Revizyon İzleme Tablosu		
Rev. No	**Rev. Tarihi**	**Açıklama**
01	06.03.2023	Cumhurbaşkanlığı Bilgi Güvenliği Rehberi Uyum çalışmaları kapsamında değişikliğe gidilmiştir.

1. AMAÇ

Bu politikanın amacı herhangi bir yerden Kurumun bilgisayar ağına erişilmesine ilişkin standartları belirlemektir. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı Kuruma gelebilecek potansiyel zararları minimize etmek için tasarlanmıştır.

2. SORUMLULUKLAR

Bu politika kurumun sağlamış olduğu hizmetlere erişen, kullanan veya destek veren kişi, kurum ve kuruluşları kapsamaktadır.

Bu politika, Kuruma bağlı bütün uzak erişim bağlantılarını kapsamaktadır ve bunun içerisine e-posta okuma veya gönderme ve intranet web kaynaklarını gözlemleme dahildir. Bütün uzaktan erişim uygulamaları bu politika tarafından kapsanmaktadır.

3. UYGULAMA

3.1 Genel

- Uzaktan erişim için yetkilendirilmiş Kurum çalışanları veya Kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.
- Uzaktan erişim metotları ile Kuruma bağlantılarda bilgi sistemlerinin güvenliğinin sağlanması için aşağıdaki politikalara göz atmak gerekmektedir.

- Şifre Güvenliği Politikası
- Taşınabilir Cihaz Politikası

3.2 Gereklilikler

- İnternet ortamından kurum içi kaynaklara kontrol dışı erişim engellenmelidir.
- İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişim gerekli ise erişen kişi veya Kurumlar VPN teknolojisini kullanacaklardır. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec protokolünü içermelidir.
- Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifrelemede (one time password authentication) veya güçlü bir passpharase (uzun şifre) destekli public /private key sistemi kullanılması tavsiye edilmektedir. Sertifika kullanılmalıdır.
- Uzaktan çalışma kapsamında kurum kaynaklarına erişim VPN teknolojileri ile sağlanmalıdır.
- Kurum çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.
- 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.
- Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahiplerine noktadan noktaya bağlantı izinleri sağlanmalıdır.
- Çalışanlar Kurum ile ilgili çalışmalarında Kurumun dışındaki e-posta hesaplarını kullanamazlar.
- Uzaktaki kullanıcı, cihazını split -tunnel veya dual homing (VPN bağlantısı esnasında başka bir bağlantı daha yapmak) olarak konfigüre edemez.

- Kurum ağına standart dışı erişim isteğinde bulunan üçüncü taraflar veya kişiler kurumun özel izni ile geçici olarak izin verilebilir.
- Uzaktan erişimlerin kısıtlı süre ve yetkilerle yapılması sağlanmalıdır. Uzaktan erişim yetkileri firmalarla yapılan gizlilik sözleşmesi ile belirlenmelidir.
- Periyodik olarak yapılan kontrollerle Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.