1. Amaç

Bu politikanın amacı, kurumun bilgi teknolojileri sistemlerine dışarıdan yapılacak olan uzak bağlantıların, özellikle VPN ve Uzak Masaüstü Bağlantısı (RDP) gibi yöntemlerin güvenliğini sağlamaktır. İzinsiz erişim, veri kaybı ve güvenlik açıklarına karşı koruma sağlanması amaçlanmaktadır.

2. Kapsam

Bu politika, bilgi teknolojileri sistemlerine dışarıdan bağlantı yapacak tüm kurum çalışanlarını, tedarikçileri ve diğer paydaşları kapsamaktadır. Kurumun tüm bilgisayar sistemleri, sunucuları ve ağ bileşenleri bu politikaya tabidir.

3. Politika

3.1. Bağlantı Yöntemleri

- Uzak bağlantı, kurum personeli için yalnızca SSL VPN üzerinden yapılmaktadır. Tedarikçi firmaların erişimleri için belirlenen IP adreslerine özel izin verilmektedir.

3.2. Uzak Masaüstü Bağlantısı (RDP)

- Uzak Masaüstü Bağlantısı (Remote Desktop Protocol - RDP), yalnızca kurum tarafından yetkilendirilmiş kişiler tarafından kullanılabilir. RDP erişimi, VPN üzerinden güvence altına alınmalıdır ve doğrudan dış ağdan erişim yapılmasına izin verilmemelidir.
- RDP erişimi sağlanan bilgisayarlarda güçlü bir şifre kullanımı zorunludur ve RDP oturumları belirlenen sürelerde gözden geçirilerek izlenmelidir.
- Çok faktörlü kimlik doğrulama (MFA), RDP bağlantılarında uygulanmalıdır. Bu, güvenlik risklerini azaltmak amacıyla yapılacak bir önlemdir.
- RDP kullanarak bağlanılacak cihazlar için anti-virüs yazılımı kurulu olmalı ve düzenli olarak güncellenmelidir.

3.3. Erişim Talebi ve Onay Süreci

Kurum dışından bağlantı talebinde bulunacak paydaşlar, e-posta yoluyla talepte bulunmalıdır. Erişim talebi Bilgi İşlem Daire Başkanlığı tarafından onaylandıktan sonra bağlantı sağlanacaktır.

3.4. Kullanıcı Yetkilendirme ve Kontrol

- VPN ve RDP kullanım yetkisi verilen tüm personel ve paydaşlar düzenli olarak listelenecek ve bu liste Bilgi İşlem Daire Başkanlığı tarafından denetlenecektir. Yetkilendirilmiş kullanıcıların bağlantı hakları periyodik olarak gözden geçirilecektir.
- VPN ve RDP kullanım hakkı verilen kişiler, kullanıcı adı ve şifre bilgilerini başkalarıyla paylaşmamalıdır. Bu tür bir paylaşım güvenlik ihlali olarak kabul edilecek ve gerekli yaptırımlar uygulanacaktır.

3.5. Bağlantı Cihazları

Kurum bilgisayarları haricindeki cihazlardan VPN veya RDP bağlantısı yapılacaksa, bu cihazlarda güncel anti-virüs yazılımı kurulu olmalı ve sürekli aktif halde olmalıdır. Virüs veya zararlı yazılımlar açısından cihazlar düzenli olarak taranmalıdır.

3.6. Erişim Kısıtlama Yetkisi

Kurum, güvenlik ve politika ihlalleri veya olağanüstü durumlarda herhangi bir bildirimde bulunmadan VPN ve RDP bağlantı erişimlerini kesme hakkına sahiptir. Bu durum acil durum yönetimi ve veri güvenliği açısından önem taşımaktadır.

4. Sorumluluklar

- VPN ve RDP erişimi verilen kişiler, bu politikanın kurallarına uymakla yükümlüdür. Yetkilerini aşan veya güvenlik riskine yol açacak herhangi bir işlem yapmaları durumunda sorumlu tutulacaklardır.
- Bilgi İşlem Daire Başkanlığı, VPN ve RDP bağlantılarını izlemek, denetlemek ve bu politikanın uygulanmasını sağlamakla sorumludur.