1. AMAÇ

Uzaktan Erişim Prosedürü'nün amacı, KU mensuplarının, sistem yöneticilerinin ve destek hizmeti alınan dış kaynakların uzaktan bilgiye ve sistemlere erişimi için geçerli olan minimum güvenlik standartlarını tanımlamaktır.

2. KAPSAM

KU Uzaktan Erişim Prosedürü, tüm KU sistemlerini ve bu sistemlere erişimi olan KU mensupları ve destek hizmeti alınan tüm dış kaynakları kapsamaktadır.

3. REFERANSLAR

3.1 KU Kullanıcı Erişim Yönetimi, Yetkilendirme ve Hesap Yönetimi Prosedürü

3.2 YÖK Öğrenci Disiplin Yönetmeliği

3.3 Koç Üniversitesi İdari Personel Yönetmeliği

3.4 COBIT.2019 kapsamında "Süreç, Organizasyonel Yapılar, Bilgi Akışları ve Varlıkları, İnsanlar, Beceriler ve Etkinlikler, Politikalar ve Prosedürler, Kültür, Etik ve Davranış, Hizmetler, Altyapı ve Uygulamalar" yönetişim bileşenlerinin ilgili yönetişim ve yönetim hedefine uygulanabilecek her biri.

3.5 ISO 27000:2018 Bilgi Güvenliği yönetim standartları ailesi tamamı.

3.6 SANS-CIS kontrolleri (En yaygın ve tehlikeli saldırıları durdurmak için belirli ve uygulanabilir yollar sağlayan, siber güvenlik eylemler dizisidir.)

3.7 5651: İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

3.8 6698: Kişisel Verilerin Korunması Kanunu

3.9 4857: İş Kanunu

3.10 2547: YÖK Kanunu

4. SORUMLULUKLAR

4.1 Prosedürün uygulatılmasından Rektörlük sorumludur.

4.2 Prosedürün yayına hazırlanmasından, iyileştirme takibinin yapılmasından ve uzaktan erişim standartlarının uygulandığının kontrol edilmesinden Bilgi Teknolojileri Direktörlüğü sorumludur.

4.3 Güvenlik politikalarını, yöntemlerini belirlemekten ve değerlendirmekten, Bilgi Güvenliği konusundaki özel durumların değerlendirilmesi ve uygulama esaslarının belirlenmesinden Bilgi Güvenliği Komitesi sorumludur.

5. TANIMLAR

5.1 **KU mensupları:** İdari çalışanlar, akademik çalışanlar, öğrenciler, mezunlar

5.2 **Trackit:** BT Talep yönetim sistemi

5.3 **Destek Hizmeti:** Üniversite'nin dışarıdan temin ettiği, güvenliğini, sürekliliğini etkileyen ve veri erişimi ya da veri paylaşımı olan hizmet alımları

5.4 **Dış Kaynak:** Üniversite'nin ihtiyaçları doğrultusunda ilgili konularda uzmanlarından hizmet alınması

5.5 **Yetkili Kullanıcı:** Bağlı olduğu bilgisayar kaynaklarına ve içinde bulunduğu ağ kaynaklarına erişebilen; kullanıcı oluşturma/silme, uygulama yükleme, veritabanı yönetimi vb. haklara sahip kişi

6. TEMEL PRENSİPLER

6.1 Bu prosedür ve bağlantılı diğer yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde KU İdari personeli için 4857 Sayılı İş Kanunu ve Koç Üniversitesi İdari

Personel Yönetmeliği, KU Akademik personel için 2547 Sayılı YÖK Kanunu, öğrenciler için YÖK Öğrenci Disiplin Yönetmeliği işletilir.

6.2 Uzaktan erişim yetkisi, asgari yetki prensibiyle yalnızca ihtiyaç duyan sınırlı sayıdaki çalışana ve ihtiyaç duyulan kaynaklara sağlanır.

6.3 Uzaktan erişim yetkisi atanacak kişilerin, erişimden önce bu konudaki güvenlik iyi uygulamaları hakkında Bilgi Güvenliği Yönergesi ve Kabul Edilebilir Kullanım Yönergesi (iç yönergeler) üzerinden haberdar olmaları sağlanır. Erişim yapacak dış kaynakların KU ile NDA imzalamış olması beklenir.

6.4 Uzaktan erişim için tanımlanacak tüm kullanıcı hesapları, yetkiler ve parolalar üniversite politikalarına uyumlu bir şekilde yönetilir. (KU Kullanıcı Erişim Yönetimi, Yetkilendirme ve Hesap Yönetimi Prosedürü)

6.5 Uzaktan erişim, çift faktörlü bir kimlik doğrulama sonucunda gerçekleşir. Kullanıcı adı ve parolaya ek olarak çift faktörlü erişim metotlarından bir veya birkaç tanesi kullanılabilir. (Ör: SMS OTP, Yazılım OTP, Donanım OTP, Soft token, IP kısıtlaması)

6.6 Uzaktan erişimler güvenli bir algoritma kullanan kriptolu bir tünel bağlantısı (SSL VPN) aracılığıyla gerçekleştirilir.

6.7 Tüm uzaktan erişim işlemleri için oturum kayıtları (log) tutulur ve 2 yıl saklanır. Bu kayıtlarda aşağıdaki bilgiler tutulur;

6.7.1 Oturum açma (Login)

6.7.2 Oturum kapama (Logout)

6.8 Yetkili dış kaynak erişimlerinde ek olarak aşağıdaki loglar tutulur.

6.8.1 Erişilen sistem

6.8.2 Yapılan işlemlerin görüntüleri veya sisteme verilen komutlar

6.9 Uzaktan erişim üzerinde oturum kontrolü bulunur. Aynı anda bir kullanıcı hesabıyla iki farklı bağlantıya izin verilmez.

6.10 1 saat inaktif olarak kalan kullanıcı oturumları kapatılır, tekrar kullanıcı adı ve parola girilmesi istenir.

6.11 Yetkili kullanıcıların uzaktan erişim için kullandığı bilgisayarlarda iz kalması engellenir, bu amaçla çerez ve sayfa önbellek ayarları kullanıcı oturumunun veya kritik bilgilerin çalınmasını ve taklit edilmesini engelleyecek şekilde yapılandırılır.

6.12 Uzaktan erişim gerçekleştirilen kullanıcı cihazlarında güvenlik kontrolleri (yama, antivirus yazılımı vb.) uygulanmaktadır ve sadece gereksinimleri karşılayan cihazlar ağa dahil edilmektedir.

6.13 Tanım dışı durumlar Bilgi Güvenliği Komitesi tarafından değerlendirilmektedir.

7. YÖNTEM

7.1 Uzaktan Erişim Yetkisinin Tanımlanması

7.1.1 Uzaktan erişim yetkisinin atanması “talep”, “onay” adımlarını içeren bir yetkilendirme süreci ile Trackit üzerinden gerçekleşir ve kayıt altında tutulur.

7.1.2 Dış kaynak uzaktan erişimleri, üniversite içinde dış kaynaktan hizmet alan proje yöneticisi onayıyla talep edilir.

7.1.3 Uzaktan erişimler iki faktörlü doğrulama ile gerçekleştirilir.

7.1.4 Dış kaynaklara atanan uzaktan erişim yetkileri zaman kısıtlı olarak verilir.
Proje bazlı çalışan dış kaynaklara KU Kullanıcı Erişim Yönetimi, Yetkilendirme ve Hesap Yönetimi Prosedürü’nde belirtilen sürelere göre hesap açılır, kullanıcı listesi üç ayda bir gözden geçirilir. Destek hizmeti alınan kullanıcılar için maksimum süre yıllık bakım hizmet anlaşması süresiyle sınırlandırılır. Süre bitiminde otomatik olarak kapatılır, tekrar erişim gereği varsa talep süreci yeniden işletilir.

7.1.5 Üniversite çalışanının / dış kaynaklı projedeki çalışanın işten ayrılması veya dış kaynaklı projenin tamamlanması ile birlikte uzaktan erişim yetkisi kapatılır.

7.1.6 Uzaktan erişim yetkilerinin gözden geçirilmesine dair kanıtlar 24 ay saklanır.

7.1.7 Uzaktan erişim yetkileri sadece ihtiyaç duyulan uygulamalar ile kısıtlanır.

7.2 Uzaktan Erişimin Standartları

7.2.1 Üniversite sistemine sadece KU NetID kullanıcı adı ve parolası ile Kurumsal VPN uygulaması aracılığıyla uzaktan erişim gerçekleştirilir.

7.2.2 Bağlantı detayları (SSH, Telnet, RDP, ağ'a direkt erişim) talebe göre trackit üzerinden değiştirilir.

7.2.3 BT Dış kaynakları VPN bağlantısı sonrası CIS Remote aracılığıyla sistemlere erişim sağlar. CIS Remote üzerinden sağlanan erişimler video kayıt altına alınır. Bu kayıtlar 1 yıl tutulur.

7.2.4 Sunuculara bağlantı sonrasında ObserveIT ile sadece izin verilen komutlar çalıştırılabilir ve bu komutlar kaydedilir. Bu kayıtlar 1 yıl tutulur.

7.2.5 SSL VPN Erişim Standartları

7.2.5.1 SSLVPN kimlik doğrulama işlemleri, tek kullanımlık parola ya da public/private key kullanımını içerecek şekilde çift yönlü olarak yapılır.

7.2.5.2 Üniversiteye yapılan SSLVPN bağlantılarında, kullanıcıların kurumsal erişimi ve diğer internet trafiği vpn tünel üzerine yönlendirilir. Kullanıcıların internet yönüne erişimleri drop edilir.

7.2.5.3 Yalnızca kütüphaneye ait elektronik veritabalarına ulaşılması için split tünellemeye izin verilmektedir.

7.2.5.4 SSLVPN kullanıcıları bir saatlik inaktif süre sonunda, otomatik olarak disconnect edilir.

7.2.5.5 SSLVPN erişimleri için bağlantı süresi sınırlanır. Bu sürenin sonunda, kullanıcı tekrar giriş yapılmaya zorlanır.

7.2.5.6 SSLVPN erişim hizmeti alan tüm kullanıcı bilgisayarları, Üniversite'nin belirlediği güvenlik standartlarını sağlar.

7.2.5.7 Üniversite ağına yapılan tüm SSLVPN erişimleri loglanır ve loglar güvenli bir yerde en az bir yıl süre ile saklanır.

7.2.5.8 SSLVPN erişimini sağlayan yazılımda son sürüm yerine, üreticiden çalışırlığı ile ilgili onay alınan sürüm tercih edilir.

7.2.5.9 Kullanıcıların aynı anda birden fazla oturum açmasına izin verilmez.

7.2.6 IPSEC VPN Erişim Standartları

7.2.6.1 IPSEC VPN bağlantılarında FIPS onaylı şifreleme algoritmaları kullanılır. 256 bit AES ya da 3DES algoritması tercih edilir. DES algoritması zafiyetler barındırdığından kullanılmaz.

7.2.6.2 Bütünlük koruma algoritması olarak SHA-1 tercih edilir.

7.2.6.3 Güçlü pre-shared key kullanılır. Pre shared key en az 10 karakter olur ve rastgele karakterlerden oluşur. Pre-shared key bilgisi, e-posta üzerinden paylaşılmaz.

7.2.6.4 IKE faz 1'de aggresive mod yerine main mod kullanılır.

7.2.6.5 IKEv1, Security Associations (SA) 86400 (24 saat) saniyeden fazla, IPSEC SA 28800 (8 saat) saniyeden fazla tanımlanır.

7.2.6.6 IPSec VPN erişimini sağlayan yazılımda son versiyon yerine, üreticiden çalışırlığı ile ilgili onay alınan yazılım versiyonu tercih edilir.

7.2.7 Bakım ve Yapılandırma Standartları

7.2.7.1 Uzaktan erişim için oluşturulan altyapılar düzenli olarak sızma testlerine tabi tutulur.

7.2.7.2 Uzaktan erişim için kullanılan altyapıların yamaları SOC istihbarat servisi ile sürekli takip edilir ve önemli güvenlik yamaları acil olarak yüklenir.

7.2.7.3 Uzaktan erişim altyapısı merkezi olarak yönetilir.

7.2.7.4 Uzaktan erişimi düzenleyen sistemler üzerindeki admin faaliyetleri, kullanıcı kayıt değişiklikleri ve parola değiştirme işlemleri loglanır ve 1 yıl süreyle saklanır.

7.2.7.5 Uzaktan erişim sunucuları yedeklenir ve bu sistemlerin acil durumlarda çalışır durumda olmasını sağlayacak “high availability” ve “replication” yöntemleri kullanılır.

8. EKLER ve KAYITLAR

Yoktur.

9. GÖZDEN GEÇİRME

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu Bilgi Teknolojileri Direktörlüğü aittir. Gözden geçirme en az yılda 1 defa yapılır. Gerekli görüldüğü zaman ve durumlarda prosedürün de revize edilmesi gereklidir.

10. DEĞİŞİKLİK/ DAĞITIM/ ONAY TABLOSU

Değişen sayfa	Tarih	Değişiklik	Değişikliği yapan
Dağıtım (İlgili Bölümler)			
Tüm Koç Üniversitesi			