1.AMAÇ

Bu politika, Hakkari Üniversitesinin sahip olduğu bilgisayar ağına uzaktan erişim standartlarının tanımlanması ve uzaktan erişim işleminden kaynaklanabilecek güvenlik açıklarının engellenmesi amacıyla hazırlanmıştır.

2.KAPSAM

Bilgi İşlem Daire Başkanlığı TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi kapsamında uzak erişim sağlayabilen tüm cihazlar/sistemleri, tüm akademik ve idari personeli ve dış paydaşları 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.Ağ: İki veya daha fazla cihazın (bilgisayar, sunucu, yazıcı, vb.) birbirleriyle veri alışverişi yapabilmesi için oluşturulan bağlantılar bütünüdür.

3.9.VPN: Uzaktan erişim yoluyla farklı ağlara bağlanmayı sağlayan bir internet teknolojisidir. VPN, sanal bir ağ uzantısı oluşturarak, ağa bağlanan cihazların fiziksel olarak bağlıymış gibi veri alışverişinde bulunmasına olanak tanır.

3.10.Tedarikçi: Başka bir kuruluşa mal, hizmet veya malzeme sağlayan bir birey veya kuruluştur.

3.11.IpSec: Internet Protokolü (IP) kullanılarak sağlanan iletişimlerde her paket için doğrulama ve şifreleme kullanarak koruma sağlayan bir protokol paketidir.

3.12.IpSec VPN: İnternet üzerinden güvenli ve şifreli bir tünel kurmak için IPsec protokolünü kullanan bir VPN türüdür.

3.13.SSL VPN: SSL veya TLS protokolleri üzerinden güvenli erişim sağlayan sanal özel ağ teknolojisidir.

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, politika 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 gerçekleştirilmesinden sorumludur.

5.UYGULAMA

5.1.İnternet üzerinden Üniversitenin herhangi bir yerindeki bilgisayar ağına erişim gerekli ise erişen kişi veya kuruluşlar, VPN teknolojisini kullanacaklardır. VPN teknolojileri IpSec VPN,SSL VPN vb. protokollerinden

birini içermelidir.

5.2. Bilgi İşlem Daire Başkanı tarafından onay verilen kullanıcılar VPN kullanabilir. VPN erişimi isteyen Üniversite personeli HUBİS üzerinden BLG-FRM-XXX Ağ ve Sistem Talep Formu doldurup taleplerini bildirmelidirler. Mevcut bilgi sistemlerinin tedarik edildiği firmaların uzaktan erişim talepleri bilgiislem@hakkari.edu.tr e-postası üzerinden yapılır.

5.3. Üniversite personelleri ve anlaşmalı tedarikçi firma çalışanları kendilerine tahsis edilen uzaktan bağlantı kaynak ve hizmetleri "BLG-POL-XXX İnternet Erişim ve Kullanım Politikası" çerçevesinde kullanmalıdır.

5.4. VPN kullanımı gerçekleştiren kullanıcılar **BLG-PRD-XXX Kullanıcı Hesap Yönetimi ve Erişim Yetkilendirme Prosedürü** gereklilikleri doğrultusunda, erişim kontrolleri Ağ ve Sistem Hizmetleri Şubesi tarafından takip edilmelidir. Periyodik olarak yapılan kontrollerle veya görev değişikliği/işten ayrılma bildirimi Bilgi İşlem Daire Başkanlığına iletildiğinde Üniversiteden ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

5.5. Uzak bağlantı yapan kullanıcı bilgisayarlarında **BLG-POL-04 Antivirüs Politikası** gereğince antivirüs yazılımları kurulu ve güncel olmalıdır.

5.6. Uzaktan erişim gerçekleştiren tedarikçiler Üniversitenin bilgisinin ekran çıktısını alamaz, transfer edemez ve Üniversite dışına çıkartamaz. Aksi taktirde oluşacak risklerde yasal yükümlülüklerden sorumlu olacaktır.

5.7. Bilgi İşlem Daire Başkanlığı tarafından üçüncü taraflara verilecek erişimler için **gizlilik anlaşması** yapılacaktır.

5.8. Uzak bağlantı yapan kullanıcı, parolalarını aile bireyleri dahil olmak üzere hiç kimseye vermemelidir.

5.9. Politika ihlali sonucunda tabi olunan yasa ve mevzuatlar çerçevesinde disiplin kuralları uygulanabilir.

6. İLGİLİ DOKÜMANLAR

6.1. KYT-PRD-01 Dokümanların Kontrolü Prosedürü

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

6.3. BLG-POL-XXX İnternet Erişim ve Kullanım Politikası

6.4. BLG-PRD-XXX Kullanıcı Hesap Yönetimi ve Erişim Yetkilendirme Prosedürü

6.5.BLG-POL-04 Antivirüs Politikası