İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

VARLIK YÖNETİMİ PROSEDÜRÜ (VYP)

HAZIRLAYANLAR	KONTROL EDEN	ONAYLAYAN
Ufuk Dikme		
Bilgi Güvenliği Yönetim Müdürü	Bilgi Sistemleri ve Teknolojileri Daire Başkanı	Genel Sekreterlik Temsilcisi

Doküman Kod	IKU-BSTDB-VYP-001	Revizyon Tarihi	
Yayın Tarihi	24.03.2021	Revizyon No	VYP-001-1.0

İÇİNDEKİLER

1. AMAÇ

Bu doküman, İstanbul Kültür Üniversitesi bilgi varlıklarının tanımlanması, sahipliklerinin belirlenmesi ve varlıkların kritikliğinin saptanması için nasıl bir yöntem izlenmesi gerektiğini tanımlar.

2. KAPSAM

Bu politikada bahsi geçen varlık yönetimi faaliyetleri, Bilgi Güvenliği Kapsamı dokümanında belirtilen tüm varlıklara ve kurum ile üçüncü taraf anlaşması imzalamış herhangi bir dış tarafa ait varlığa uygulanır.

3. TANIMLAR VE KISALTMALAR

KISALTMALAR	TANIMLAR
PAYDAŞ	Kurum bünyesinde yürütülen faaliyetlerden olumlu veya olumsuz bir şekilde doğrudan veya dolaylı bir şekilde etkilenecek kurumlar, gruplar veya kişilerdir.
ÜÇÜNCÜ TARAF	Kuruma sözleşme ile hizmet sağlayan tüzel kişiler ve personelleri.
PERSONEL	Kurumda çalışan memuru ve/veya sözleşmeli personeli.
BİLGİ GÜVENLİĞİ	Kurum varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunması.
BGYS	Bilgi Güvenliği Yönetim Sistemi.
VARLIK	Kurum için değerli olan ve bu nedenle uygun şekilde korunması gereken unsurlardır.
VERİ (DATA)	Birbiri ile ilişkilendirilmemiş kayıt alanları (field) veya kayıtlardır (record).
ENFORMASYON (MALÛMAT, İNFORMATİON):	İşlenmiş veya bir dizi işlem / uygulama ile anlam kazanmış verilerdir. Günlük uçak / otobüs hareket planları, uçak / otobüs yolcu listeleri gibi.
BİLGİ (KNOWLEDGE)	Değer kazanmış enformasyondur ve enformasyonun bir veya birkaç amaca yönelik olarak bir araya getirilmesidir. Bir ay içinde kaç sefer yapılmış, toplam kaç yolcu taşınmış, yüzde kaç doluluk oranı sağlanmış gibi.

4. UYGULAMA

4.1. Varlık Envanterinin Oluşturulması

4.1.1. Varlıkların Belirlenmesi

- İstanbul Kültür Üniversitesinde, BT hizmetlerinin verildiği varlıklar, Bilgi Güvenliği Koordinatörü ve BGYS Ekibinin desteği ile belirlenir.

- BGYS Ekibi, varlıkların belirlenmesi amacıyla ilk olarak kapsam dâhilindeki fonksiyonel işlemleri ve/veya iş süreçlerini inceler. Bu inceleme sırasında faaliyet sahipleri ve/veya süreç sorumluları ile birebir görüşme yapar, ilgili dokümantasyonları inceler veya otomatik tarama araçları kullanır.

4.1.2. Varlıkların Sahipliği

- İstanbul Kültür Üniversitesindeki, kapsam dahilinde yer alan varlıkların sahibi ve emanetçisi (kullanıcısı/ sorumlusu) tanımlanır.
- İlgili varlık sahip ve emanetçisi "Varlık Envanteri Listesi" içinde belirtilir.

Varlık sahipliği ile ilgili dikkat edilmesi gereken iki kavram aşağıda tanımlanmıştır.

Varlık sahipliği: Varlıkla ilgili karar verme yetkisi olan, üzerinde uygulanmakta olan güvenlik kontrollerine karar veren veya uygulanmasını sağlayan kişidir. Varlıklarla ilgili karar verme yetkisine sahip olması sebebiyle varlık bilgilerini bu kişi sağlar.

NOT: Varlık sahipliği, mülkiyet anlamında sahiplik değildir.

Görevleri:

- Varlığın üretiminden, geliştirilmesinden, kullanılmasından, bakımından ve varlık üzerindeki güvenlik kontrollerinin gerçekleştirilmesinden sorumludur.
- Bilginin bütünlüğü, gizliliği ve erişilebilirliğinin sağlanması için gereken şartları tanımlar.
- Varlık için uygun fiziksel ve mantıksal güvenlik seviyelerini belirler.
- Varlığın, erişilebilir olmasını sağlar. Erişilebilirlik toleranslarını belirler.
- Uygulanabilir erişim kontrol politikalarını göz önünde bulundurarak erişim kısıtlamalarını tanımlar ve periyodik olarak gözden geçirir.
- Verilerin yedekleme/geri dönüş programlarını tanımlar, yedekleme/geri dönüş test sonuçlarını ve geri dönüş sonrasındaki verinin bütünlüğünü periyodik olarak gözden geçirir.

Varlık Emanetçisi (Kullanıcısı / sorumlusu): Varlığın işletilmesi ve korunması işlemlerini gerçekleştiren kişidir.

Bu kavramlar aşağıdaki örnek senaryo ile açıklanmıştır:

1. Veri tabanı yönetim sisteminin (Oracle, MsSQL vs) sahibi veri tabanı yönetim ekibidir.
2. Veri tabanı içerisinde yer alan veriler ise iş süreci sahibinindir.
3. Buna göre veri tabanında yer alan "proje finansal bilgisi" verisinin sahibi Finans Uzmanı'dır ve veriye ilişkin değerlendirmeleri bu uzman yapar.
4. Veri tabanına veri ekleyen, değiştiren, silen, sorgulayan, raporlayan kişi ise varlık emanetçisidir.

Görevleri:

- Varlık sahibi tarafından belirlenmiş kontrolleri uygulayarak, varlığı korumakla yükümlüdür.
- Veriyi / bilgiyi paylaşmadan önce sahibinden izin alır.
- Düzenli olarak yedekleme faaliyetlerini gerçekleştirir.
- Varlık sahibi tarafından tanımlanmış olan erişim kontrollerini uygular.

4.2. Varlıkların Gruplanması ve Sınıflandırılması

4.2.1. Varlıkların Gruplanması

- Veri, kurum için değeri olan ve sayısal/basılı olarak saklanabilen, tanımlanabilir bilgi parçasıdır.
- Verinin tutulduğu, iletildiği, üretildiği, işlendiği, saklandığı, paylaşıldığı ortamlar / yapılar / cihazlar bilgi varlıklarıdır.
- Veriye örnek olarak veri tabanı kayıtları, kaynak kodlar, görüntüler, sayısal dokümanlar, müşteri bilgileri, planlar, finansal kayıtlar, sözleşmeler verilebilir.
- Bilgi varlıklarına örnek olarak veri tabanı ortamları, e-posta sunucuları, yedekleme üniteleri, yazılımlar, ağlar, internet hatları verilebilir.
- Bilgi varlıkları fiziksel veya sayısal olabilir. Fiziksel bilgi varlıkları, bilginin oluşturulmasında, işlenmesinde, iletilmesinde, çıktı elde edilmesinde ve saklanmasında esas rolü oynayan varlıklardır.
- Altyapı (destek) varlıkları ise bilgi ve bilgi işlem ortamlarının sürekliliğini, güvenliğini sağlayan varlıklardır. Enerji destek üniteleri, iklimlendirme sistemleri, uyarı sistemleri, izleme ve kayıt sistemleri örnek olarak verilebilir.

İstanbul Kültür Üniversitesinin varlıkları aşağıda listelenen başlıklar altında gruplanır:

Basılı Bilgiler: İstanbul Kültür Üniversitesi için kurumsal değere sahip olan, basılı olarak saklanan iç/dış yazışmalar, sözleşmeler, resmi yazılar, personel özlük dosyaları, kriptografik anahtarlar, şifreler, sistem parolaları, bunların tutulduğu fiziksel ortamlar vb. unsurlardır.

Sayısal Bilgiler: İstanbul Kültür Üniversitesi için kurumsal değere sahip olan, sayısal olarak oluşturulan ve saklanan iş süreç belgeleri, raporlar, kriptografik anahtarlar, şifreler, sistem parolaları, bunların tutulduğu elektronik ortamlar, sorgular, politikalar, yönergeler, esaslar, e-posta yazışmaları vb. unsurlardır.

Kurumsal Uygulamalar: İstanbul Kültür Üniversitesindeki iş süreçlerinin yürütülmesi amacıyla kullanılan, başka kurumlar / firmalar tarafından geliştirilen, işletilen ya da İstanbul Kültür Üniversitesi tarafından geliştirilen, geliştirilmesi ihale edilen yazılım varlıklarıdır.

Lisanslı Uygulamalar: İstanbul Kültür Üniversitesinde bilgi işleme amacıyla kullanılan tüm paket programlar, kullanıcı işletim sistemleri vb. varlıklarıdır.

Kaynak Kodlar: Kurum tarafından iç/dış kaynaklar kullanılarak geliştirilen uygulamalara ait kodlardır.

Veri Tabanı Yönetim Sistemleri: İstanbul Kültür Üniversitesinin yürüttüğü hizmetleri sunabilmek için, sistematik erişim imkânı olan, yönetilebilir, güncellenebilir, birbirleri arasında tanımlı ilişkiler bulunabilen veri kümeleri uygulamalarıdır.

Sunucular: İstanbul Kültür Üniversitesinin sorumluluğundaki farklı konumlarda bulunan değişik rollerin yüklü olduğu fiziksel ve sanal sunucuları içerir. Örnek: Etki alanı, e-posta sunucusu, web sunucusu, sanallaştırma sunucuları, güvenlik sunucuları, ağ yönetimi izleme sunucuları, sistem yönetim sunucuları vb.

Depolama Üniteleri: İstanbul Kültür Üniversitesi bünyesinde bulunan verileri/bilgileri depolamak için kullanılan kurumsal depolama aygıtlarıdır. Örneğin: sunucu üzerindeki disk ünitesi, storage üniteleri, yedekleme kartuşları, taşınabilir diskler vb.

Ağ Cihazları: Ağ hizmetlerini sunmak için İstanbul Kültür Üniversitesi bünyesinde kullanılan aktif ve pasif cihazlar ile ağ altyapısında kullanılan diğer ekipman (pach panel, hub, access point, vb.) ağ cihazları başlığı altına toplanır.

Güvenlik Cihazları: Kurumda bulunan bilgilerin gizliliği, bütünlüğü ve devamlılığını sağlamak amacıyla konumlandırılmış cihaz ve uygulamalardır. Güvenlik Duvarı, yük dengeleyiciler, Saldırı Önleme Sistemi, SIEM cihazları gibi.

Kullanıcı Bilgisayarları: Kurum personeli ve 3.tarafların günlük işlerini yürütmek için kullandıkları kişisel masaüstü ve dizüstü bilgisayarlardır. Bilgisayarlar farklı konumlarda sabit veya mobil olarak kullanılabilir.

Çevre Birimleri: Kurum veya 3. Taraf personel tarafından kullanılan yazıcı, tarayıcı, faks cihazı, fotokopi makinesi veya personele çeşitli hizmetler vermesi amacıyla bulundurulan telefon santrali, konferans görüşme sistemi vb. dir.

Altyapı (destek): Kurumda bulunan ve bilgi teknolojileri cihazlarının sağlıklı bir şekilde çalışabilmesi ve diğer birimlere hizmet verebilmesi için ihtiyaç duyduğu sistemler bütünüdür. Elektrik sistemi: jeneratör, kesintisiz güç kaynağı, pano, sigorta, elektriksel kablolama, sistem odası iklimlendirme sistemleri, sistem odası yangın algılama ve gazlı söndürme sistemi, yangın söndürücüler, güvenlik kameraları, giriş kontrol sistemleri vb.

Binalar / odalar: BSTDB, destek hizmetlerinin, kurum açısından kritikliği olan çalışma ortamlarıdır. Arşiv odaları, muhasebe departmanı, sistem odası, UPS odası, santral odası, giriş / çıkış kontrol noktaları gibi.

Diğer: Yukarıda tanımlanan kategorilere girmeyen varlıklar bu başlık altında toplanır. Ör: Kartuş kasası, projeksiyon cihazı, büyük ekranlar, akıllı tahta vb.

4.2.2. Bilgilerin Sınıflandırılması

Koruyucu / caydırıcı önlemlerin alınabilmesi amacıyla bilgiler değerine, yasal gereksinimlere, hassasiyetine ve kritikliğine göre sınıflandırılır.

İstanbul Kültür Üniversitesinde, varlık sahipleri aşağıda tanımlanan dereceleri kullanarak bilgileri sınıflandırır. Bilgilerin sınıflandırmasında yalnızca basılı bilgiler, elektronik / sayısal bilgiler ve kaynak kodlar değerlendirilir.

Bilgi sınıflandırma, üç parametreye göre yapılır.

a) Gizlilik,
b) Bütünlük (Tahrifat, Değiştirme)
c) Saklama süreleri

Gizlilik niteliğine göre:

Herkese Açık: Halka açık bilgilerdir. Bilgiye herhangi bir kişinin erişmesi, kurum dışına çıkması kurum için bir kayıp/zarar oluşturmaz. Örneğin, vizyon, misyon, kurumsal duyurular, kurumsal faaliyetler gibi.

Kuruma özel: Kurumun geneline açık olan bilgilerdir. Başka kaynaklar üzerinden de erişilebilirdir. Kurum içi genel duyurular, genel yazışmalar, dönemsel bildirimler (yaz kıyafeti, servis hareket noktaları vs.), kurum telefon rehberi, toplanma alanları, yönlendirme levhalarını içeren bilgiler, acil durum görev tanımları gibi.

Tahrifat veya değişiklik kurum içi hizmetlerde sorun oluşturabilir. Ancak herhangi bir kayıp oluşturmaz.

Hizmete Özel: Bilginin kurum içinde birim haricinde paylaşılması veya kurum dışına çıkması durumunda göz ardı edilebilir düzeyde kayıp/sıkıntı yaşanabilir. Bilginin ifşası kuruma ciddi bir zarar vermez, bilgiye erişim kurum içerisindeki belirli çalışanlara açıktır. Teknik servis kataloğu, organizasyon şeması, süreç bilgileri, bölüm / birim bilgileri gibi.

Gizli: Bilginin kurum dışına çıkması durumunda ciddi kayıplar/zararlar oluşabilir. Bilginin tehlikeye atılması yasal ve mevzuata uygunsuzluk yaratır. Bilgiye erişim "bilmesi gereken ilkesi" ne uygun olarak kısıtlanmalıdır. Proje raporları, proje değerlendirme raporları, detaylı topoloji vb.

Fiziksel tahrifat kurumu yasal olarak zor duruma düşürebilir.

Çok gizli (sır): Bilginin kurum dışına çıkması durumunda çok ciddi büyüklükte kayıplara, zararlara ve imaj kaybına yol açabilir. Proje finansal bilgileri, Kurum ile ilgili davaların bilgileri, etki alanı yöneticisi şifresi vb.

Kişiye özel bilgiler çok gizli sınıfında değerlendirilir. Kurumda çalışan, kuruma hizmet veren tedarikçi çalışanlarının özel bilgileridir. Bilginin kurum dışına çıkması / kurum içinde paylaşılması, yayılması yasal ve mevzuata aykırı uygunsuzluk yaratabilir. Örnek: Çalışan maaş bilgileri, hastalık / tahlil sonuçları, mahkeme ilamları gibi.

Bütünlük (tahrifat & değiştirme)

Çok düşük (ihmal edilebilir): Tahrifat (silinme, yanma, okunmaz hale gelme vs.) veya değiştirme kurumsal işleyişte sorun oluşturmaz. Bir kaydın kökeni ve doğruluğunu gösteren hiçbir sistematik denetim veya tanımlanmış sürece gerek yoktur.

Çeşitli kurumsal fonksiyonlara uygun olarak özgünlük ve gözetim zincirini kullanmaya gerek yoktur.

Güvenirliğinin doğrulanmasına gerek yoktur.

Düşük: Tahrifat (silinme, yanma, okunmaz hale gelme vs.) veya değişiklik kurum içi hizmetlerde sorun oluşturabilir. Ancak herhangi bir kayıp oluşturmaz.

Bazı kurumsal kayıtların saklanması gerekebilir. Ancak resmi bir süreç, saklama ve sorumluluk gerektirmez. Bilginin kimin tarafından üretildiği, ne zaman üretildiği, hangi kategorilere ait olduğu meta veri yapısı mevcuttur.

Veri, bilgiler metada bilgileri ile yedekleme veya saklama yöntemlerine tabi tutulabilir. Ancak saklama süreleri gibi hususlar departmanlara bırakılmıştır.

Orta: Tahrifat (silinme, yanma, okunmaz hale gelme vs.) veya değişiklik hizmeti etkileyebilir. İçerdiği konular itibarıyla diğer gizlilik dereceli konular dışında olan ancak güvenlik işlemine ihtiyaç gösteren evrak, belge, doküman ve bilgiler Hizmete Özel bilgidir.

Kurumsa bilgilerin gerekli düzeyde sistem ve süreçlerin gereksinimlerini karşılayabilmek için bilginin değiştirilemezliğini ve bunun için gözetim zincirlerini sağlamak üzere resmi bir süreç vardır.

Kurumsal verilerin / bilgilerin bütünlüğü ile ilgili özel hedefler belirlemiştir. Logların tutulması gibi.

Yüksek: Fiziksel tahrifat (silinme, yanma, okunmaz hale gelme vs.) kurumu yasal olarak zor duruma düşürebilir.

Değişiklik kurumsal bilgi ve hizmeti etkiler. Değişiklikler kontrol altında tutulmalıdır. Paylaşımlarda kriptografik kontroller uygulanabilir. Kayıtların doğruluğunu sağlamak için gerekli tüm sistemler, iş uygulamaları ve elektronik ortamlar için meta veri gereksinimleri açıkça tanımlanmalıdır. Meta veri tanımlama süreci organizasyon kayıt yönetimi uygulamalarının ayrılmaz bir parçasıdır.

Orijinalliğini göstermek için gerektiği gibi güvenlik ve imza gereksinimleri ve gözetim zincirine ihtiyaç vardır. İnkâr edilemezlik karşılanmalıdır. (E-imza)

Çok yüksek: Fiziksel tahrifat kurumu yasal olarak zor duruma düşürür. Mutlaka fiziksel olarak uygun şartlar altında korunmalıdır.

Değişiklik kurumsal bilgi ve hizmeti etkiler. Değişiklikler kontrol altında tutulmalıdır. Paylaşımlarda kriptografik kontroller uygulanmalıdır.

Yeni kayıt üreten sistemler / meta veri ve sorumluluk zinciri dahil olmak üzere tüm değiştirilemezlik gereksinimleri için resmi tanımlanmış bir süreç olmalıdır. Değiştirme işleyişi düzenli olarak

denetlenmelidir. Organizasyon sürekli ve güvenilir olarak kayıtların doğruluğunu ve güvenilirliğini gösterebilmelidir.

Saklama Sürelerine göre:

Çok düşük (İhmal edilebilir): Kurum çalışma şartlarına veya yasal sürelere göre 1 (bir) yıldan fazla saklama ihtiyacı olmayan bilgiler veya saklama süresi olmayan anonim bilgiler

Düşük: Kurum şartlarına veya yasal sürelere göre 1-3 yıl saklanması gereken bilgiler

Orta: Kurum şartlarına veya yasal sürelere göre 3-5 yıl saklanması gereken bilgiler

Yüksek: Kurum şartlarına veya yasal sürelere göre 5-0 yıl saklanması gereken bilgiler

Çok yüksek: Kurum şartlarına veya yasal sürelere göre süresiz saklanması gereken bilgiler

4.2.3. Varlık Değerinin Belirlenmesi

Bilginin değeri, bilginin bulunduğu bilgi varlıklarının değerini belirler. Risk değerlendirme sürecinde varlıkların sayısal değerine gereksinim varsa, varlığın üzerinde yer alan bilginin en yüksek değeri ile belirlenir.

Bilgi veya Destek Varlığın İş Sürekliliği açısından Erişilebilirlik Değeri.

Bilgi veya destek varlıklarının erişilebilirlik değeri, bir kısmi veya tam kesinti veya felaket durumunda o varlığa olan ihtiyaç veya bağımlılık halidir.

Çok düşük (ihmal edilebilir): Bilgilere 2 hafta veya daha fazla erişilemediği durumda kurum iş süreçleri çok az etkilenir. Örnek: Kalite Yönetim Sistemi. Herhangi bir şekilde kâğıt veya başka ara yüzlerle işleyiş sürdürülebilir.

Düşük: Bilgilere 1-2 hafta boyunca erişilemediği durumda kurum iş süreçleri az etkilenir. Örnek: kurumsal duyuruların yer aldığı portal. Farklı arayüz ve faaliyetlerle kurumsal işleyiş devam edebilir.

Orta: Bilgi veya destek varlıklarına 2-7 gün boyunca erişilemediği durumda kurum iş süreçleri etkilenir. Örnek: dosya sunucuları. Yerel ağ içinde ağ anahtarları.

Yüksek: Bilgi veya destek varlıklarına 1 gün boyunca erişilemediği durumda kurum iş süreçleri ciddi şekilde etkilenir. Örnek: e-posta uygulamaları / sunucuları. Yük dengeleyiciler, ERP uygulamaları / sunucuları. Hizmet kısmi olarak önceliği olan alanlarda verilir. FKM'den hizmet sürdürülebilir.

Çok yüksek: Varlıklar 7x24 erişilebilir olmalıdır. Aksi halde kurum iş süreçleri çok ciddi etkilenir. Örnek: DC, storage sistemler, internet altyapısı, elektrik altyapısı.

Bilgi Değerlendirme Kriterleri	Çok Düşük 1	Düşük 2	Orta 3	Yüksek 4	Çok Yüksek 5
Gizlilik	**Anonim:** Halka açık hassas olmayan bilgilerdir. Bu bilgilerin yetkisiz açıklanması kurumu etkilemez. Örnek: basın bültenleri, kurum web sitesinde halka açık yayınlanan bilgiler ve duyurular vb.	**Hizmete özel:** Hassas olmayan bilgilerdir. Başka kaynaklar üzerinden de erişilebilirdir. Kurum içi genel duyurular, genel yazışmalar, dönemsel bildirimler (yaz kıyafeti, servis hareket noktaları vb.)	**Özel:** Kuruma ait olan ancak halkın veya dış tarafların erişimine açık olmayan bilgilerdir. Bu bilgilerin yetkisiz açıklanması kuruma sınırlı şekilde zarar verebilir. Ör: Proje raporları, sözleşmeler vb.	**Gizli:** Kurum içi yüksek değerdeki hassas ve özel bilgilerdir. Sadece belirlenmiş kişilerin kullanımına açıktır. Bu bilgilerin yetkisiz açıklanması kuruma ciddi zarar verebilir (yasal veya mali yükümlülük, itibar ve güven kaybı vb.) Ör: detaylı topoloji, denetim raporları, proje finansal bilgileri, kurul kararları vb.	**Çok Gizli (Sır):** Kurumun en önemli ve özel bilgileridir. Sadece belirlenmiş kişilerin kullanımına açıktır. Bu bilgilerin yetkisiz açıklanması kuruma çok ciddi zarar verebilir (Kurum yetkililerine adli soruşturma, maddi cezalar) Ör: Hukuk davası dokümanları, veri tabanları, yüksek yetkili şifreler vb. Kişiye özel bilgiler.

Bilgi Değerlendirme Kriterleri	Çok Düşük 1	Düşük 2	Orta 3	Yüksek 4	Çok Yüksek 5
Tahrifat & Değiştirme (Bütünlük)	Tahrifat (silinme, yanma, okunmaz hale gelme vs.) veya değiştirme kurumsal işleyişte sorun oluşturmaz. Bir kaydın kökeni ve doğruluğunu gösteren hiçbir sistematik denetim veya tanımlanmış sürece gerek yoktur. Çeşitli kurumsal fonksiyonlara uygun olarak özgünlük ve gözetim zincirini kullanmaya gerek yoktur. Güvenirliğinin doğrulanmasına gerek yoktur.	Tahrifat (silinme, yanma, okunmaz hale gelme vs.) veya değişiklik kurum içi hizmetlerde sorun oluşturabilir. Ancak herhangi bir kayıp oluşturmaz. Bazı kurumsal kayıtların saklanması gerekebilir. Ancak resmi bir süreç, saklama ve sorumluluk gerektirmez. Bilginin kimin tarafından üretildiği, ne zaman üretildiği, hangi kategorilere ait olduğu metadata yapısı mevcuttur. Veri, bilgiler metada bilgileri ile yedekleme veya saklama yöntemlerine tabi tutulabilir. Ancak saklama süreleri gibi hususlar departmanlara bırakılmıştır.	Tahrifat (silinme, yanma, okunmaz hale gelme vs.) veya değişiklik hizmeti etkileyebilir. İçerdiği konular itibarıyla diğer gizlilik dereceli konular dışında olan ancak güvenlik işlemine ihtiyaç gösteren evrak, belge, doküman ve bilgiler Hizmete Özel bilgidir. Kurumsa bilgilerin gerekli düzeyde sistem ve süreçlerin gereksinimlerini karşılayabilmek için bilginin değiştirilemezliğini ve bunun için gözetim zincirlerini sağlamak üzere resmi bir süreç vardır. Veri, bilgiler metada bilgileri ile yedekleme veya saklama yöntemlerine tabi tutulabilir. Ancak saklama süreleri gibi hususlar departmanlara bırakılmıştır.	Fiziksel tahrifat (silinme, yanma, okunmaz hale gelme vs.) kurumu yasal olarak zor duruma düşürebilir. Değişiklik kurumsal bilgi ve hizmeti etkiler. Değişiklikler kontrol altında tutulmalıdır. Paylaşımlarda kriptografik kontroller uygulanabilir. Kayıtların doğruluğunu sağlamak için gerekli tüm sistemler, iş uygulamaları ve elektronik ortamlar için metadata gereksinimleri açıkça tanımlanmalıdır. Metadata tanımlama süreci organizasyon kayıt yönetimi uygulamalarının ayrılmaz bir parçasıdır. Orijinalliğini göstermek için gerektiği gibi güvenlik ve imza gereksinimleri ve gözetim zincirine ihtiyaç vardır. İnkâr edilemezlik karşılanmalıdır. (E-imza)	Fiziksel tahrifat kurumu yasal olarak zor duruma düşürür. Mutlaka fiziksel olarak uygun şartlar altında korunmalıdır. Değişiklik kurumsal bilgi ve hizmeti etkiler. Değişiklikler kontrol altında tutulmalıdır. Paylaşımlarda kriptografik kontroller uygulanmalıdır. Yeni kayıt üreten sistemler / metadata ve sorumluluk zinciri dahil olmak üzere tüm değiştirilemezlik gereksinimleri için resmi tanımlanmış bir süreç olmalıdır. Değiştirme işleyişi düzenli olarak denetlenmelidir. Organizasyon sürekli ve güvenilir olarak kayıtların doğruluğunu ve güvenilirliğini gösterebilmelidir. (Log yönetimi-DLP uygulamaları) İnkar edilemezlik karşılanmalıdır. (E-imza)

Bilgi Değerlendirme Kriterleri	Çok Düşük 1	Düşük 2	Orta 3	Yüksek 4	Çok Yüksek 5
Saklama Süreleri	Kurum çalışma şartlarına veya yasal sürelere göre 1 (bir) yıldan fazla saklama ihtiyacı olmayan bilgiler veya saklama süresi olmayan anonim bilgiler.	Kurum şartlarına veya yasal sürelere göre 1-3 yıl saklanması gereken bilgiler.	Kurum şartlarına veya yasal sürelere göre 3-5 yıl saklanması gereken bilgiler.	Kurum şartlarına veya yasal sürelere göre 5-10 yıl saklanması gereken bilgiler.	Kurum şartlarına veya yasal sürelere göre 10 yıl veya üzeri veya süresiz saklanması gereken bilgiler.
Varlık Erişilebilirlik	Bilgilere 2 hafta veya daha fazla erişilemediği durumda kurum iş süreçleri çok az etkilenir. Örnek: Kalite Yönetim Sistemi. Herhangi bir şekilde kâğıt veya başka ara yüzlerle işleyiş sürdürülebilir.	Bilgilere 1-2 hafta boyunca erişilemediği durumda kurum iş süreçleri az etkilenir. Örnek: kurumsal duyuruların yer aldığı portal. Farklı arayüz ve faaliyetlerle kurumsal işleyiş devam edebilir.	Bilgi veya destek varlıklarına 2-7 gün boyunca erişilemediği durumda kurum iş süreçleri etkilenir. Örnek: dosya sunucuları. Yerel ağ içinde ağ anahtarları.	Bilgi veya destek varlıklarına 1 gün boyunca erişilemediği durumda kurum iş süreçleri ciddi şekilde etkilenir. Örnek: e-posta uygulamaları / sunucuları. Yük dengeleyiciler, ERP uygulamaları / sunucuları. Hizmet kısmi olarak önceliği olan alanlarda verilir. FKM'den hizmet sürdürülebilir.	Varlıklar 7x24 erişilebilir olmalıdır. Aksi halde kurum iş süreçleri çok ciddi etkilenir. Örnek: DC, storage sistemler, internet altyapısı, elektrik altyapısı

4.3. Varlıkların Etiketlenmesi

İstanbul Kültür Üniversitesinde, değerine, yasal gereksinimlere, hassasiyetine ve kritikliğine göre sınıflandırılan varlıklar aşağıdaki yöntemlere göre etiketlenir:

Basılı bilgiler: Basılı bilgi gizlilik değeri taşıyorsa, gizlilik derecesi "Gizlilik Sınıfı" içinde "Çok Gizli" ve "Gizli" olarak tanımlanan derecelere göre kaşe ile belirtilir.

Sayısal bilgiler: Sayısal bilgi, gizlilik değeri "Çok Gizli" ve "Gizli" olarak tanımlanan derecelere göre doküman adının başına sırasıyla "G5" ve "G4" ifadeleri konularak işaretlenir.

Uygulamalar: Uygulama ve uygulama yoluyla ulaşılabilen bilgiler gizlilik değeri taşıyorsa, gizlilik derecesi "Varlıkların Sınıflandırılması" başlığında tanımlanan derecelere göre, destekleniyorsa kullanıcı ara yüzüne girişte veya ara yüzde bulunulduğu sırada uyarı olarak çıkacak şekilde belirtilir.

Veri tabanları: Veri tabanı içerisindeki bilgiler gizlilik değeri taşıyorsa, gizlilik derecesi "Varlıkların Sınıflandırılması" başlığında tanımlanan derecelere göre, verilere erişim sağlanan yönetim ara yüzüne veya uygulama ara yüzüne girişte veya ara yüzde bulunulduğu sırada uyarı olarak çıkacak şekilde belirtilir.

Sunucular/Ağ ve Güvenlik Cihazları: Sunucu/Ağ ve Güvenlik Cihazı gizlilik değeri taşıyorsa, gizlilik derecesi "Erişilebilirlik" değerinde tanımlanan derecelere göre sunucu/ağ ve güvenlik cihazları üstüne "Uyarı" ile belirtilir.

Fiziksel Varlıklar: Fiziksel varlıklar herhangi bir sınıflandırma sınıfına bağlı olmaksızın etiketlenir. Etiketleme kuralı: Kod- Bulunduğu Yer- Cihaz Tanımı- Cihaz Türü- Sıra No. Kod sırasına göre "Varlık Envanter Listesi" üzerinde kayıt altına alınır.

Altyapı, çevre birimleri, kullanıcı bilgisayarları: İstanbul Kültür Üniversitesinin demirbaş kayıt yönetimi şartlarına göre etiketlenir.

Bina-Odalar: Bina yerleşim tablosundaki adresleme yapısına göre etiketlenir.

4.4. Varlık Envanteri Yönetimi

Varlık sahipleri, farklı araçlar ile otomatik veya elle toplanan varlık bilgilerini BGYS Ekibi'ne iletir ve ekip bu bilgileri **Varlık Envanteri Listesi** üzerine işler. Toplanan verileri BGYS Ekibi tarafından periyodik olarak gözden geçirilir ve düzenlenir.

Risklerin doğru hesaplanabilmesi için varlık envanteri listesi güncel olmalıdır. Eklenen, el değiştiren, imha edilen, taşınan veya içeriklerinde değişiklik olan varlıklar altı ayda bir (6 ay) varlık sahipleri tarafından kontrol edilir. Herhangi bir değişiklik durumunda varlık sahibi ilgili değişikliği BGYS Ekibine bildirir. BGYS Ekibi, **Varlık Envanteri** Listesi üzerinde ilgili güncellemeyi yapar.

Kurum bünyesine yeni giren varlıklar, varlık sahibi veya varlık emanetçisi tarafından varlık envanterine eklenmesi için BGYS Ekibine iletilir.

El değiştirecek varlıklar için (kullanıcı bilgisayarları, mobil cihazlar gibi) el değiştirme işlemi yapılmadan önce içerisindeki bilgiler silinir.

İçerisinde özel, gizli ve sır sınıfında bilgi bulunan bir ortam kullanıcı değiştirecekse, kullanılan ve kullanılmayan alanları da dâhil olacak şekilde, tüm ortam mutlaka güvenli olarak silinir/biçimlendirilir, üzerine veri yazılarak tekrar geri dönülmeyecek şekilde biçimlendirilir.

Kullanıcı bilgisayarları, mobil cihazlar gibi kullanıcılara zimmetli varlıklar Zimmet Yönetimi'ne tabi tutulur. İstanbul Kültür Üniversitesi herhangi bir şart olmadığı durumda sunucular, sistem ekipmanları, uygulamalar için zimmet uygulaması yapılmaz.

Varlık Envanter Listesinde yazılım ve fiziksel varlıklar için envantere giriş ve envanterden çıkış tarihleri ile gerekçeleri kaydedecek alanlar oluşturulur.

4.5. Varlıkların İmhası

İstanbul Kültür Üniversitesine ait, ekonomik ömrünü tamamlayan veya onarılamaz biçimde arızalanan cihazlar imha edilir.

Bu tip cihazlar üzerindeki veri depolama birimleri mümkünse önce yazılımsal olarak üzerine yazma yöntemi ile silinir sonrasında fiziksel olarak imha edilir ve demirbaş kaydından düşülür.

İş ihtiyaçları doğrultusunda taşınan, tamire gönderilen, bir başka kuruma hibe edilen veya kullanıcı profili değişen cihazlar, veri depolama birimlerinin üzerine yazma/silme yöntemi uygulanarak okunamaz hale getirilir.

Bilgi taşıyan varlık, lisanslı bir yazılım içeriyorsa ilgili lisans sözleşmesi incelenir, çoğu durumda ilgili yazılım tamamen silinir.

Etki alanı içinde kullanılan kullanıcı bilgisayarları ve mobil cihazlar üzerinde kullanıcı profilleri kaldırıldıktan sonra başka kullanıcının kullanımına tahsis edilir.

Varlık imha edilmeden önce ilgili varlık sahibi tarafından "Varlık İmha Formu" doldurulur ve birim yöneticisi tarafından onaylandıktan ve Bilgi Güvenliği Koordinatörü tarafından paraflandıktan sonra varlık imha edilir. Varlığın imhası bitirildikten sonra süreç doğrulanır ve "Varlık İmha Formu" kalan kısımları doldurularak imha kayıt altına alınmış olur. Varlık İmha Formu Bilgi Güvenliği Koordinatörü tarafından saklanır.

4.5.1. Bilgi Varlıkları İmha Yöntemleri

Bilgi varlıkları imha işlemleri, varlığın üzerindeki bilginin geri döndürülemeyecek şekilde imha edildiğini garanti etmelidir.

Fiziksel İmha: Üzerinde veri tutan her türlü veri depolama birimi, tekrar kullanılma ihtimalini ortadan kaldırmak için parçalama işlemine tabi tutulur. Benzer şekilde bilgi sızıntısını önlemek amacıyla basılı belgeler fiziksel imha işlemine tabi tutulur. Fiziksel imha uygulanmadan önce mümkünse varlık üzerinde ilk önce üzerine yazma yöntemi sonrasında fiziksel imha uygulanır. Fiziksel imha esasları aşağıda anlatılmıştır.

- Veri depolama birimi cihazdan çıkarılır.
- Veri depolama biriminin değişik yerlerinden delik açılır.
- Basılı belgeler kıyma makinesinden geçirildikten sonra ortaya çıkan kâğıtlar farklı çöp poşetlerine koyulur.
- Yakma, eritme, kıyma, ezme, parçalama, yöntemleri ile fiziksel imha işlemi gerçekleştirilir.
- Fiziksel imha ve doğrulama işlemleri tamamlandıktan sonra imha doğrulaması belgelendirilmelidir.
- Bu doküman "Varlık İmha Formu"na ek olarak iliştirilmelidir.

Yönetim kararına istinaden, gizlilik ve imha şartlarının sözleşme dahilinde imza altına alınması koşulu ile toplu imha hizmeti alınabilir.

İmha İşleminin Doğrulanması

Çeşitli geri dönüş uygulamaları ile doğrulama işlemi gerçekleştirilebilir. Doğrulama işlemi, imha süreci içerisinde kesinlikle uygulanması gereken bir aşamadır.

Fiziksel İmha yönteminin doğrulanması: Fiziksel imha işlemi varlık sahibi gözetiminde sorumlu personel tarafından yapılır. İmha işlemi tamamlandıktan sonra veri depolama birimlerinin fiziksel olarak muayenesi yapılır. Varlık sahibi tarafından varlığın fiziksel olarak kullanılamaz halde olduğu onaylanır ise kayıt altına alınır ve doğrulama işlemi sonuçlandırılır.

Kabul Edilemez İmha Yöntemleri

İşletim sistemi üzerinde bilgileri silmek kabul edilemez bir yöntemdir. Bu yöntem ile bilgiler tamamen silinmez ve uygun programlar ile geri döndürülebilir bir şekilde varlık üzerinde bulunmaya devam eder. Bilgiler geri döndürülebilir olduğundan bu yöntem kabul edilemez bir yöntemdir.

Bilgi içeren sabit disk veya depolama birimlerinin çöpe atılması kesinlikle kabul edilemez. Bu yöntem güvenli değildir ve veri sızıntısına neden olabilir.

4.6. Varlıkların Taşınması

Kurum bilgi varlıklarının yetkisiz şekilde tesis dışına çıkarılmasını engellemek amacıyla, kurum güvenlik personeli sürekli tetikte olmalıdır. Şüpheli durumlar söz konusu olduğunda güvenlik görevlisi varlık ile ilgili **Varlık Transfer Formu**'nu görmek isteyebilir. Bu konu ile ilgili koordinasyon Bilgi Güvenliği Koordinatörü tarafından ilgili birimlere yapılır.

Taşınabilir Ortam Varlıkları

Yedekleme ortamları, taşınabilir diskler, flash bellekler ve/veya kritik veri taşıyan CD/DVD vb. depolama ortamları, İstanbul Kültür Üniversitesi dışına çıkarılmadan önce varlık sahibi tarafından "**Varlık Transfer Formu"** ile kayıt altına alınır. Bilgi Güvenliği Koordinatörü tarafından onaylandıktan sonra transfer işlemine başlanır.

Varlıkların transfer işlemi varlık sahibi tarafından veya Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı tarafından yapılır. Varlığın transferi sırasında "**Varlık Transfer Formu"** kullanılır.

Yedekleme ortamları, taşınabilir diskler, flash bellekler ve/veya kritik veri taşıyan CD/DVD vb. depolama ortamları yangın, sel baskını vb. durumlara karşı korunaklı kasada muhafaza edilir.

Sunucular, Ağ ve Güvenlik Cihazları ve Veri Depolama Cihazları:

Sunucular, ağ veya güvenlik cihazları, veri depolama cihazları, İstanbul Kültür Üniversitesi dışına çıkarılmadan önce varlık sahibi tarafından "**Varlık Transfer Formu"** ile kayıt altına alınır. Bilgi Güvenliği Koordinatörü tarafından onaylandıktan sonra transfer işlemine başlanır.

Veri kartuşları, diskler elektromanyetik ortamlardan, toz, sıcaklık gibi çevresel faktörlerden etkilenmeyecek taşıma materyalleri ile transfer edilir.

Varlıkların transfer işlemi varlık sahibi tarafından veya Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı tarafından mümkün olan en korunaklı şekilde yapılır.

Kurum Bünyesinden İzin Alınmadan Çıkarılabilecek Donanımlar

Personele tahsis edilen dizüstü bilgisayar, el bilgisayarları, flash disk vb. ile içerisinde kurum için kritik öneme sahip bilgilerin bulunmadığı cihazlar "**Varlık Transfer Formu"** doldurulmadan kurum dışına çıkarılabilir.

Basılı evrakların veya CD/DVD üzerine kaydedilmiş bilgiler

Basılı veya elektronik ortam üzerine yazılmış kurumsal bilgiler, sınıflandırma veya kullanımına dair kurallara bağlı olarak belirlenmiş kurallara göre transfer edilir. Kurum kaynakları dışında transfer araçları kullanılacaksa, transfer şekline bağlı olarak anlaşmalı kuruluşlarla çalışılır.

5. GÖZDEN GEÇİRME VE REVİZYON

Bu doküman, Bilgi Güvenliği Koordinatörü tarafından periyodik olarak yılda bir kez gözden geçirilir. Bilgi güvenliği ile ilgili diğer politika ve prosedürlerdeki değişiklikler dokümanın gözden geçirilmesini gerektirebilir. Gözden geçirilen ve güncellenen doküman onaylanır ve ilgili taraflara iletilir.

6. İLGİLİ DOKÜMANTASYON

- Varlık Envanteri Listesi
- Varlık İmha Formu
- Varlık Transfer Formu

7. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar