P08 UZAKTAN ERİŞİM POLİTİKASI

1.1 Amaç

Bu politikanın amacı herhangi bir yerden kurum çalışanlarının veya tedarikçilerin kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları minimize etmek için tasarlanmıştır. Bu zararlar şunlardır; Kurumun gizli ve hassas bilgilerinin kaybı, prestij kaybı ve içerideki kritik sistemlerde meydana gelen zararlar vb.

1.2 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.

Bütün uzaktan erişim uygulamaları bu politika tarafından kapsanmaktadır.

1.3 Politika

Uzaktan erişim politikası aşağıdaki gibidir.

1.4 Genel

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

b) Uzaktan erişim metotları ile kuruma bağlantılarda bilgi sistemlerinin güvenliğinin sağlanması için aşağıdaki politikalara göz atmak gerekmektedir.

Şifre Politikası
Sanal Özel Ağ (VPN) Politikası

1.4.1 Gereklilikler

a) İnternet üzerinden kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. Bu, veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec VPN, L2TP, SSL VPN, PPTP vb. protokollerinden birini içermelidir.

b) Mümkünse uzaktan erişim güvenliği bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one time password authentication) veya güçlü bir passphrase (uzun şifre) destekli public /private key sistemi kullanılması tavsiye edilmektedir. Daha fazla bilgi için P06 Şifre politikasına bakınız.

c) Uzaktan erişim gerçekleştiren kullanıcıların veya tedarikçilerin erişim şifreleri en yılda bir değiştirilecektir. Verilen şifreler kurumun şifreleme politikasına uygun olmalıdır.

ç) Uzaktan erişim gerçekleştiren tedarikçiler kurumun bilgisinin ekran çıktısını alamaz, transfer edemez ve kurum dışına çıkartamaz. Aksi taktirde oluşacak yasal yükümlülüklerden sorumlu olacaktır.

d) Kurum çalışanları hiçbir şekilde kendilerinin login (bağlantı) ve e-posta şifrelerini aile bireyleri dâhil olmak üzere hiç kimseye vermemelidirler.

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

f) Çalışanlar kurum ile ilgili çalışmalarında kurumun dışındaki e-posta hesaplarını kullanmamalıdırlar.

g) Uzaktan bağlananlar makinesinde zararlı kod, truva atı vs. olduğundan şüpheleniyorsa bağlantıyı gerçekleştirmemelidir.

ğ) Kurum ağına erişecek tüm kullanıcı ve kurumlar ile gizlilik sözleşmesi yapılmış olmalıdır.

h) Periyodik olarak yapılan kontrollerle veya görev değişikliği/işten ayrılma bildirimi Bilgi İşlem Daire Başkanlığına iletildiğinde kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları buna göre düzenlenmelidir.

ı) Kurum, uzaktan erişim verdiği kullanıcı veya kurumlarda alması gereken güvenlik tedbirlerinde herhangi bir aksaklık gördüğünde uzaktan erişim bağlantısını eksiklik düzelinceye kadar kesme hakkına sahiptir.

i) Kurum güvenli erişimin sağlanabilmesi için gerekli gördüğü takdirde kullanıcının veya kurumun sadece belli zaman aralıklarında veya istek yapılan durumda uzaktan erişimine izin verebilir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVANI	BGYS YÖNETİM TEMSİLCİSİ (DAİRE BAŞKANI)	GENEL SEKRETER
ADI SOYADI	Dr. Naci BAYRAK	Prof.Dr. Ahmet DUMLU
İMZA		