	SANAL ÖZEL AĞ (VPN) POLİTİKASI		
Doküman No: PLT.17	**Yayın Tarihi:** 25.04.2022	**Revizyon Tarihi:** -	**Revizyon No:** -

1. AMAÇ

Bu politikanın amacı Muğla Sıtkı Koçman Üniversitesi'nin VPN protokolünün kullanımı hakkındaki standartları belirlemektir.

2. KAPSAM

Bu politika kurumun bütün çalışanlarını, sözleşmelileri veya tedarikçileri ve kısaca kurumun herhangi bir birimindeki bilgisayar ağına uzaktan veya yakından erişen bütün kişi ve kurumları kapsamaktadır.

3. KISALTMALAR

Bu prosedürde geçen;

3.1. **MSKÜ:** Muğla Sıtkı Koçman Üniversitesi'ni

3.2. **VPN:** Virtual Private Network (Sanal Özel Ağ)'ü

ifade eder.

4. TANIMLAR

4.1. **VPN:** Farklı bir noktadaki başka bir ağdan internete bağlanmayı sağlayan sistemdir.

5. SORUMLULUKLAR

Bu politika ile ilgili gereklerin uygulanmasından üniversite ağından dahili veya harici olarak yararlanan tüm kullanıcılar sorumludur.

6. UYGULAMA

a) Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.

b) İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdır. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamalıdır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vb. protokollerinden birini içermelidir.

c) Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one-time password authentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/private key sistemi kullanılması tavsiye edilmelidir. Daha fazlası için şifre politikasına bakınız.

d) Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

e) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

Hazırlayan Bilgi Güvenliği Ekibi	Kontrol Eden Bilgi İşlem Daire Başkanlığı	Onaylayan Rektör Yardımcısı

f) Taşınabilir cihazlarda VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.
g) Kurum bilgisayarları haricinde VPN bağlantısı yapılacak cihazlarda anti-virüs yazılımları kurulu ve güncel olmak zorundadır.
h) Sadece kurumun onay verdiği kullanıcılar VPN'i kullanabilir.
i) VPN kullanım hakkı verilen kişiler listelenmeli ve en az yılda bir kez kontrol edilmelidir.
j) Kurum gerekli gördüğü durumlarda herhangi bir uyarıda bulunmadan VPN bağlantı erişimlerini kesme hakkına sahiptir.

6.1. Yaptırım

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri, tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

7. İLGİLİ DOKÜMANLAR

-