1. AMAÇ

Veri Sınıflandırma Prosedürü'nün amacı, verinin gerektirdiği güvenlik düzeyine uygun olarak sınıflandırılmasına ilişkin kuralları belirlemektir.

2. KAPSAM

Koç Üniversitesi Bilgi Teknolojileri ve Sistemleri başta olmak üzere Üniversite'nin elektronik ortamlarda olan tüm bilgi varlıklarının üzerinde bulunan verileri ve Bilgi Teknolojileri'ne ait fiziksel ortamlarda yer alan tüm varlıkların üzerinde bulunan verileri kapsamaktadır.

3. REFERANSLAR

3.1 Fiziksel ve Çevresel Güvenlik 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 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

3.8 6698 sayılı Kişisel Verilerin Korunması Kanunu

3.9 4857 sayılı İş Kanunu

3.10 2547 sayılı Yükseköğretim Kanunu

4. SORUMLULUKLAR

4.1 Bu prosedürün uygulatılmasından Rektör sorumludur.

4.2 Prosedürün yayına hazırlanmasından, onaylanmasından, yayımlanıp devreye alınmasından, iyileştirme takibinin yapılmasından ve veri sınıflandırma ve işleme standartlarının uygulandığının kontrol edilmesinden Bilgi Teknolojileri Direktörlüğü sorumludur.

4.3 Verilerin sınıflandırması ile ilgili farkındalığın artırılması için eğitimlerin ve bilgilendirici bültenlerin hazırlanmasından Bilgi Teknolojileri Direktörlüğü bünyesindeki Bilgi Güvenliği Ekibi sorumludur.

4.4 Sistem tarafından otomatik olarak etiketlenmemiş bir verinin doğru sınıflandırmayla etiketlenmesinden son kullanıcı sorumludur.

4.5 Bu prosedürün Koç Üniversitesi'ne bağlı Koç Üniversitesi Hastanesi için işletilmesinden Koç Üniversitesi Hastanesi bizzat sorumludur. Buna ek olarak hastanelere özel olarak işletilmesi gereken bu Prosedür konusuna ilişkin kurallar ayrıca Koç Üniversitesi Hastanesi [Başhekimliği] tarafından yayımlanır ve uygulanır.

5. TANIMLAR

5.1 KU Mensupları: İdari çalışanlar, akademik çalışanlar, öğrenciler.

5.2 Veri Sahibi: Verilere erişme, düzenleme hakkına sahip olan ve verilerin nasıl kullanıldığına dair kararları veren kişiler veya ekiplerdir. Veri Sahibi, verileriyle her gün çalışmayabilir, ancak bir veri alanını denetlemek ve korumaktan sorumludur.

5.3 Bilgi Varlıkları: Dijital veya basılı ortamlarda veri barındıran her türlü BT sistemi, bilgisayarlar, veri depolama sistemleri, öğrenci bilgileri, proje tasarımları ve süreçler vb. varlıklardır.

5.4 Varlık: Üniversite için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır. Bilgisayarlar, mobil cihazlar, monitörler, ağ cihaz/yazılımları, printerlar, projektörler, sunucular varlık olarak değerlendirilir.

5.5 Veri: Üniversitenin tüm sistemlerinde, çalışanlarında, kütüphanelerinde tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen bilgidir**.**

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.

6. TEMEL PRENSİPLER

4.1 Bu Prosedür ve bağlantılı diğer yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde Üniversite idari çalışanları için 4857 sayılı İş Kanunu ve Koç Üniversitesi İdari Personel Disiplin Yönetmeliği, Üniversite akademik personel çalışanları için 2547 sayılı Yükseköğretim Kanunu, öğrenciler için Yükseköğretim Öğrenci Disiplin Yönetmeliği kuralları uygulanır.

4.2 Veri Standartları

4.2.1 Bilginin elektronik olarak işlenmesi amacıyla kullanılacak bilişim ve bilgi işlem sistemlerinin, Üniversite bilgi güvenliği yönerge ve prosedürlerine uygun olarak temin edilmiş, korunmuş ve kullanılmakta olduğundan emin olunmalıdır.

4.2.2 Bilginin, yazılı, sözlü, görsel ortamlarda işlenmesi söz konusu olduğunda, bilginin kullanıldığı ortamın ve altyapının, Üniversite bilgi güvenliği yönerge ve prosedürlerine uygunluğu sağlanmalı; bilgiyi kullanan tüm tarafların da bu yönerge ve prosedürlerin gereklerinden haberdar olduğundan ve bunlara uyduğundan emin olunmalıdır.

4.3 Tanım dışı durumlar Bilgi Güvenliği Komitesi tarafından değerlendirilmektedir.

7. YÖNTEM

5.1 Verinin Sınıflandırılması

Verilerin kullanılış biçimlerinin farklı olması nedeniyle beş hassasiyet grubuna ayrılmaları benimsenmiştir. Bu sınıflamalar aşağıdaki şekilde tanımlanmıştır:

Sınıf	Açıklama	Örnek
ÇOK GİZLİ	Sınırlı kişiler tarafından bilinmesi gereken, başka kişi/kişiler/kuruluşlar ile paylaşılması, kaybolması durumunda Üniversite'nin mevcudiyetini ve faaliyetini ciddi olarak olumsuz etkileyecek ulusal ya da uluslararası risklere, milli güvenliğe, milli savunmayaya da uluslararası anlaşmazlıklara neden olacak, zarar verebilecek, yasal soruşturma ya da incelemeye neden olacak verilerdir.	Ulusal güvenlik ya da savunma sanayi projeleri için kullanılacak her türlü proje ve amacı olan buluş ile ilgili bilgiler (yazılımlar, çizimler, proje belgeleri vb.), yatırım planları, yatırım stratejileri ve hedefleri ile ilgili bilgiler, sektörde büyük değişikliklere neden olacak, rekabet koşullarını değiştirecek buluş ya da metodolojiler ile ilgili bilgiler vb.
GİZLİ	Yetkisiz kişi/kişiler/kuruluşlar ile paylaşılması ya da kaybolması durumunda Devletin menfaatlerini, güvenliğini veya Üniversite'nin operasyonlarını, imajını veya gelirlerini ciddi olarak etkileyecek ve aksatacak veriler bu kapsama girer.	Şifreler, iş planları, maaş bilgileri, sözleşmeler, teklifler, maliyet raporları, şartnameler, hassas tasarım çalışmaları, hasta bilgileri, satış bilgileri, servis bilgileri, lansmanı yapılmamış yeni hizmetler, iş ortaklığı anlaşma içerikleri, stratejik planlar, personele ait özlük bilgileri, uygulanan güvenlik kontrolleri, kredi kartı bilgileri vb. bu kategoriye girmektedir. Ayrıca, 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında özel nitelikli veri olarak tanımlanan kişisel veriler de bu kategoriye girmektedir.
HİZMETE ÖZEL	Sadece Üniversite içinde paylaşılan veya ihtiyaç durumunda hizmet alınan ve Gizlilik Sözleşmesi imzalanan kurumlarla paylaşılan ve Üniversite veya belirtilen kurumların dışına çıkması onaylanmayan, izinsiz paylaşımı ya da kaybı Üniversite organizasyonu için imaj kaybı gibi sonuçlar doğurabilecek, uygunsuzluklar yaratabilecek ancak ciddi maddi zararlara ya da hasarlara neden olmayacak verilerdir.	Hizmet alınacak firmalarla paylaşılabilecek operasyonel bilgiler, projelerle ilgili dokümanlar, proje gereği Gizlilik Sözleşmesi imzalanmış firmalarla paylaşılan iş özelindeki bilgiler vb. bu kapsama girer. Ayrıca, Üniversite içinde dağıtımı yapılan toplantı zamanları, genel üniversite bilgilendirmeleri, duyurular, telefon listeleri, çalışan listeleri, eğitim bilgileri, formlar, yazışma örnekleri, prosedürler, operasyonel bilgiler, proje planları, ad, soyad ve IP adresleri içeren dokümanlar vb. bilgiler de bu kategoriye girmektedir.

GENEL	Geneli ilgilendiren en düşük güvenlik seviyesindeki veriler olup paylaşılması ya da kaybolması durumunda risk oluşmayan, herkese açık verilerdir. "GİZLİ", "HİZMETE ÖZEL" ve "ÇOK GİZLİ" olarak gizlilik sınıflandırması belirlenmemiş olan veriler "GENEL" olarak sınıflandırılır.	Basın açıklamaları, genel duyurular, kurumsal web sayfaları, hizmet katalogları, tanıtım broşürleri vb.

5.2 Verinin Sınıflandırılmasına İlişkin Genel Kurallar

5.2.1 Kapsam dahilindeki tüm birimler verilerini bu prosedürdeki kriterlere göre sınıflandırırlar, verilerini sınıfına uygun şekilde işaretlerler. ÇOK GİZLİ belgelerin etiketlenmesi gereklidir.

5.2.2 Verinin işlenmesi, aktarımı, depolanması ve imhası esnasında veri sınıflandırması dikkate alınır.

5.2.3 Sınıflandırmada bir değişim ihtiyacı doğduğunda, veri sahibi yeni sınıflandırmasını belirler ve bu değişimden etkilenecek birimleri / kişileri bilgilendirir. Veri kataloğunun güncellenmesi için de BT Direktörlüğü'ne talepte bulunur.

5.2.4 Verilerin saklandığı ortamda birden fazla gizlilik sınıfında veri bulunması durumunda en kritik seviyedeki gizlilik sınıfı için geçerli olan kurallar uygulanır.

5.2.5 Birim yöneticileri, çalışanlarının, çalışmaya konu olan verilerin nasıl sınıflandırılacağı konusunda yol gösterici olur, birimi tarafından oluşturulan verilerin sınıflandırıldığından emin olur.

5.3 Verinin Etiketlenmesine ve İşlenmesine İlişkin Genel Kurallar

5.3.1 Üniversite tarafından kullanılan verilerin etiketlenmesi bu verilerin gizliliğini ve korumasını sağlamak açısından çok önemlidir. "Çok Gizli" olarak sınıflandırılan bilgi varlıkları her zaman için etiketlenir.

5.3.2 Etiketlendirme işlemine hassasiyet gösterilmesi ve tüm ilgili personel tarafından benimsenmesi için Bilgi Güvenliği Ekibi çalışanları farkındalık çalışmaları ile bilgilendirir.

5.3.3 Etiketlendirme işleminin veri kaynağında nasıl yer alacağı genel olarak Veri Sahibinin kararı ile belirlenir.

5.3.4 Belgeler, E-posta veya elektronik bilgi notlarında (memorandum) etiketler "Konu" veya "Altbilgi" bölümünde bulunmalıdır.

5.3.5 Basılı doküman, Manyetik teyp, disket, CD-ROM, ses kaseti ve diğer depolama medyalarında ise etiketler açıkça görülecek şekilde konur.

5.3.6 Veri merkezinde bulunan tüm donanımlar gizli olarak kabul edilir ayrıca bir etiketlemeye gerek duyulmaz.

5.3.7 Sistem tarafından otomatik olarak etiketlenmemiş bir bilgi varlığının doğru sınıflandırmayla etiketlenmesinden son kullanıcı sorumludur.

5.3.8 GİZLİ - ÇOK GİZLİ bilgilerin istemci bilgisayarlar arasında dosya alışverişi (e-posta vb.) söz konusu olduğunda dosyalar şifrelenir, şifreli iletilen dosyaların açılması için alıcıya iletilecek

bilgiler (şifre vb.) iletiye kesinlikle dahil edilmez, ikinci bir kanaldan (sms vb. ile) doğrudan alıcısına iletilir.

5.3.9 GİZLİ - ÇOK GİZLİ bilgilerin taşınabilir depolama ortamları ile (örneğin; şifreli USB vb.) aktarımı söz konusu ise bu ortamların şifrelenmesi gerekmektedir. Aktarım işlemi tamamlandıktan sonra gizli bilgiler uygun şekilde bu taşınabilir ortamdan silinir.

5.3.10 GİZLİ - ÇOK GİZLİ bilginin (kağıt, CD/DVD, bilgisayar vb. gibi) fiziksel ortamda aktarımı ile ilgili kurallar aşağıda belirtilmiştir:

5.3.11 Aktarımı gerçekleştirecek olan yetkili personel Üniversite dışında bir üçüncü taraf ise, bağlayıcı sözleşme maddeleri arasında, taşıyıcının sorumlulukları ve taşıyıcıdan gizlilik konusunda beklentiler yer alır.

5.3.12 Gönderen taraf, aktarılan bilgi varlığının alıcının eline geçip geçmediğini kontrol eder (örneğin; telefon ile teyit alınır), teyit edilememesi durumunda olayın takibi için yöneticine haber verir.

5.3.13 Aktarılan bilgi varlığının gerçek alıcısından önce açılmadığının bilinmesi amacıyla kapak kısmı imzalanarak kuryeye teslim edilir. Aktarımların dolaylı yollarla, elden ele teslimat şeklinde değil, bir seferde gönderenden alıcıya ulaşacak şekilde gerçekleşmesi esastır.

5.3.14 Bilgi varlıklarının imha edilmesi veya saklanmasına devam edilmesi kararı arşiv prosedürüne ve BT Donanım Hurda Hibe Sürecine göre yapılmaktadır.

5.3.15 Çalınma ve bilgisayara fiziksel olarak yetkisiz kişilerin erişebilmesi riskine karşı taşınabilir bilgisayarların diskleri şifrelenmelidir. ÇOK GİZLİ bilgiler, taşınabilir bilgisayarlarda tutulmamalı, Üniversite tarafından sağlanacak olan merkezi sunucularda tutulmalıdır.

5.3.16 ÇOK GİZLİ bilgi içeren fiziksel bir bilgi varlığının (örneğin; kâğıt, CD/DVD, bilgisayar vb.) depolanması ile ilgili kurallar aşağıda belirtilmiştir:

5.3.17 Basılı belgelerin depolanması ilgili birimin ihtiyaçlarına göre yapılır. Arşiv prosedürü kapsamına girenler bu prosedür doğrultusunda depolanacaktır.

5.3.18 Arşivlenmemiş fiziksel bilgi varlıkları ilgili birim tarafından kilitli ortamlarda saklanır.

5.3.19 Depolanan fiziksel bilgi varlıkları Fiziksel ve Çevresel Güvenlik Prosedürü'ne göre uygun fiziksel önlemler ile korunur.

5.3.20 Saklama gerektiren bilgi varlıklarının saklandığı ortamların kullanım ömrü dikkate alınarak önlem alınır.

5.3.21 Varlık sınıflandırmaları ve alınacak aksiyonları içeren kuralların açıklamaları aşağıdaki tabloda belirlenmiştir:

SINIF	AKSİYON
ÇOK GİZLİ	**Etiketlenmesi:** Varlık etiketlenmelidir. **Erişim:** Sadece görevi gereği onaylanmış erişim yetkisi bulunan kişiler erişebilir. Erişimler sadece güncelleme ve doğrulama amacı ile yapılabilmelidir. ÇOK GİZLİ varlıkların üzerinde çalışma yapılırken, bu varlıklara erişim yetkisi olduğundan emin olunmayan bir başka kişinin çalışma ortamına gelmesi durumunda, gelen kişinin erişimini veya görüşünü engelleyecek şekilde korunur. Bu ortamlar terk edilirken, geride hiçbir bilgi ve belge kalmayacak şekilde kontrol ve temizlik yapılır. ÇOK GİZLİ varlıkların aktarımından önce, bilgiyi talep edenin bu bilgiye erişim yetkisi bulunduğundan emin olunur. Erişim yetkisinin bulunduğunu belgelendirme sorumluluğu bilgiyi talep eden taraftadır. **Üniversite İçi Dağıtım:** Fiziki dokümanlar üzerinde çok gizli ibaresiyle zarflanarak veya özel zarfla ve tutanak tutularak elden teslim edilir. **Üniversite Dışı Dağıtım:** Fiziki dokümanlar üzerinde çok gizli ibaresiyle zarflanarak veya özel zarfla ve tutanak tutularak elden teslim edilir. **Elektronik Dağıtım:** Varlığın dağıtımı uygun değildir. Kurum içi ya da kurum dışından yapılacak amaca uygun erişimler güvenli kriptolama yöntemleri ile korunmalıdır. **Taşınması:** Üretim ortamından test ya da geliştirme ortamına taşınırken bu ortamlara ait anahtarlarla kriptolanmalı ve/veya şifrelenmelidir. **Depolama:** Varlıklar sürekli olarak kriptolu olarak saklanmalıdır. Üretim ortamına ait anahtarlar başka ortamlarda paylaşılmamalıdır. Kişi bazında erişim kontrolleri uygulanmalıdır. Varlığın saklandığı sistem Bilgi Güvenliği Yönergesine uymalıdır. ÇOK GİZLİ varlıkların kullanıldığı çalışmaların yürütüldüğü ortamda (örneğin; ofis ortamı, veri merkezi vb.) herhangi bir kayıt işlemi (örneğin; ses kaydı, görüntü kaydı, vb.) yapılamaz. Mevzuat ya da sözleşme yükümlülükleri ile belirlenmiş saklama sürelerine uyulur. **İmha Edilmesi:** Fiziki medya ve kağıtlar tekrar kullanılmayacak şekilde yok edilir. Fiziki medyanın tekrar kullanılmaması gereken durumlarda medya üzerindeki bilgi güvenli bir şekilde güvenli silme amaçlı programlar kullanılarak sıfırlanarak silinir. ÇOK GİZLİ bilgi içeren hiçbir varlık doğrudan çöpe atılmaz. İçerdiği bilginin yetkisiz kişilerce erişilebilir olmadığından emin olunur ve ilgili birim tarafından imha işlemi sonuna kadar takip edilir.

GİZLİ	**Etiketlenmesi:** GİZLİ bilgilerin kâğıt ortamına aktarıldığı durumlarda (örneğin; bordro listesi, şifre listesi vb.) doküman sayfalarının altına (sadece kapak sayfasında da belirtilebilir) veya uygun bir bölümüne GİZLİ ibaresi mühür, bilgisayar çıktısı veya el ile yazılır. GİZLİ bilgi içeren yedek kartuşları ve harici diskler üzerinde GİZLİ ifadesi taşıyan etiket yapıştırılmalıdır. Etiketleme zorunlu değildir. Sistem odalarında bulunan kaynaklarda saklanan varlıklar için fiziksel bir etiketleme gerekmemektedir. **Erişim:** Sadece görevi gereği onaylanmış erişim yetkisi bulunan çalışanlar tarafından erişilmelidir. GİZLİ varlıklar üzerinde çalışma yapılırken, bu varlıklara erişim yetkisi olduğundan emin olunmayan bir başka kişinin çalışma ortamına gelmesi durumunda, gelen kişinin erişimini veya görüşünü engelleyecek şekilde korunur. Bu ortamlar terk edilirken, geride hiçbir bilgi ve belge kalmayacak şekilde kontrol ve temizlik yapılır. GİZLİ varlıkların aktarımından önce, bilgiyi talep edenin bu bilgiye erişim yetkisi bulunduğundan emin olunur. Erişim yetkisinin bulunduğunu belgelendirme sorumluluğu bilgiyi talep eden taraftadır. **Üniversite İçi Dağıtım:** Üniversite içi e-posta sistemi ile ya da elden dağıtılmalıdır. **Üniversite Dışı Dağıtım:** Güvenli e-posta şifreleme yöntemleriyle şifrelenerek dağıtılmalıdır. **Elektronik Dağıtım:** Üniversite içi dağıtımda yetkisi olan çalışanlara gönderilmelidir. Üniversite dışına şifrelenmiş halde dağıtılmalıdır. Harici kurumlarla paylaşılması durumunda gerekli görülmesi durumunda Hukuk Müşavirliği birimince kanuni uygunluk şartı aranmalıdır. **Taşınması:** Üretim ortamından test ya da geliştirme ortamına taşınırken tutarlılığı bozulmayacak şekilde değiştirilmelidir. Değiştirme yöntemi varlık bazında ele alınmalı ve içeriğine, diğer varlıklarla ilişkisine bakılarak kararlaştırılmalıdır. **Depolama:** Kişi ya da rol bazlı erişim kontrolleri uygulanır. Varlığın saklandığı sistem Bilgi Güvenliği Yönergesi'ne uymalıdır. GİZLİ varlıkların kullanıldığı çalışmaların yürütüldüğü ortamda (örneğin; ofis ortamı, veri merkezi vb.) herhangi bir kayıt işlemi (örneğin; ses kaydı, görüntü kaydı vb.) yapılamaz. Mevzuat ya da sözleşme yükümlülükleri ile belirlenmiş silme/saklama kurallarına ve sürelerine uyulur. **İmha Edilmesi:** Fiziki medya ve kağıtlar tekrar kullanılmayacak şekilde yok edilir. Fiziki medyanın tekrar kullanılmaması gereken durumlarda medya üzerindeki bilgi güvenli bir şekilde güvenli silme amaçlı programlar kullanılarak sıfırlanarak silinir. GİZLİ bilgi içeren hiçbir varlık doğrudan çöpe atılmaz. İçerdiği bilginin yetkisiz kişilerce erişilebilir olmadığından emin olunur ve ilgili birim tarafından imha işlemi sonuna kadar takip edilir. KVKK kapsamında özel nitelikli hassas verilerin mevzuata uygun olarak yok edilmesi gerekir.
HİZMETE ÖZEL	**Etiketlenmesi:** HİZMETE ÖZEL varlıkların kâğıt ortamına aktarıldığı durumlarda doküman sayfalarının altına (sadece kapak sayfasında da belirtilebilir) veya uygun bir bölümüne HİZMETE ÖZEL ibaresi mühür, bilgisayar çıktısı veya el ile yazılır. Zorunlu değildir.

	Erişim: Üniversite içindeki tüm kullanıcılar tarafından erişilebilir. Üniversite dışından sadece işin mahiyetine göre gerekli durumlarda ilgili kişi ve kurumlarla, kontrollü olarak paylaşılabilir. **Üniversite İçi Dağıtım:** Üniversite içi e-posta sistemi ile ya da elden dağıtılmalıdır. **Üniversite Dışı Dağıtım**: Güvenli e-posta şifreleme yöntemleriyle şifrelenerek dağıtılması önerilir. **Elektronik Dağıtım:** Üniversite içi için herhangi bir kısıt yoktur, ancak Üniversite dışına şifrelenmiş halde dağıtılması önerilir. **Taşınması:** Üniversite içinde herhangi bir kısıt yoktur. **Depolama:** Üniversite içinde varlığa erişim için kontrol uygulanmasına gerek yoktur. Varlığın saklandığı sistem Bilgi Güvenliği Yönergesi 'ne uymalıdır. Üniversite dışında sadece belirlenen kişiler erişebilecek şekilde kişi ya da rol bazlı erişim kontrolleri uygulanır. **İmha Edilmesi:** Fiziki medya ve kağıtlar tekrar kullanılmayacak şekilde yok edilir. Fiziki medyanın tekrar kullanılması gereken durumlarda medya üzerindeki bilgi güvenli bir şekilde sıfırlanarak silinir.
GENEL	**Etiketlenmesi:** Etiketlenmesine gerek yoktur. GENEL olarak sınıflandırılmış varlıklara fiziksel veya mantıksal etiketleme yapılması mecburi olmayıp ihtiyaç ve isteğe bağlıdır. **Erişim:** Herhangi bir kısıt yoktur. **Üniversite İçi Dağıtım:** Herhangi bir kısıt yoktur. **Üniversite Dışı Dağıtım:** Herhangi bir kısıt yoktur. **Elektronik Dağıtım:** Herhangi bir kısıt yoktur. **Taşınması:** Herhangi bir kısıt yoktur. **Depolama:** Herhangi bir kısıt yoktur. **İmha Edilmesi:** Herhangi bir kısıt yoktur.

5.4 Bakım, Onarım ve Devre Dışı Bırakma Kuralları

5.4.1 Bilgi içeren sistemlerin ve depolama ortamlarının bakımı, onarımı ve devre dışı bırakılması sırasında uyulması gereken kurallar aşağıdaki gibidir:

5.4.2 3. taraflarca yapılacak olan bakım ve onarım işlemlerinde bakım veya onarımı yapılacak sistemden ÇOK GİZLİ bilgi varlıkları ayrılarak saklanır.

5.4.3 Bunun mümkün olmadığı durumlarda bakım işlemi ÇOK GİZLİ bilgi varlıklarına erişim yetkisine sahip bir çalışanın gözetiminde yapılmalı ve sistemden bilgilerin alınmasına engel olacak önlemler alınmalıdır.

5.4.4 Depolama ortamının kendisi (örneğin; sabit disk) bakım, onarım gibi amaçlarla kurum dışına çıkarıldığı durumlarda bakım, onarım çalışması yapacak firma ile gizlilik sözleşmesi düzenlenmelidir.

5.4.5 Çalışanların kendi kullandıkları cihazları satın alması da devre dışı bırakma olarak değerlendirilip, bu durumda cihazın diskinin teslim edilmemesi veya önce cihazın iade edilerek sıfırlanması (minimum 7 defa, disk üzerine random şekilde 0 ve 1ler yazılarak wipe işlemi uygulanması) sonrasında çalışana teslim edilmesi gerekmektedir.

8. EKLER VE KAYITLAR

Yoktur.

9. GÖZDEN GEÇİRME

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu BT Direktörlüğü'ne aittir. Gözden geçirme en az yılda 1 defa yapılır. Gerekli görüldüğü zaman ve durumlarda doküman revize edilir.

10. DEĞİŞİKLİK/DAĞITIM TABLOSU

Değişen sayfa	Tarih	Değişiklik	Değişikliği yapan
4	09.06.2022	Gizli ve Çok gizli tanımlamaları düzenlenmiştir.	Derya Erhan
5	09.06.2022	Kurum içi tanımı silinmiş, hizmete özel tanımı eklenmiştir.	Derya Erhan
Dağıtım (İlgili Bölümler)			
Tüm Koç Üniversitesi			