

 OSTİM TEKNİK ÜNİVERSİTESİ A N K A R A	VPN KULLANIMI VE UZAKTAN ÇALIŞMA POLİTİKASI	Doküman No	BS.PO.003
		Revizyon Tarihi	07.11.2024
		Revizyon No	01
		Sayfa No	1 / 3

1. AMAÇ

Bu politikanın amacı VPN (sanal özel ağ) protokolünün kullanımı hakkında standartları belirlemektir.

2. KAPSAM

Bu politika VPN ile kurum ağına bağlanacak kurumla, çalışanlarını, sözleşmelileri, danışmanları, geçici çalışanları ve diğer bütün personeli kapsar.

3. TANIMLAR VE KISALTMALAR

- BYDB:** Bilgi Yönetimi Daire Başkanlığı. Bilginin gizliliğini, bütünlüğünü ve kesintisiz kullanılabilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümente edilmiş, yönetimce kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünü.

4. GÖZDEN GEÇİRME

Senede en az bir defa ve ihtiyaç halinde (büyük değişiklikler veya önemli güvenlik olayları olduğunda) BYDB ile gözden geçirilip varsa değişiklikler onaya sunulur.

5. SORUMLULUKLARI

Bu dokümanın hazırlanması, düzenlenmesi ve yayınlanması BYDB sorumluluğundadır. BYDB Başkanı tarafından kontrol edilerek üst yönetim adına onaylanır.

6. UYGULAMA

VPN Kullanımı

- VPN kullanım hakkı verilen kişiler VPN hakkını hiç kimseye kullandıramaz.
- VPN konfigürasyonu mümkünse tek yönlü şifreleme (one-time password authentication, örnek; token device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi ile yapılmalıdır.
- Kurum ağına bağlanıldığında, bilgisayardan çıkan ve bilgisayara giren trafik sadece VPN kanalından iletilir.
- Çift tünel (split tunnel - aynı anda iki VPN bağlantısı) sistemine izin verilmemektedir; sadece bir ağ bağlantısına izin verilir.

 OSTİM TEKNİK ÜNİVERSİTESİ A N K A R A	VPN KULLANIMI VE UZAKTAN ÇALIŞMA POLİTİKASI	Doküman No	BS.PO.003
		Revizyon Tarihi	07.11.2024
		Revizyon No	01
		Sayfa No	2 / 3

- Kurumun VPN ağ geçitlerinin kurulması ve yönetimi yetkili Bilgi İşlem personeli tarafından yapılır.
- Kullanıcı VPN bağlantıları 120 dakika kullanılmadığı takdirde bağlantıları otomatik olarak kesilir. Kullanıcı tekrar bağlanmak için log-on olmak zorundadır.
- Ping veya diğer ağ komutları bağlantıyı açık tutmak için kullanılamaz.
- Kuruma ait olmayan bilgisayarlara sahip kişiler, kurumun VPN ve ağ politikalarına uygun bir şekilde cihazlarını konfigure etmek zorundadır.
- Periyodik olarak yapılan kontrollerle kurumdan ilişkisi kesilmiş veya görevi değişmiş kullanıcıların VPN hakları kaldırılır.
- Uzak masaüstü bağlantısı VPN üzerinden yapılır. VPN üzerinden yapılan uzak masaüstü bağlantılarda aşağıdaki kurallar geçerlidir:

- ✓ Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.
- ✓ Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişilere Bilgi Güvenliği Şube Müdürlüğü'nden sorumlu Daire Başkan Yardımcısı izni ile geçici izin verilir.

Uzaktan Çalışma / Erişim Uzak Masaüstü Bağlantıları

- Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.
- ISDN veya telefon hatları ile uzaktan erişen yönlendiriciler minimum olarak CHAP kimlik doğrulama protokolünü kullanmalıdırlar.
- Uzaktan erişim yöntemi ile kuruma erişen bütün bilgisayarlar en son güncellenmiş anti virüs yazılımına sahip olmalıdırlar.
- Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişilere Bilgi Güvenliği Şube Müdürlüğü'nden sorumlu Daire Başkan Yardımcısı'nın özel izni ile geçici olarak izin verilebilir.

 OSTİM TEKNİK ÜNİVERSİTESİ A N K A R A	VPN KULLANIMI VE UZAKTAN ÇALIŞMA POLİTİKASI	Doküman No	BS.PO.003
		Revizyon Tarihi	07.11.2024
		Revizyon No	01
		Sayfa No	3 / 3

- Periyodik olarak yapılan kontrollerle kurumdan ilişkisi kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılır.

9. REVİZYON GEÇMİŞİ

Revizyon No	Tarih	Açıklama
01	07.11.2024	Entegre Kalite Yönetim Sisteminde kalite yönetiminde zorluklar ile karşılaşılması sebebiyle ISO 9001 Kalite Yönetim Sistemi (KYS) ve ISO 27001 Bilgi Güvenliği Yönetim Sisteminin (BGYS) ve dokümanlarının ayrılması ve ayrı ayrı takip edilmeleri kabul edilmiştir. Bu sebeple doküman kodlamalarında revizyon yapılmıştır.

Hazırlayan	Kontrol Eden	Onaylayan
İlknur ALŞAHİN Kalite Birimi	Kenan IŞIK Kalite Koordinatörü	Prof.Dr. Murat Ali YÜLEK Rektör
E-imzalıdır/paraflıdır	E-imzalıdır	E-imzalıdır