1. AMAÇ

Bu prosedürün amacı Koç Üniversitesi sistemlerine erişim hakkı olan kullanıcıların Koç Üniversitesi (KU)'ne ait Bilgi Sistemleri'ne erişim amaçlı kullanılan KU NetID ve diğer hesap parolalarının (tüm uygulamalar, işletim sistemleri ve veri tabanları) standart ve kurallarının belirlenerek uygulanmasını sağlamaktır.

2. KAPSAM

KU Parola Prosedürü tüm KU sistemlerinin erişiminde kullanılan KU mensuplarının, mezunların ve destek hizmeti alınan tüm firma çalışanlarının hesaplarını kapsamaktadır.

Bu kapsam; KU bilgi işlem ortamında kullanılan tüm ekipman türleri üzerinde kullanılan işletim sistemlerinde, uygulama sistemlerinde veri tabanlarında, kapalı sistemleri uzaktan başlatmak için kullanılan yöntemlerde, paylaşım sistemlerinde, e-posta ve mesajlaşma sistemlerinde, erişim için yetkilendirmenin gerektiği tüm uygulama, sistem ve çözümlerde oluşturulmuş her türlü hesap türlerini içermektedir.

3. REFERANSLAR

3.1. KU Bilgi Güvenliği Yönergesi

3.2. KU Kabul Edilebilir Kullanım Yönergesi

3.3. KU NetID Hesap Yönetim Prosedürü

3.4. YÖK Öğrenci Disiplin Yönetmeliği

3.5. Koç Üniversitesi İdari Personel Yönetmeliği

3.6. 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.

3.7. ISO 27000:2013 Bilgi Güvenliği yönetim standartları ailesi tamamı.

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

3.9. 6698: Kişisel Verilerin Korunması Kanunu

3.10. 4857: İş Kanunu

3.11. 2547: YÖK Kanunu

4. SORUMLULUKLAR

4.1. . Bu prosedürün uygulatılmasından Rektör sorumludur.

4.2. Prosedürün yayına hazırlanmasından, iyileştirme takibinin yapılmasından, parola standartlarının ve genel kuralların uygulanmasından, kullanıcılar için ilk parolaların oluşturulmasından, parolanın unutulması / kaybedilmesi / çalınması gibi durumlarda destek hizmeti vermekten, kritik sistemlerin ve hesapların parolalarının saklanmasından Bilgi Teknolojileri Direktörlüğü sorumludur.

4.3. Bilgi Güvenliği konusundaki özel durumların değerlendirilmesi ve uygulama esaslarının belirlenmesinden Bilgi Güvenliği Komitesi sorumludur.

5. TANIMLAR

5.1. Üniversite: Koç Üniversitesi

5.2. Rektör: Koç Üniversitesi Rektörü

5.3. Prosedür: Parola Prosedürü

5.4. KU mensupları: İdari çalışanlar, akademik çalışanlar, öğrenciler.

5.5. BT: Bilgi Teknolojileri

5.6. Parola/Şifre: Kullanıcının, Koç Üniversitesi bilgi sistemlerine ve uygulamalarına kullanıcı adı ile birlikte kendisini tanıtmasını ve işlem yaratma ve/veya sonuçlandırmasını sağlayan, sadece kendisinin bildiği ve dilediğinde değiştirebileceği alfa nümerik karakterlerden oluşan tanımdır.

5.7. Yetkili Kullanıcı Hesabı: Bağlı olduğu bilgisayar kaynaklarına ve içinde bulunduğu ağ kaynaklarına erişebilen; kullanıcı oluşturma/silme, uygulama yükleme, veri tabanı yönetimi vb. haklara sahip hesap türüdür.

5.8. Servis Hesabı: İşletim sistemlerinde çalışan servisler için oluşturulmuş, güvenlik yetkilendirmelerine bağlı olarak servisin bağlı olduğu bilgisayar kaynaklarına ve içinde bulunduğu ağ kaynaklarına erişme yeteneğini belirleyen hesap türüdür.

5.9. Kullanıcı Hesabı: Bilgi sistemlerinde kişiyi tanımlamak için oluşturulan, sistemde kimlik doğrulaması yapmak ve o sistemin kaynaklarına, verilen yetki doğrultusunda, gerekli erişimi (tanımlı parola ile eşleştirilerek) sağlamak için kullanılan, tüm işlemlerde kişiyi temsil eden alfabetik kod veya alfa nümerik kişiye özel koddur.

5.10. Bilgi Sistemleri: Bilgi sistemleri, Üniversite'nin sahip olduğu, kiraladığı, uyarladığı, muhafaza altına aldığı veya kontrolü altında olan kaynakları; bu kapsamda kişisel veya kurum tarafından sağlanan bilgisayarları, ağları, bulut ve internet temelli hizmetleri, taşınabilir cihaz/depolama aygıtlarını, yazılımları ve bunlar ile ilgili her türlü donanım, teçhizat ve fikri mülkiyeti ifade eder.

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. Bu prosedüre dair tüm istisnalar ancak Bilgi Güvenliği Komitesi onayı ile uygulanır.

6.3. KU Bilgi Sistemlerinde yer alan tüm sorumlular ve kullanıcılar "KU Bilgi Güvenliği Yönergesi" içinde yer alan esaslara göre ilgili cihazlardaki çalışmalarını gerçekleştirirler ve parola/kullanıcı hesaplarını korumakla sorumludurlar.

6.4. Parolalar tüm sorumlular ve kullanıcılar tarafından, gizli bilgi olarak değerlendirilir ve hiç kimseyle paylaşılmaz.

6.5. Tüm sorumlular ve kullanıcıların parolalarını güvenli bir şekilde saklama yolu olmaması durumunda parolalar, kâğıda basılı olarak, elektronik dosyalarda veya cep telefonu gibi el cihazlarında tutulmamalı, saklama yöntemi de onaylanmış olmalıdır.

6.6. Sistem Yöneticileri, standart kullanıcı hesaplarını özel yetkili kullanıcı hesabı olarak yetkilendiremezler.

6.7. Sistem yöneticileri ve Servis operasyonları yetkilileri, standart kullanıcı hesaplarına ve sistemler özelinde ayrılmış farklı özel yetkili kullanıcı hesaplarına sahip olmalıdır. Örneğin; domain admin yetkisine sahip özel yetkili kullanıcı hesabıyla sadece domain controller üzerinde oturum açılmalı, sunucular için farklı, diğer sistemler için farklı kullanıcı hesapları kullanılmalıdır.

6.8. Parola Standartları

6.7.1 Parolalar oturum açılan kullanıcı adıyla aynı olamaz.

6.7.2 Parola içerisinde kullanıcının adı ve soyadı geçemez.

6.7.3 Parolalar ekranda görünür olamaz.

6.7.4 Parola uzunluğunun en az 12 karakter olması, küçük harf, büyük harf, rakam ve sembollerden en az üçünü içerecek şekilde oluşturulması zorunludur.

6.7.5 En son kullanılan 5 parola yeni parola olarak kullanılamaz. Bu kontrolü aşmak amacıyla, minimum parola yaşı 1 gün (24 saat) olarak ayarlanmıştır.

6.7.6 Parola içerisinde boşluk kullanımına izin verilmez.

6.7.7 Parola içerisinde ardışık harf veya rakamlar kullanılamaz. (Örnek: 123, abc, dcba, 4321)

6.7.8 Jenerik, paylaşılmış, ortak, grup parolalar verilmez.

6.7.9 Parolalar, öğrenciler, idari ve akademik çalışanlar için yılda bir zorunlu olarak değiştirilir.

6.7.10 Sunucular, switch'ler ve güvenlik duvarları için yönetici parolaları yılda bir değiştirilir.

6.7.11 İlk üretilen parola tekil olmalıdır ve ilk kullanımdan sonra kullanıcının parola değişikliği yapması zorunludur.

6.7.12 Parolanın 10 kez hatalı girilmesi durumunda hesap 5 dakika süresince kilitlenir. 5 dakika içerisinde yeni hatalı deneme olmazsa hesabın kilidi açılır.

6.7.13 Kullanıcıların telefon, e-posta vb. yöntemlerle yüz yüze olmadan parola sıfırlama istekleri kullanıcı doğrulama yöntemi kullanılarak gerçekleştirilir.

6.7.14 Parolalar, veri tabanında şifrelenerek saklanır.

6.7.15 Parola örnekleri aşağıdaki gibidir;

6.7.15.1 Doğru Parola Örnekleri: AnTkk?27!6973, IsTaRRTkd34Jk

6.7.15.2 Yanlış Parola Örnekleri: canakkale, 1234567890

6.7.15.3 Zayıf Parola Örnekleri: Istanbul12345, Ankara06

6.8 Kritik Parolaların Saklanması ve Yönetimi

Aşağıdaki tablo hangi tip parolaların kritik parola olduğunu göstermektedir. Bu parolalar, kaybolma ve unutulma riskine karşı dikkatli bir şekilde BT parola sorumlusu ve Bilgi Güvenliği ekibi koordinasyonu ile muhafaza edilir.

Sistem	**Parola Tipi**
İşletim Sistemi	Yönetici (Administrator) Parolası/Parolaları
BT Sistemi / İş Uygulaması	Super User Parolası (mevcut olduğu durumlarda) Yönetici (Administrator) Parolası/Parolaları Sistem Parolası (Veritabanı bağlantısı için) mevcut olduğu durumda
Veritabanı	Veritabanı Super User Parolası Veritabanı Yönetici (Administrator) Parolası Veritabanı Güvenlik Görevlisi Parolası
Güvenlik Duvarları, Network, Switch vb.	Yönetici (Administrator) Parolası/Parolaları

7. YÖNTEM

7.1. Parolanın Oluşturulması

7.1.1 Sistem yöneticisi, Servis operasyonları yetkilisi vb. yetkili hesaplara ait parolalar şifreli bir USB içerisinde Bilgi Güvenliği Yöneticisi tarafından koordine edilerek toplanır. Toplanan

parolalar BT direktörüne saklanması için verilir.

7.1.2 Tüm sorumlular ve kullanıcılar kullanmakta oldukları farklı sistemler için LDAP, SSO vb. merkezi yönetimin mümkün olmadığı durumlarda, standartlara uygun farklı parolalar seçerler.

7.1.3 Kullanıcının ilk iş gününde kendisine tanımlanan hesap bilgileri ve geçici parolaları, sistem üzerinden SMS yoluyla gönderilir.

7.1.4 Kullanıcılar, verilen geçici parolaları ve ilk defa tanımlanan parolalarını ilk girişte mutlaka değiştirilmelidir.

7.1.5 Üçüncü parti firmalardan alınan uygulama ve yazılımların üzerinde tanımlı olan parolalar kurulumdan hemen sonra Uygulama ve yazılımdan sorumlu ürün yöneticisi tarafından değiştirilir.

7.1.6 Bir güvenlik sorunu hissedildiği takdirde, ilgili parolalar acilen kullanıcı tarafından değiştirilir ve konu ile ilgili BT Ofis Servis Masası veya KU Yardım Masası bilgilendirilir.

7.1.7 Belirli kısıtlardan ötürü parola standartları uygulanamadığında, bu uygulama belgelenir ve Bilgi Teknolojileri Direktör'lüğüne iletilir.

7.2. Parolanın Unutulması / Kaybedilmesi / Çalınması

7.2.1. İlgili sistem üzerindeki uygulama izin veriyorsa;

Parola sahibi unuttuğu / kaybettiği sisteme ait parolayı tekrar oluşturabilmek için eğer ilgili sistem üzerindeki uygulama izin veriyorsa, söz konusu uygulama üzerindeki parola değişikliği adımlarını uygular.

7.2.2. İlgili sistem üzerindeki uygulama izin vermiyorsa;

İlgili kişi Koç Üniversitesi kimlik kartı ile bizzat "BT Hizmet Masasına" başvurmalıdır.

7.2.2.1.İlgili kişi bizzat gelemiyor ise;

7.2.2.1.1. Ticket açarak,

7.2.2.1.2. BT Hizmet Masası'na telefon ederek,

7.2.2.1.3. it@ku.edu.tr'ye e-posta atarak yeni parola talebinde bulunur.

7.2.3. Talep Hizmet Masası tarafından değerlendirilerek sistemdeki geçerli cep telefonuna yeni parolası SMS yolu ile iletilir. Kullanıcı "https:// it.ku.edu.tr " üzerindeki "Parola Değişimi" link aracılığı ile veya https://account.activedirectory.windowsazure.com/ChangePassword.aspx parola değişim ekranından kendisine verilen yeni parolayı vakit kaybetmeden değiştirmelidir.

8. EKLER ve KAYITLAR

Yoktur.

9. GÖZDEN GEÇİRME

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

10. DEĞİŞİKLİK/ DAĞITIM/ ONAY TABLOSU

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