1. AMAÇ

Bu prosedürün amacı Koç Üniversitesi bilgi sistemlerine erişimde kullanılan kullanıcı hesaplarının yaratılması, izlenmesi ve silinmesi standartlarını tanımlamak, kullanıcıların erişmeye yetkili olacağı uygulamaları ve sistemleri belirleyerek, diğer sistem ve uygulamaları yetkisiz erişimlere karşı korunmaktır.

2. KAPSAM

KU mensupları ve destek hizmeti alınan tüm firma çalışanları ve üniversite tarafından Bilgi Sistemleri ve Bilgi Teknoloji uygulama ve servislerine kampüs içinden veya dışından erişim hakkı verilen tüm kullanıcıları kapsar.

3. REFERANSLAR

3.1 Log Yönetimi Prosedürü

3.2 Parola Prosedürü

3.3 Uzaktan Erişim Prosedürü

3.4 KU NetID Hesap Prosedürü

3.5 YÖK Öğrenci Disiplin Yönetmeliği

3.6 Koç Üniversitesi İdari Personel Yönetmeliği

3.7 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.

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

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

3.10 5651: İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

3.11 6698: Kişisel Verilerin Korunması Kanunu

3.12 4857: İş Kanunu

3.13 2547: YÖK Kanunu

4. SORUMLULUKLAR

4.1 Prosedürün yayına hazırlanmasından, onaylanmasından, yayımlanıp devreye alınmasından, iyileştirme takibinin yapılmasından, bilgi sistemlerine erişimde kullanılan kullanıcı hesaplarının yaratılması, izlenmesi ve silinmesi standartlarının uygulandığının kontrol edilmesinden Bilgi Teknolojileri Direktörlüğü sorumludur.

4.2 Güvenlik politikalarını, yöntemlerini belirlemekten ve değerlendirmekten, 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:** Kullanıcı Erişim Yönetimi, Yetkilendirme ve Hesap Yönetimi Prosedürü

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

5.5 **BT:** Bilgi Teknolojileri

5.6 **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.

5.7 **Trackit:** BT Talep yönetim sistemi

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

5.9 **Dış Kaynak:** Üniversite'nin ihtiyaçları doğrultusunda ilgili konularda hizmet alınan uzman, birim ya da kuruluş.

5.10 **KKD:** Kayıt Kabul Direktörlüğü

5.11 **KUSİS:** Öğrenci bilgi ve yönetim sistemi, öğrenci verilerini yönetmek için kullanılan bir bilgi yönetim sistemidir. Öğrencilerin derslere kaydedilmesi; not verme, akademik başarı transkriptleri ve ortak müfredat etkinlikleri ve öğrenci değerlendirme puanlarının sonuçlarını belgelemek;

öğrenci programları oluşturmak, öğrenci katılımını izleme; gibi öğrencilerle ilgili diğer veri ihtiyaçlarını yönetmek amacıyla kullanılmaktadır.

5.12 **Alias:** E-posta takma adı, ikincil E-posta adresi

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 İdari ve Akademik çalışanların kullanıcı hesaplarının açılmasında veya kapatılmasında referans kaynak olarak Üniversite İnsan Kaynakları, öğrenci ve mezun hesaplarında KKD, sponsorlu hesaplarda hesap sponsorunun (tam zamanlı bordrolu akademik veya idari çalışan) veya İnsan Kaynakları'nın bildirimleri esas alınır.

6.4 Üniversite'de işe başlayan, pozisyon değişikliği olan, ayrılan idari ve akademik çalışanların kullanıcıları ile ilgili bilgiler, Üniversite İnsan Kaynakları tarafından Bilgi Teknolojileri Direktörlüğü'ne iletilir.

6.5 Üniversite'de öğrenime başlayan öğrenci ile ilgili bilgiler KUSİS üzerinden tamamlanınca saat başı çalışan bir script aracılığı ile ve otomatik olarak öğrenci hesabı oluşturulur.

6.6 Mezun hesapları kullanıcı aksini belirtmediği takdirde açık kalır.

6.7 Discontinued hesapların (hesabını kapatmak isteyen, kaydını sildiren, vefat eden vb. sebepleri barındıran hesap tipi) takibi için haftalık kontroller gerçekleştirilir ve kapatmalar yapılır.

6.8 KU mensuplarının kullanması gereken bilgi sistemleri ve kaynaklara erişiminde, sahip olması gereken minimum yetki (KU NetID Hesap Prosedürü'nde belirtildiği üzere) doğrultusunda kaynaklara doğrudan erişim sağlanır. Bu sebeple, standart kullanıcı erişim profilleri tanımlanır.

6.9 Bilgi veya sistemlere erişimle ilgili yasal veya sözleşmelerin zorunlu kıldığı kısıtlamalara uyulması gereklidir. İş ve güvenlik gereklilikleri doğrultusunda, bilgi, uygulama ve iş servislerine erişim kontrol altında tutulur. Kullanıcılara, ihtiyaçları doğrultusunda, sadece gereken erişim alanları ve yolları tanımlanır.

6.10 Bilgi sistemleri kullanıcı erişim hakkı tahsis edilmesi ve yetkilendirmesi sürecinde uyulması gereken kurallar aşağıdaki gibidir:

6.10.1 Bir kullanıcı hesabı yaratılabilmesi için, söz konusu sistem ya da servise uygun düzenlenmiş ve onaylanmış ilintili bir talep olmalıdır.

6.10.2 Kullanıcıya erişim hakları ataması yapılırken, iş amaçlarına uygunluğu ve Üniversite'nin güvenlik politikasıyla tutarlı olduğu kontrol edilir.

6.10.3 Kullanıcıların aktivitelerinden sorumlu tutulması ve takibi için tek bir kullanıcı hesabı kullanılır, grup kullanıcı hesabı kullanımına ise ancak yapılan işe uygunsa izin verilir.

6.10.4 Tüm kullanıcı hesapları atandığı kişiye özel ve benzersiz olarak oluşturulur.

6.10.5 Kullanıcı hesaplarına ait parolalar Üniversite'nin parola prosedürüne uygun olarak oluşturulur ve yönetilir.

6.10.6 Kullanıcı hesapları uzun süre kullanılmadığında ya da kullanılmayacağı bilinen durumlarda kullanıma kapatılır.

6.10.7 Kullanıcıların ilave yetki talebi yapmaları durumunda, işe uygunluğunun ve görevler ayrılığına uyumun kontrol edilebilmesi amacıyla, talepler ticket sistemi üzerinden ilgili servis sahibine iletilir ve servis sahibinden uygunluk onayı alınır.

6.10.8 Üniversite'den ayrılan idari/akademik çalışanın erişim hakları İnsan Kaynakları'ndan gelen bildirim sonrası en kısa sürede kapatılır.

6.10.9 Mezun öğrenci, kapatılmasını talep ettiği takdirde, KKD'den gelen bildirim sonrası en kısa go

6.10.10 Kullanıcı hesapları yönetim sorumluları güvenlik olaylarının araştırılmasında yetkili kişi ve kurumlar ile iş birliği içinde davranır.

6.10.11 Her KU mensubu ve destek hizmeti çalışanı kendi parolası ile yapılmış olan tüm işlemlerle ilgili tüm mali, hukuki ve cezai yükümlülükten sorumludur. Sistemlere ve uygulamalara erişen kullanıcıların yetki aşımına yönelik hareketleri Bilgi Teknolojileri Direktörlüğü tarafından izlenir ve yetki ihlalleri kontrol edilerek ilgili yöneticiler bilgilendirilir.

6.10.12 E-posta adresleri sadece iletişim amacıyla kullanılmak üzere tahsis edilip başka amaçla kullanılmaz (Sosyal medya üyeliği, üyelik hesabı vb. amaçla kullanılmaz).

7. YÖNTEM

7.1 Hesap Adı Oluşturma Kuralları

7.1.1 Kişisel hesaplar için hesap adı ismin ilk harfi ve soyadı birleşiminden oluşur.

7.1.2 Oluşturulan hesap adının başka bir kullanıcıya ait olması durumunda hesap adı tekil bir hesap adı elde edilene kadar ismin ilk 2 harfi ve soyadı, ismin ilk 3 harfi ve soyadı vb. şekilde türetilir. Alternatif olarak isim ve soyadı birleşimi de kullanılabilir.

7.1.3 Öğrenci hesaplarında oluşturulan hesap adının sonuna kayıt olduğu yılın son iki rakamı eklenir.

7.1.4 Kullanıcı adı değişikliği talebinde bulunan öğrenciler için KKD'nin, idari ve akademik çalışanlar için İnsan Kaynakları'nın bilgisi/onayı dahilinde değişiklik gerçekleştirilir.

7.2 KU NetID Değişikliği ve Alias E-posta Adresi Tanımlama

7.2.1 Öğrencinin yasal nedenlerden dolayı adı/soyadı değişikliği sonrası e-posta adresi değişirse eski e-posta adresi alias olarak tanımlanır. E-posta adresi değişikliği için resmi beyan zorunludur (yeni kimlik belgesi, mahkeme kararı vb).

7.2.2 İdari veya akademik çalışanın isteği üzerine ya da yasal nedenlerden dolayı adı/soyadı değişikliği sonrası e-posta adresi değiştirilir. Eski e-posta adresi yeni adresine alias olarak tanımlanır. E-posta adresi değişikliği için resmi beyan zorunludur (yeni kimlik belgesi, mahkeme kararı vb).

7.2.3 Çalışan en fazla 1 adet alias talep edebilir.

7.2.4 Oluşturulan alias adının başka bir kullanıcıya ait olması durumunda alias adı tekil bir hesap adı elde edilene kadar ismin ilk 2 harfi ve soyadı, ismin ilk 3 harfi ve soyadı vb. şekilde türetilir. Alternatif olarak adı - soyadı birleşimi veya soyadı - adı olarak kullanılabilir.

7.2.5 Alias süresiz olarak tanımlanır.

7.2.6 Mezun statüsündeki öğrencilere mezuniyet sonrası ek Alias tanımı yapılmaz.

7.2.7 Alias değişikliği talebinde bulunan öğrenciler için KKD'nin, idari ve akademik çalışanlar için İnsan Kaynakları'nın bilgisi/onayı dahilinde değişiklik gerçekleştirilir.

7.3 Hesap Tiplerinin Belirlenmesi

STANDART HESAP				
Hesap Tipi	**Açıklama**	**Hesap Süresi**	**Varsayılan Servis Yetkileri**	**Talep ve Onay**
İdari ve Akademik	Bordrolu idari ve akademik personel, görevlendirme, proje personeli	Süresiz	• E-posta • Kişisel Dosya Alanı • Ağ Erişimi • Ortak Yazıcılar ve Bilgisayarlar • VPN • Yazılım Arşivi • KU Daily duyuru	SAP Sistemi-İK
Öğrenci	Lisans, yüksek lisans, doktora öğrencileri	Süresiz	• E-posta • Kişisel Dosya Alanı • Ağ Erişimi • Ortak Yazıcılar ve Bilgisayarlar • VPN • Yazılım Arşivi • KU Daily duyuru	(KUSİS-KKD)-BT
Mezun	Koç Üniversitesi mezunu	Süresiz	• E-posta • KUSIS	(KUSİS-KKD)-BT
Değişim Programları Öğrencisi	Koç Üniversitesine değişim programı ile gelen öğrenci	Maksimum 5 yıl	• KUSIS	(KUSİS-KKD)-BT
Birim Hesapları	Birim adına oluşturulan e-mail gönderimleri	Süresiz	• E-posta	Dekanlık-BT Direktörlük-BT

	için yapılan e-mail hesapları Örnek: Genel Sekreterlik Mail Hesapları			

SPONSORLU HESAP				
Hesap Tipi	**Açıklama**	**Hesap Süresi**	**Varsayılan Servis Yetkileri**	**Talep ve Onay**
Misafir	Üniversite'den ayrılmış Akademik Personel veya Üniversite ile ilgili çalışma yapan veya Üniversite'yi temsil eden kişiler için açılır. (Örnek: Bordrosuz idari çalışan, KUH misafir çalışan, misafir öğretim üyesi, misafir araştırmacı, TÜBİTAK bursiyeri, distinguished research fellow)	Maksimum 6 ay (Yenilenebilir)	• KU NetID: Kişinin merkezi directory'i de tutulmasıdır. • Talep Edilen Servisler değerlendirme sonrası aktif edilir. Örnek: Ağ Erişimi, Yazıcı, VPN, Kişisel dosya alanı, e-posta, HPC vb.	Dekanlık-İK-BT Direktör Rektör
Birim	Seminer, etkinlik, proje, idari/akademik birim, sistem test kullanıcısı gibi amaçlar için açılır. Örnek: Öğrenci Kulüp Mail Adresleri, Seminer ya da etkinlik mail adresleri	Maksimum 6 ay- Etkinlik sürecince yenilenebilir. Kulüp mail adresleri için 1 dönem boyunca açık kalabilir.	• KU NetID: Kişinin merkezi directory'i de tutulmasıdır. • Talep Edilen Servisler değerlendirme sonrası aktif edilir. Örnek: Ağ Erişimi, Yazıcı, VPN, Kişisel dosya alanı, e-posta vb.	Direktörlük-BT Dekanlık-BT

Danışman	Koç Üniversitesi SAP danışmanı, IT danışmanı veya x bir birim danışmanı, KU mensubu olmayan kişilerdir. Örnek: Sistem ve web uygulamalarının gerekli güncellemeleri ve geliştirilmesi, yönetilen hizmetler (SAP, KUSİS, Web)	Maksimum 1 ay (Yenilenebilir) BT Direktör onayıyla 1 yıla kadar	• KU NetID: Kişinin merkezi directory'i de tutulmasıdır. • Talep Edilen Servisler değerlendirme sonrası aktif edilir. Örnek: Ağ Erişimi, Yazıcı, VPN, Kişisel dosya alanı, e-posta vb.	Direktörlük-BT Dekanlık-BT
Alt İşveren	Üniversite için çalışma yapan dış firmalardır. Örnek: ITB, Siemens gibi.	Sözleşme süresi kadar, maksimum 1 yıl olmak üzere Aylık aktif olan hesap kontrolleri hizmet alan birim tarafından düzenli kontrol edilir. Ayrılan personelin hesabının kapatılması talebi açılır.	• KU NetID: Kişinin merkezi directory'i de tutulmasıdır. • Talep Edilen Servisler değerlendirme sonrası aktif edilir. Örnek: Ağ Erişimi, Yazıcı, VPN, Kişisel dosya alanı, e-posta vb.	Direktörlük-İK Dekanlık-İK

7.4 E-posta ve AD Kullanıcı Hesabı Yaratma/Değiştirme/Kapatma

7.4.1 E-posta ve AD kullanıcı hesapları için;

Üniversite'de işe başlayan, pozisyon değişikliği olan, ayrılan idari ve akademik çalışanların kullanıcıları ile ilgili bilgiler Üniversite İnsan Kaynakları tarafından,
Üniversite'de öğrenime başlayan öğrenci ve mezunlar ile ilgili bilgiler KUSİS üzerinden, sponsorlu hesaplara ait bilgiler (tam zamanlı bordrolu akademik veya idari çalışan) İnsan Kaynakları tarafından Bilgi Teknolojileri Direktörlüğü'ne iletilir.

7.4.2 Kullanıcı hesabı yaratılması, hesap ile ilgili değişiklik yapılması veya hesabın kapatılmasına ilişkin süreç aşağıda açıklanmaktadır.

7.4.3 E-posta Dağıtım/Tartışma Grupları (Google Groups, Microft 365 vb.) için Uygulanacak Prensipler

7.4.3.1 E-posta Dağıtım/Tartışma Grupları İdari Personel, Akademik Personel ve Öğrenciler tarafından kullanılabilir.

7.4.3.2 E-posta dağıtım/tartışma grupları self servis bir hizmet olarak sunulur ihtiyaç olması halinde KU mensubu, KU hesabı ile Google grup oluşturulabilir. Google grubu oluşturan KU mensubunun mail adresine "Kabul Edilebilir Kullanım Yönergesi" otomatik bir mail ile gönderir. Grup sahibi yönergedeki tüm maddeleri kabul etmiş sayılır.

7.4.3.3 E-posta dağıtım listesi Microsoft 365 grupları olarak BT tarafından oluşturulur.

7.4.3.4 Grup üyeleri grubun sahibi tarafından eklenir/güncellenir.

7.4.3.5 Grubun tanımlanmasından 1 yıl sonra kullanıma devam edilip edilmeyeceğine dair grup sahibine bildirim gönderilir. Grup sahibinin devam etmesini istemesi durumunda grup 1 yıl daha açık kalır, aksi halde 30 gün sonra silinir.

7.4.3.6 Grubun kötüye kullanımı durumda haber vermeksizin BT tarafından arşivlenebilir/silinebilir.

7.4.3.7 Oluşturulan Google gruplara dış domain kullanıcısı ekleme yetkisi ancak IT tarafından değerlendirilip uygun görülmesi halinde verilebilir. Trackit üzerinden talep kabul edilir.

7.5 İdari ve Akademik Hesaplar

7.5.1 İdari veya Akademik hesaplar İK talebi ile açılır, uzatılır.

7.5.2 İdari veya Akademik hesaplar, hesap sahibinin Üniversite ile ilişiği kesildiğinde İK talebi ile kapatılır.

7.5.3 Üniversite ile ilişiği kesilen hesap sponsorlu kişisel hesaba çevrilebilir. Bu durumda talep İK tarafından yapılır.

7.5.4 Ayrılan çalışanın e- postalarının bir başkasının e-posta hesabına yönlendirmesi yapılmaz. Ayrılan çalışanın hesabına gelen e-posta'ya talep halinde otomatik bilgilendirme cevabı yazılır. Talep İK'dan gelmelidir.

7.5.5 Ayrılan çalışanın eski e-posta ve eski verilerine erişim ayrılan çalışanın İK tarafından alınmış izin ve talebi ile başka bir çalışana yapılabilir. Talep BT'ye İK'dan iletilmelidir.

7.5.6 Ayrılan çalışana eski e-posta ve verileri verilmez.

7.5.7 İnsan Kaynakları Direktörlüğü talebi ile yeni başlayan veya devam eden çalışana BT tarafından hesap ve bilgi güvenliği eğitimi verilir.

7.6 Öğrenci Hesapları

7.6.1 Yeni kayıt yapan öğrenci hesapları Kayıt ve Öğrenci İşleri Direktörlüğü talebi ile açılır. Gerekli hesap bilgileri KUSIS öğrenci bilgi sistemi üzerinden alınır.

7.6.2 Okulla ilişiği kesilen öğrencinin hesabı Kayıt ve Öğrenci İşleri Direktörlüğü talebi veya Öğrenci Dekanlığı talebi ile kapatılır veya tekrar açılır.

7.7 Mezun Hesapları

7.7.1 Mezun olan öğrencilerin hesapları Kayıt ve Öğrenci İşleri Direktörlüğü talebi ile mezun hesap tipine çevrilir. Hesap kapanmaz, e-posta ve KUSIS erişimi harici yetkiler iptal edilir.

7.8 Sponsorlu Hesaplar

7.8.1 Hesap sponsoru tam zamanlı bordrolu akademik veya idari personel olmalıdır. Sponsor ilgili birim/fakülte/enstitü yöneticisi tarafından atanır (Rektör, Dekan, Birim en üst idari yöneticisi). Hesap sponsoru değiştiğinde BT Direktörlüğü bilgilendirilmelidir.

7.8.2 Danışman sponsor hesapların talepleri ilgili Direktörlükler, diğer sponsorlu hesapların talepleri (açılış, kapanış, yenileme ve yetkilendirme) İK tarafından yapılır.

7.8.3 Sponsor, hesap açılış/yenileme talebinde hesabın kapatılacağı tarihi ve hesabın açılış/yenileme amacını belirtir. Sponsorlu hesap tiplerine göre izin verilen maksimum hesap süreleri Sponsorlu Hesap Tablosunda yer almaktadır.

7.8.4 Açılışta belirtilen hesap süresi dolan hesap otomatik olarak kapanır.

7.8.5 Seminer, etkinlik, proje gibi birim hesap açılış, yenileme, kapatma talepleri ilgili Dekanlıklar tarafından yapılır. Ayrı hesap açılmaz. Paylaşılmış hesap açılır, teknik nedenlerden dolayı paylaşılmış hesap açılmıyorsa süreli ve sponsorlu hesap açılır ve sponsor tarafından talep edilen minimum kişiye erişim yetkisi verilir. Sponsorlu Hesap Tablosu'ndaki servislere göre Birim Hesabı açılır. Paylaşılmış hesaplar üzerinden herhangi bir servise üyelik ve giriş sağlanamaz. Sadece yetkilendirilmiş kişiler iletişim amaçlı kullanabilir.

7.8.6 Öğrenci kulüpleri için hesap açılış, yenileme, kapatma talepleri Öğrenci Dekanlığı tarafından gelmelidir. Sponsorlu Hesap Tablosuna göre Birim Hesabı açılır. Hesap adlarında kulüp adını içeren bir örnek olur (örnek-club@ku.edu.tr). E-posta adresleri sadece iletişim amacıyla kullanılmak üzere tahsis edilip başka amaçla kullanılmaz (Sosyal medya, üyelik vb. amaçla kullanılmaz).

7.8.7 Yenilenecek hesap için sponsor, hesap kapanış tarihinden en geç bir hafta önce yenileme talebini İnsan Kaynakları Direktörlüğü'ne yapmalıdır.

7.8.8 Sponsorlu hesapların açılış/yenileme talebinde belirtilen amaç ile sınırlı olarak kullanılması esastır.

7.8.9 Sponsorlu hesaplara Sponsorlu Hesap Tablosunda belirtilen varsayılan servis yetkileri otomatik olarak verilir.

7.8.10 Sponsorlu hesap sahipleri Üniversite adına kayıtlı yazılım kaynaklarını kullanamaz.

7.8.11 Paylaşılmış hesaplar üzerinden herhangi bir servise üyelik ve giriş sağlanamaz. Sadece yetkilendirilmiş kişiler iletişim amaçlı kullanabilir.

7.9 Değişim Programları Öğrencisi

7.9.1 Değişim programlarıyla gelen öğrencilerin hesapları Kayıt ve Öğrenci İşleri Direktörlüğü talebi ile açılır. Gerekli hesap bilgileri KUSIS öğrenci bilgi sistemi üzerinden alınır.

7.9.2 Okulla ilişiği kesilen öğrencinin hesabı Kayıt ve Öğrenci İşleri Direktörlüğü talebi veya Öğrenci Dekanlığı talebi ile kapatılır veya tekrar açılır.

7.9.3 Değişim programını tamamlayan öğrencilerin hesapları Kayıt ve Öğrenci İşleri Direktörlüğü talebi ile "volunteer discontinued" hesap tipine çevrilir. Hesap kapanmaz, KUSIS öğrenci bilgi sistemi erişim harici bütün yetkiler iptal edilir.

7.9.4 KUSIS erişimi ve hesap 5 yıl sonunda tamamen kapatılır.

7.10 Veritabanı Kullanıcı Erişim ve Yetkilendirme

7.10.1 Üniversite'de veritabanlarına erişim talebi, yetki tipi, erişim amacı ve erişim süresi Trackit sistemi üzerinden alınır. İlgili talep değerlendirildikten sonra kısıtlı erişim için çalışma yapılır. İlgili veritabanı erişiminin verilmesi için ilgili kayıt servis sahibinin onayına düşer. Servis sahibinin onayından sonra yetkili veritabanı yöneticisi gerekli tanımlamaları yaparak veritabanı yetkilendirmelerini gerçekleştirir.

7.10.2 Kullanıcılar herhangi bir yetki verilmeden tanımlanır. Eğer sistem yöneticisi yetkisi isteniyor ise Ayrıcalıklı Yetkiye Sahip Hesaplar için tanımlanmış süreç işletilir.

7.10.3 Veritabanı kullanıcı yetkilendirmeleri Yetki Onay Matrisi'ne uygun olarak yapılmaktadır.

7.11 Uygulama Kullanıcı Hesabı Yaratma/Değiştirme/Kapatma

7.11.1 Merkezi Kimlik Yönetim Sistemi ile Entegrasyonu Olan Uygulamalar

7.11.1.1 Üniversite'de öğrenime başlayan öğrenci ile ilgili bilgiler KUSİS üzerinden tamamlanınca saat başı çalışan bir script aracılığı ile ve otomatik olarak öğrenci hesabı oluşturulur.

7.11.1.2 Üniversite'de göreve başlayan idari çalışanlar, akademik çalışanlar ile ilgili bilgiler SAP üzerinden tamamlanınca Bilgi Teknolojileri Direktörlüğü'ne otomatik olarak ticket açılır ve manuel olarak hesap oluşturulur.

7.11.1.3 Uygulamalarda local hesap talepleri ticket sistemi üzerinden alınır. İlgili IT bölüm yöneticisi bilgisi/onayı dahilinde hesap açma işlemi gerçekleşir.

7.11.2 Merkezi Kimlik Yönetim Sistemi ile Entegrasyonu Olmayan Uygulamalar

7.11.2.1 Uygulama kullanıcı hesapları için, hesap açma talepleri Trackit üzerinden alınır. Kişi talep açarken yönetici onayı ile birlikte tanımlanması gereken rolleri iletilmesi ya da departmanda çalışan aynı rollere sahip örnek bir kullanıcının adını iletilmesi gerekmektedir. Ardından kullanıcı adı oluşturularak gerekli bilgiler kişiye iletilir.

7.11.2.2 Merkezi Kimlik Yönetim Sistemi ile Entegrasyonu Olmayan Uygulamalar listesi üzerinden kontrol edilerek manuel olarak servis sahipleri tarafından kapatılır/silinir.

7.11.2.3 İK, Trackit üzerinden hesabın kapatılması/silinmesi için talep iletir ve servis sahibi tarafından manuel olarak hesap kapatılır/silinir.

7.12 Yetki Onay Matrisinin Oluşturulması

7.12.1.1 Her uygulama için rollerin ve yetkilerin yer aldığı, ayrıca ilgili rollerde giriş yapabilecek kullanıcıların listelendiği 3-6 dosyada yetki onay matrisi tutulmaktadır.

7.12.1.2 Yetki onay matrisi çevrimiçi ortamda (Jira/ SharePoint) güncel olarak tutulmaktadır.

7.13 Ayrıcalıklı Kullanıcı Erişim&Hesap Yönetimi

7.13.1 Tüm kullanıcı hesaplarına ve yapılandırmalarına ek olarak, ayrıcalıklı kullanıcı hesapları (ör. root ve yönetici haklara sahip hesaplar) sadece belirli iş gereksinimleri doğrultusunda ve görev tanımları doğrultusunda verilir.

7.13.2 Ayrıcalıklı yetkilere sahip kullanıcıların Üniversite'den ayrılması durumunda, ayrılan kullanıcının erişim hakları hemen silinir veya bloke edilir.

7.13.3 Servis hesapları (ör. root ve yönetici haklara sahip hesaplar) herhangi bir kullanıcı ile aynı kullanıcı adına sahip olmamalıdır.

7.13.4 Ayrıcalık yetkilere sahip kullanıcı hesapları bir sorumlu ile ilişkilendirilmelidir. Bu ilişkilendirmenin gerçekleşemediği durumlarda sistem ayrıcalıklı yetkiye sahip kullanıcı hesabının hangi bireysel kullanıcı tarafından kullanıldığına ilişkin bir denetim izi oluşturmak zorundadır.

7.13.5 Ayrıcalıklı yetkiye sahip kullanıcı hesapları, daha düşük yetkilerin yeterli olduğu durumlarda kullanılmaz.

7.13.6 Ayrıcalıklı yetkiye sahip kullanıcı hesapları 6 ay boyunca kullanılmadığı durumlarda yetkiler kaldırılır.

7.13.7 Kullanıcı hesaplarına ait parolalar Üniversite parola prosedürüne uygun olarak oluşturulur ve yönetilir.

7.13.8 Kullanıcıların ilave yetki talebi yapmaları durumunda, işe uygunluğunun ve görevler ayrılığına uyumun kontrol edilebilmesi amacıyla, talepler ilgili servis sahiplerine iletilir ve uygunluğu için görüşleri alınır.

7.13.9 Görevler ayrılığı prensibi kullanıcıların iş kritik fonksiyonları yapabilmelerini engellemek için uygulanmalıdır. Mümkün olduğunca aşağıdaki görev çiftlerinin aynı kişi tarafından yapılmaması gerekir:

7.13.9.1 Sistem yöneticisi ve ağ yöneticisi

7.13.9.2 Sistem geliştirme & bakımı ve değişiklik yönetimi

7.13.9.3 Güvenlik yönetimi ve güvenlik denetimi

7.13.9.4 Geliştirme ve canlı ortam rolleri

7.13.10 Kullanıcının işten çıkması durumunda ağ erişimi hemen kesilmelidir.

7.14 Ek Yetki Taleplerinin İşlenmesi

7.14.1 Ekstra bir yetki talebi olması durumunda, Trackit üzerinden ilgili çalışan kayıt açar. Açılan kayıt talep sahibi çalışanın yöneticisi ve ilgili sistem/birim/modül sorumlusunun onayına sunulur.

7.14.2 Onaylanan talepler için Yetki Onay Matrisi'ne istinaden gerekli yetkilendirmeler gerçekleştirilir. Talep tamamlandıktan sonra ilgili kayıt kapatılır ve talep sahibine otomatik olarak e-posta yolu ile bilgilendirme yapılır.

7.15 Yetki Taleplerinin Gözden Geçirilmesi

7.15.1 Mevcut yetkiler, Yetki Onay Matrisi' ne göre sorumlu birim çalışanı tarafından senede 1 (bir) kez gözden geçirilir. Servis sahibi sürecin başlatılmasından sorumludur. Süreç Trackit üzerinden başlatılır ve her bir uygulama için ilgili yetkilendirme sorumlusuna gözden geçirme talep kaydı açılır.

7.15.2 Açılan talepler sonrasında yetkilendirme sorumlusu, talebin açılma tarihinden itibaren 1 (bir) ay içerisinde, yetkileri incelemiş, değişiklik taleplerini iletmiş ve kaydı kapatmış olmalıdır.

7.15.3 Değişiklik talepleri bu süreç kapsamında tanımlanmış olan "Ek Yetki Taleplerinin İşlenmesi" maddesine göre gerçekleştirilir.

7.16 Düzenli Erişim Kontrolleri

7.16.1 Erişim güvenliğinden emin olmak için işe başlayan, pozisyon değişikliği olan, ayrılan idari ve akademik çalışanların kullanıcı hesapları düzenli olarak gözden geçirilir, gereksiz kullanıcı hesapları kaldırılır.

7.16.2 Yetki gözden geçirme sürecine dahil olan uygulamalar üzerinde erişim hakları ve görevler ayrılığı ilkesine uyumu yetki taleplik dönemlerde kontrol edilir.

7.16.3 Ek - 1 Yetki Gözden Geçirme Sürecine Dahil Olan Uygulamalar Listesi bu prosedürün bir parçası olarak en az yılda 1 kez gözden geçirilir ve gerektiği durumlarda güncellenir. Bu gözden geçirme ile sürece dahil olan tüm sistemler üzerinde yetkisiz erişim hakları bulunmadığı teyit edilir.

7.16.3.1 Ek - 1 Yetki Gözden Geçirme Sürecine Dahil Olan Uygulamalar Listesi güncellemesi, Bilgi Güvenliği Komitesi'nde görüşülür ve onaylanır.

7.16.4 Üniversite içinde pozisyon değişikliği yapılan çalışanın erişim yetkileri gözden geçirilir ve yeni iş gereksinimlerine uygun şekilde yeniden atanır. Kullanıcı farklı departmana geçtiyse grup üyelikleri değişir. Yönetici talebi ile iş devri süresince yetkiler kısa süreli olarak bırakılabilmektedir.

7.16.5 Kullanılan her sistem için log yönetim aracı ile yetkilendirme denetim izleri tutulur. Tutulan denetim izleri periyodik olarak gözden geçirilir. Bu süreç "Log Yönetimi Prosedürü'nde" anlatılmıştır.

7.17 Uzaktan Erişim (VPN) Talepleri

7.17.1 Üniversite etki alanı dışından Üniversite Bilgi Sistemlerine yapılacak olan bağlantılarda VPN istemci uygulaması kullanılır. Uzaktan Erişim Prosedürü'nde tanımlandığı üzere, VPN erişim talepleri, Trackit üzerinden Bilgi Teknolojileri Direktörlüğü'ne iletilir.

7.17.2 Talebin gerekçesi Bilgi Güvenliği ekibinin incelemesi sonucunda uygun görüldüğü takdirde VPN erişimi sağlanır.

7.17.3 Kullanıcıların, Üniversite etki alanı dışından kendi kullanıcı hesapları ile yaptıkları işlemler loglanır ve kullanıcılar gerçekleştirdikleri tüm işlemlerden sorumludur.

7.17.4 Üçüncü taraflara ilişkin erişim hakları, gerektikçe aktif hale getirilir ve kullanılmadığı durumda erişim izni bloke edilmiş olarak tutulur.

7.18 Dosya Sunucusu Erişim Talepleri

7.18.1 Kullanıcıların dosyalarının bulunduğu ve yedeklendiği için güvenli bir ortamda bulunan Dosya Sunucusu için klasör erişim talebi Bilgi Teknolojileri Direktörlüğü'ne, Trackit üzerinde açılan kayıt ile iletilir.

7.18.2 İlgili kayıt klasörün sahibi birim yöneticisinin onayına gönderilir ve birim yöneticisinin onayının ardından talebin gereklilikleri yerine getirilerek kayıt kapatılır.

7.19 Sponsorlu Hesaplar için Erişim Yetkilendirme ve Kontrolü

7.19.1 Erişim sağlayacak ya da sağlanacak firmalar Üniversite'nin güvenlik ve gizlilik başta olmak üzere Üniversite tarafından belirlenen tüm bilgi teknolojileri yönerge ve prosedürlerine uymak zorundadır. Bu yönerge ve prosedürlerin ihlali sonucu erişim hemen sonlandırılacaktır.

7.19.2 Üniversite Bilgi Teknolojileri Direktörlüğü, herhangi bir zamanda erişimin sonlandırılması veya başlatılması hakkını saklı tutar. Üniversite adına proje yürüten üçüncü taraf firmaların ağ servislerine erişimi, olması gereken kadar tanımlanır. Mümkün olduğu durumda çalışma yapacak üçüncü taraf çalışanına BT çalışanı/idari çalışan da eşlik etmelidir.

7.19.3 Sponsorlu hesaplar maksimum 3 ay süre ile sınırlandırılır.

7.19.4 Dış kaynaklara atanan uzaktan erişim yetkileri zaman kısıtlı olarak verilir. Proje bazlı çalışan dış kaynaklara proje süresince erişim verilir, kullanıcı listesi üç ayda bir gözden geçirilir.

7.19.5 Destek hizmeti alınan kullanıcılar için maksimum süre yıllık bakım hizmet anlaşması süresiyle sınırlandırılır. Kullanıcı listesi üç ayda bir gözden geçirilir. Süre bitiminde otomatik olarak kapatılır, tekrar erişim gereği varsa talep süreci yeniden işletilir.

7.19.6 Sponsorlu hesaplar, mümkünse, Üniversite tarafından temin edilecek bilgisayarlar üzerinde ve standart kullanıcı erişim hakları ile çalışır. Üçüncü taraf çalışanın kullanabileceği sistemler, yapacakları iş ve haberleşme gereksinimleri ile sınırlıdır.

7.20 Acil Durum Erişim Yetkilendirme ve Kontrolü

7.20.1 Yetki değişikliğinin gerektiği, en kısa süre içerisinde gerçekleştirilmesi gereken ve acil olduğuna karar verilen durumlarda, Üniversite çalışanı/ KU mensubu yetkileri ile ilgili olarak iletilen erişim talepleri için istisnai durum sebebiyle ilgili servis sahibinin onayı alınmadan yetki değişikliği gerçekleştirilebilir.

7.20.2 Bu tür acil durumlar veya izin, eğitim, rahatsızlık vb. geçici yokluk durumlarında gelen acil yetki talepleri ile ilgili servis sahibinin azami bir alt veya bir üst unvandaki kişiye onaya sunulabilir.

7.20.3 Gerekli yetki talebi karşılanırken ilgili BT çalışanı tarafından Üniversite'nin genel organizasyon yapısı ve iş akışı göz önünde bulundurularak, ilgili geçici onaylar alınır ve uygun görülen talepler için, gerekli tanımlamalar yapılır. Durumun aciliyeti geçtikten sonra ve ilgili yönetiye erişilebildiğinde, mevcut onayların yanı sıra servis sahibinin de onayı talep edilir.

8. EKLER ve KAYITLAR

Ek - 1 Yetki Gözden Geçirme Sürecine Dahil Olan Uygulamalar Listesi

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
11	03.08.2021	7.12.1.1 maddesinde yer alan	Ertuğrul Doğan
11	03.08.2021	“iki ayrı” ibaresi kaldırılmış,	Ertuğrul Doğan
13	03.08.2021	“ilgili rollerde giriş	Ertuğrul Doğan
8	20.05.2022	yapabilecek kullanıcıların	Enis Alper Ekiz
4	20.05.2022	listelendiği yetki onay	Enis Alper Ekiz
18	20.05.2022	matrisi tutulacaktır.” İfadesi eklenmiştir. 7.13.7 maddesinde yer alan “Paralo Prosedürü’ne uyum” ifadesi kaldırılmıştır. 7.16.3 maddesine 1.16.3.1 maddesi eklenmesi yapılarak “ Ek-1 Yetki Gözden Geçirme Sürecine Dahil Olan Uygulamalar Listesi güncellemesi, Bilgi Güvenliği Komitesi’nde görüşülür ve onaylanır.” İfadesi eklenmiştir. 7.4.3.3 maddesi silinmiştir. 7.4.3.7 maddesi eklenmiştir. 6.10.12 maddesi eklenmiştir. 7.8.11 maddesi eklenmiştir. 7.4.3.2 maddesi güncellenmiştir. 7.8.5 maddesi güncellenmiştir.	Enis Alper Ekiz

		Sponsorlu Hesap tablosunda Birim hesapları Maksimum 6 ay olarak güncellenmiştir.	
Dağıtım (İlgili Bölümler)			
Tüm Koç Üniversitesi			