucanlar, truva atı, istenmeyen e-postalar vb.) Üniversite bünyesinde oluşturmak ve dağıtmak yasaktır.

5.8. Bilgisayarlara takılan taşınabilir aygıtlar, çalıştırılmadan önce antivirüs yazılımı tarafından taranmalıdır.

5.9. Virüs bulaşma ihtimaline karşı kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile Ağ ve Sistem Hizmetleri Şubesi çalışanları tarafından BLG-PRD-XXX Yedekleme Prosedüründe belirtilen zaman ve usullere göre yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır.

5.10. Bu politika ve bağlantılı diğer politika, yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde Üniversite idari/sözleşmeli personel için 4857 sayılı İş Kanunu, 657 sayılı Devlet Memurları Kanunu ile Devlet Memurları Disiplin Yönetmeliği, akademik personel için 2547 Sayılı Yükseköğretim Kanunu, öğrenciler için Yükseköğretim Kurumları Öğrenci Disiplin Yönetmeliği işletilmektedir. Misafir kullanıcılar için 5651 sayılı yasa, 7545 sayılı kanun ve TCK

6. İLGİLİ DOKÜMANLAR

6.1. KYT-PRD-01 Dokümanların Kontrolü Prosedürü

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

6.3. BLG-FRM-XXX Ağ ve Sistem Talep Formu

6.4. BLG-PRD-XXX Yedekleme Prosedürü