ERİŞİM KONTROL PROSEDÜRÜ

T.C. SAĞLIK BAKANLIĞI
ÇORUM
İL SAĞLIK MÜDÜRLÜĞÜ

1. Kurum sunucularına erişim için SSL VPN kullanılmalıdır.
2. SSL VPN ile bağlantı verilen kullanıcılar sadece yetkisi olduğu sunuculara erişecek şekilde erişim kısıtlaması yapılmalıdır.
3. SSL VPN gerçekleştirecek kullanıcılara(firma ve kurum personeli) mutlaka kurumsal gizlilik sözleşmesi imzalatılmalıdır. Eğer firmanın Kurumsal gizlilik sözleşmesi yok ise ilgili firma ile kurumsal gizlilik sözleşmesi de imzalanır.
4. SSL VPN gerçekleştirecek kullanıcılar(firma personeli) mutlaka Kurumsal SSL VPN Erişim Talep Formunu imzalamalıdır.
5. SSL VPN gerçekleştirecek kullanıcılar(kurum personeli) mutlaka Personel SSL VPN Erişim Talep Formunu imzalamalıdır.
6. Kullanıcılara Sunucu yönetimi için sadece ihtiyaç duyulan portlara erişim yetkisi verilmelidir. Yetkili kullanıcıların erişimi için TELNET yerine SSH ve RDP gibi şifreli protokoller kullanılmalıdır.
7. Kullanıcılara sadece yetkisi olduğu sunucularda erişim yetkisi verilmelidir.
8. Sunucuların kendi aralarında servis ve yönetimleri için belirli portlarla erişim sağlanması gerekmektedir.
9. Kullanıcıların sunucu yönetim için sağlanan erişimde admin/root yetkisi sistem grubu dışında verilmemelidir.
10. Kullanıcıların sunucu yönetim için sağlanan erişimde merkezi kullanıcı yönetimi (MS AD, LDAP, sshkey) ile yapılmalıdır.
11. Kullanıcıların sunucu yönetim için sağlanan erişimde kısıtlı erişim yetkileri tanımlanmalıdır.
12. Dış dünyadan sunucular üzerindeki servislere erişim için 80, 443, 7001, 8080, 8443 gibi servis portları da özel durumlarda verilmelidir.
13. Sunucu servislerinin yönetim işlemlerinde yetkili kullanıcı bilgileri, Bilgi İşlem Birimine teslim edilmelidir. Bilgi İşlem Birimi nezaretinde ve tarafından yürütülmelidir.
14. Kurumun yedekleme sistemlerine sadece kurum personeli erişim yapmalıdır. Firmaların yapacakları tüm işlemler Bilgi İşlem Birimi nezaretinde yürütülmelidir.
15. Ağ cihazlarının şifreleri default şifrelerde bırakılmamalı ve kompleks şifreler(parola güvenliği ilkelerine uygun olarak) kullanılmalıdır.
16. Kullanıcı bilgisayarlarına uzak bağlantıda kullanılan uygulamalarda (Netsupport, anydesk, radmin vb. programlarda) Bağlantı sağlanacak kullanıcının onayı ile bağlantı sağlanmalıdır. Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.
17. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeler yapılmış olmalıdır.
18. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

Hazırlayan	Kontrol Eden	Onaylayan
Samet ŞENSOY Bilgi Güvenliği Yetkilisi	Ahmet Bahadır ÜNLÜ Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Uzm. Dr. Ömer SOBACI İl Sağlık Müdürü