1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı varlıklarının yönetilmesinde uygulanacak kuralları oluşturmayı amaçlar.

2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı idaresi altında olan her türlü Bilişim Sistemleri, donanımları, yazlım ve otomasyonları kapsar.

3. SORUMLULAR

- Bilişim Sistemi Kullanıcıları
- Bilgi İşlem Daire Başkanlığı

4. TANIMLAR

5. UYGULAMA

5.1 Varlık Envanteri Prosedürü

Kurum içerisindeki bütün varlıklar belirlenir. Bilgi varlık listesi veritabanlarını, veritabanı dosyalarını, sistem dokümantasyonlarını, kullanıcı kılavuzlarını, prosedürleri, eğitim dokümanlarını, süreklilik planlarını, sistem yazılımlarını, geliştirme araçlarını, Kurum adına geliştirilen yazılımlara ait kaynak kodlarını, yazılım varlıklarını, uygulama yazılımlarını, fiziksel varlıkları (bilgisayar ekipmanları, işlemciler, sistem denetim izi dosyaları, dizüstü bilgisayarlar vb.) içerir, ancak bunlarla kısıtlı tutulmayabilir. Bütün bilgi varlıkları varlık sahipleri tarafından sınıflandırma kılavuzuna göre sınıflandırılır. Fiziksel olarak korunması gereken bütün bilgi varlıkları, takip edilmesi amacıyla numaralanır ve kimlik etiketi ile takip edilebilir. Bilgi varlıkları için fiziksel takip ve kontroller gerçekleştirilirken bu etiketlerden yararlanılır. Bilgi varlığı sahibi, kendi sahipliğinde bulunan varlıklar hakkındaki bilgilerin, bilgi varlıkları envanterinde güncel tutulmasını sağlamakla yükümlüdür. Harcama Yetkilisi, varlık envanterini, envanter oluşturulduktan sonra Taşınır Kayıt Yetkilisi ile kontrol eder. Harcama Yetkilisi, Taşınır Kayıt Yetkilisi ile beraber bağlı olduğu birime yönelik bilgi varlıklarının listesini takip eder ve gerektiğinde güncellenmesini sağlar. Uygun şekilde tam bir listesini tutar. Varlık envanteri yıllık olarak Harcama Yetkilisi ve Taşınır Kayıt Yetkilisi tarafından birlikte gözden geçirilir.

5.2 Varlıkların Sınıflandırılması

Bilgi varlıklarının sınıflandırılma şeması ve ilgili kılavuzlar aşağıdakileri içerir:

- Varlığın türünü
- Varlığın kritiklik derecesini
- Bilgi varlığının değerini
- Bilgi güvenliği ihlalinin ya da varlığın kaybolmasının etkilerini

5.3 Sınıflandırmanın Uygulanması

Varlık sınıflandırması, Kurum kontrolü altında saklanan, iletilen ya da kullanılan bütün varlıklar için kullanılır; örneğin, Kurum müşterileri, hizmet sağlayıcıları ve iş ortakları tarafından verilen bilgiler bu veri sınıflandırma şeması ile korunur. Aynı şekilde Kurum çalışanları da üçüncü parti bilgilerinin korunmasını sağlar. Bu veri sınıflandırma şeması ayrıca üçüncü partilere ait bilgiler için de kullanılabilir. Veri sınıflandırma yöntemi ile yazılı olmayan veri, kişilerin sahip olduğu bilgiler ve bilgi birikimi arasında bir ayrım yapılamaz.

5.4 Tutarlı Koruma

Kurum'un bilgi varlıkları, oluşturulmalarından imha edilmelerine kadar geçen süre boyunca korunur. Bilginin nerede bulunduğundan, hangi formda tutulduğundan ya da teknolojisinden ve hangi amaç için kullanıldığından bağımsız olarak ne kadar kritik bir bilgi olduğuyla orantılı olarak korunur. Her ne kadar bu veri sınıflandırması, veri tutarlığı ve verinin korunması için genel bir kılavuz niteliği taşısa da, Kurum çalışanları bu kavramı günlük operasyon ihtiyacıyla uyumlu olarak genişletebilir. Kurum verilerinin korunması ve imha edilmesi, kritik verilerin kritiklik derecesinin revize edilmesi, KVKK kapsamında ayrıca değerlendirilmektedir.

5.5 Bilgi Sınıflandırma Kılavuzu ve Sınıflandırmanın İptali

Varlıkların sınıflandırılması ve bu sınıflandırmanın iptali sırasında varlık sahipleri tarafından aşağıdaki kılavuz izlenir.

5.5.1 Sınıflandırma

Her bilgi varlığı sahibi, kendi sorumluluğundaki varlıkları Varlık Sınıflandırma prosedürlerine ve Risk Yönetimi Prosedürü'ne göre sınıflandırır. İş Birimi Yöneticileri ve Taşınır Kayıt Yetkilisi, varlıkların bilgi varlığı sahipleri tarafından altı ayda bir güncellenmelerini sağlar ve kendi sorumluluklarındaki varlıkların gözden geçirilmesi, arşivlenmeleri ya da imha edilmeleri gereken varlıkların belirlenmesi için süreci başlatır. Müşterilere ait veriler, müşteri ile yapılan sözleşmenin yasal süresinin sonunda arşivlenir. Bu işlemler sözleşmedeki hükümlere ya da bilgi güvenliği yasalarına uygun şekilde gerçekleştirilir.

5.5.2 Sınıflandırmanın İptali / Gizlilik Sınıfının Düşürülmesi

Sınıflandırmanın iptali veya gizlilik sınıfının düşürülmesi sırasında ilgili varlık sahibi aşağıdaki kılavuza uyar:

- İlgili bilgi varlığı sahibi gerekli gördüğü zaman Taşınır Kayıt Yetkilisinin de onayını alarak bilgi varlığının sınıflandırmasını iptal edebilir ya da gizlilik sınıfını düşürebilir. Bu işlemi gerçekleştirirken orijinal listedeki sınıflandırma etiketini günceller ve gerekli kullanıcıları haberdar eder.
- Kurum'daki kritik bilgilerde hangi tarihte sınıflandırmanın iptal olacağı ya da gizlilik sınıfının düşürüleceği belirtilebilir. Bu konuda bir bilgi girilmediği takdirde, bilgi

sahibi tarafından güncellenene kadar veri en son atanan kritiklik seviyesinde değerlendirilir.

- Harcama Yetkilisi ve Taşınır Kayıt Yetkilisi, sınıflandırmanın değiştirilmesini belirlenen zamandan önce ya da sonra gerçekleştirebilir.
- Harcama Yetkilisi ve Taşınır Kayıt Yetkilisi altı ayda bir bilgi varlıklarının sınıflandırmasının değiştirilmesi ile ilgili kontrolleri yapar.

5.6 Varlık Yönetimi Rol ve Sorumlulukları

5.6.1 Bilgi Varlığı Sahibi

Varlık Sahibi ya da Bölüm Müdürü, varlık sınıflandırmasını kılavuzlara ve varlık sınıflandırma şemasına uygun bir şekilde yapmakla sorumludur (Varlığın gizlilik, bütünlük ve erişilebilirlik kriterlerine göre). Varlık Envanteri ve Risk Değerlendirmeleri, Harcama Yetkilisi ve Taşınır Kayıt Yetkilisi tarafından kontrol edilir ve onaylanır. Tüm belgeler üzerinde versiyon kontrolü yapılır ve her yapılan değişiklik yeni bir versiyon olarak kaydedilir. Bilgi varlığının sahibi, uygulanması gereken kontrolleri gerçekleştirir. Bilgi varlığının güvenliğinden o varlığın sahibi sorumludur.

5.6.2 Bilgi Varlığı Sorumlusu

Bilgi varlığı sorumlusu, varlık sahibinden farklı bir kişi olabileceği gibi, varlık sahibi de olabilir. Varlık sorumlusu, varlığın korunmasından ve gerekli kontrollerin uygulanmasından sorumludur (varlık sahibinin belirttiği ve onayladığı bilgi varlığı kontrolleri) ve sınıflandırılmış varlıklarda koruma mekanizmalarının oluşturulmasını sağlar.

5.6.3 Bilgi Varlıkları Kullanıcıları

Kurum için bilgi önemli olduğundan ve Kurum içerisinde yaygın olarak kullanıldığından, bütün kullanıcılar bu bilgilerin korunmasında önemli role sahiptirler ve kendilerine verilen bu bilgileri korumakla yükümlüdürler. Kamuya açık olmayan kritik bilgi ile çalışan tüm kullanıcılar Varlık Yönetimi Politikası'nı, standartlarını ve prosedürlerini uygular.

5.7 Varlık Sınıflandırma Standartları

5.7.1 Gizlilik Kriterleri

Gizlilik kriteri seviyesi, bilgi varlığına ne seviyede bir erişim olacağını belirtir. Varlık değeri 1-5 Aralığında verilir; 1 en düşüktür, 5 en yüksek seviyedir.

Varlık Değeri	Erişilebilirlik	Açıklama
Çok Düşük (1)	Kamuya Açık	Bu tür bilgilerin paylaşılmasının bilgi varlığı gizliliği üzerinde herhangi bir etkisi yoktur; bu sebeple çok düşük gizlilik seviyesine sahiptirler. Bu bilgi formları ya kamuya açık kaynaklardan gelmektedir ya da Kurum tarafından kamuya açılmak üzere oluşturulmuştur. Örnek: Süreli yayınlar, kamu bültenleri, yayınlanan Kurum mali tabloları, yayınlanan basın bültenleri vb.
Düşük (2)	Kurum İçi	(Bütün bölümler ve personeller için) Bu bilgiler Kurum'a özeldir. Bilgi üzerinde sadece Kurum'un hakkı vardır (istisna: Bazı tür dokümanlarda, örneğin, sözleşmelerde tarafların hepsinin dokümana erişimleri olabilir). Bu tür dokümanlar sadece Kurum tarafından kullanılır ve üçüncü parti ya da kuruluş dışından kişilerle paylaşılmaz. Örnek: Personel notları, Kurum haberleri, mektuplar, personel bilinçlendirme belgeleri ve bültenleri, hizmet sözleşmeleri vb.
Orta (3)	Hizmete Özel	Hizmete Özel bilgi, bilgi türlerinin hassas olanlarındandır. Bu tür bilgiler "yalnızca bilmesi gerekenler" ilkesine uygun olarak paylaşılır. Kurum dışındaki Kurumlarla paylaşılması gereken, "Gizli" olarak sınıflandırılmayan ancak kamuya açık olmayan tüm bilgiler bu kategoriye girer. Örnek: Özlük bilgileri, iş planları, yayınlanmamış finansal tablolar, Asgari güvenlik standartları, Firewall ve Router konfigürasyonları.
Yüksek (4)	Gizli	Gizli Bilgi, bilgi türleri içerisinde hassas olan bilgilerdendir, bilginin kullanılması ya da yetkisiz kişilerin eline geçmesi Kurum'un işlerini etkiler; ancak bu etki orta vadede telafi edilebilir. Belirli kısıtlamalar ve kontroller uygulanır. (Örneğin, kısıtlı sayıda personel ya da bölüme erişim hakkı verilir.) Örnek: Çalışan bordro bilgileri, Organizasyonel planlar.
Çok Yüksek (5)	Çok Gizli	Çok Gizli Bilgiler en hassas bilgi formlarıdır. Kullanılması veya paylaşılması Kurum'un işlerini doğrudan etkiler. Üst seviye kısıtlamalar ve kontroller uygulanır (çok kısıtlı sayıda personele erişim hakkı tanınır). Örnek: stratejik planlar, yatırım kararları vb.

5.8 Bilgi Sınıflandırma Matrisi

5.8.1 Güvenlik Kontrol Matrisi

Güvenlik	Bilgi Sınıfı				
Hizmet	**Kamuya Açık**	**Kurum İçi**	**Hizmete Özel**	**Gizli**	**Çok Gizli**
Kimlik ve Kimlik Doğrulaması	Yok	Kullanıcı isimleri ve şifreleri	Yüksek güvenlik kontrolü (şifreli kullanıcı adları, şifreler, Güvenlik sertifikaları)	Yüksek güvenlik kontrolü uygulanır	Yüksek güvenlik kontrolü uygulanır
Yetkilendirme ve Erişim Kontrolü	Değişikliklerdeki erişim kontrolü	İş bölümleri veya fonksiyonları tarafından izin verilmesi, bilgi kategorisine göre erişim kontrolü uygulanması	Kullanıcı adı ve rolüne göre, özel amaçlı klasör ve dokümanlara erişim	Bazı alanlar için erişim kontrolleri-Kullanıcı adı ve bölümüne göre ilgili klasör ve dokümanlara erişim	Her alan için erişim yetkilendirme denetimi
Denetleme	Sistem düzeyinde modifikasyonlar, olaylar ve alarmlar için	Kullanıcı erişimleri, hatalı erişimler ve alarmlar için sistem seviyesinde kontrol	Sistem seviyesinde kullanıcı erişimleri, dosya değişiklikleri, erişimlerin inkâr edilememesi, alarmlar için	Bütün olaylar ve alarmlar	Bütün olaylar ve alarmlar
Medyaların Fiziksel Kontrolü (kâğıt, çıkarılabilir diskler, yazılabilir CD-ROM, vb)	Yok	Etiketleme, işaretleme, belgelerin imhası, güvenli depolama	Etiketleme, işaretleme, belgelerin imhası, güvenli depolama	Etiketleme, işaretleme, belgelerin imhası, güvenli depolama, erişim listesi.	Etiketleme, işaretleme, belgelerin imhası, güvenli depolama, erişim listesi, denetimler
Güvenlik Operasyonları	Sistem yapılandırması seviyesinde denetim ve güvenlik olaylarının incelenmesi	Sistem yapılandırması seviyesinde denetim ve güvenlik olaylarının incelenmesi	Sıklıkla gerçekleştirilen sistem yapılandırması seviyesinde denetim ve güvenlik olaylarının incelenmesi	Sıklıkla gerçekleştirilen sistem yapılandırması seviyesinde denetim ve güvenlik olaylarının incelenmesi	Sıklıkla gerçekleştirilen sistem yapılandırması seviyesinde denetim ve güvenlik olaylarının incelenmesi

5.8.2 İletim Kontrol Matrisi

Bilginin iletildiği Ortam	Kamuya Açık	Kurum İçi	Hizmete Özel	Gizli	Çok Gizli
Yerel ağ ya da geniş ağlar	Ağ üzerindeki kapsamı sınırlamak için erişim kontrol listelerinin kullanılması	Ağ üzerindeki kapsamı sınırlamak için erişim kontrol listelerinin kullanılması	Ağ üzerindeki kapsamı sınırlamak için erişim kontrol listelerinin kullanılması	Şifreleme	Şifreleme
Faks	Özel bir ihtiyaç yok	Erişimleri şifrelenmiş Faks	Kimlik doğrulama Erişimleri şifrelenmiş Faks Programlanmış numaraların kullanılmaması Gönderi numaralarının doğrulanması Faksların geldiği ve gönderildiği yerlerin bilinmesi	Kimlik doğrulama Erişimleri şifrelenmiş Faks Faks kullanımının en düşük seviyeye getirilmesi	Kimlik doğrulama Mesajlaşma yazılımlarının kullanılması Faks kullanımının en düşük seviyeye getirilmesi
Yazıcı	Özel bir ihtiyaç yok	Fiziksel olarak güvenli bir yerde bulunan yazıcının kullanılması	Kimlik doğrulama Fiziksel olarak güvenli bir yerde bulunan yazıcının kullanılması Hedef yazıcının doğrulanması	Kimlik doğrulama Fiziksel olarak güvenli bir yerde bulunan yazıcının kullanılması Hedef yazıcının doğrulanması	Kimlik doğrulama Fiziksel olarak güvenli bir yerde bulunan yazıcının kullanılması Hedef yazıcının doğrulanması

Bilginin iletildiği Ortam	Kamuya Açık	Kurum İçi	Hizmete Özel	Gizli	Çok Gizli
Video ve sesli konferans	Özel bir ihtiyaç yok	Konferans sahibi katılımcıları onaylamalı	Şifreleme Konferans sahibi katılımcıları onaylamalı	Şifreleme Konferans sahibi katılımcıları onaylamalı	Şifreleme Konferans sahibi katılımcıları onaylamalı Görüşmenin dinlenemediğinden emin olunmalı Gizli metin ya da belgelerin kamera tarafından görüntülenmediğine emin olunmalı
Modem veya ISDN	Şifre ile koruma	Şifre ile koruma Sahibi erişim ihtiyaçlarını belirler	Güvenilir ve güçlü bir kimlik doğrulama mekanizması	Güvenilir ve güçlü bir kimlik doğrulama mekanizması	Şifreleme Daha Güvenli bir kimlik doğrulama mekanizması
Veritabanı	Yetkisiz erişimlerin kısıtlanması için erişim kontrol listelerinin oluşturulması	Şifre ile koruma	Veri kullanılmadığı durumlarda şifrelenir	Veri kullanılmadığı durumlarda şifrelenir	Veri kullanılmadığı durumlarda şifrelenir
E-Posta	Özel bir ihtiyaç yok	Özel bir ihtiyaç yok	Şifreleme	Şifreleme	Şifreleme “Yüksek derece de önemlidir, kopyasını bulundurmayınız” diye bilgilendirme notu düşülür
Kağıt	Özel bir ihtiyaç yok	Dış Posta İç Posta	Sertifikalı dış posta İç Posta	Kayıtlı dış posta Kapalı zarf kullanımı	Kayıtlı dış posta İki katlı zarf kullanımı Mesaj servisleri kullanılamaz Elden teslim edilir

5.8.3 Depolama Kontrol Matrisi ve Etiketleme

Bilginin bulunduğu Ortam	Kamuya Açık	Kurum İçi	Hizmete Özel	Gizli	Çok Gizli
Sunucu	Özel bir ihtiyaç yok	Güçlü ve karmaşık şifre kullanımı Fiziksel olarak korunaklı bir sistem odasına konulur	Şifreleme Güvenli bir kimlik doğrulama mekanizması Kısıtlanmış erişim listesi Denetim izi mekanizmaları etkinleştirilir Fiziksel olarak korunaklı bir sistem odasına konulur	Şifreleme Güvenli bir kimlik doğrulama mekanizması Kısıtlanmış erişim listesi Denetim izi mekanizmaları etkinleştirilir Fiziksel olarak korunaklı bir sistem odasına konulur	Şifreleme Güvenli bir kimlik doğrulama mekanizması Kısıtlanmış erişim listesi Denetim izi mekanizmaları etkinleştirilir Fiziksel olarak korunaklı bir sistem odasına konulur
Masaüstü Bilgisayar	Özel bir ihtiyaç yok	Güçlü ve karmaşık şifre kullanımı	Şifreleme Güvenli bir kimlik doğrulama mekanizması	Şifreleme Güvenli bir kimlik doğrulama mekanizması Ana Bilgisayarda, Sunucularda veyaşifre kontrolleriyle korunan taşınabilir ortamlarda tutulur	Şifreleme Güvenli bir kimlik doğrulama mekanizması Ana Bilgisayarda, Sunucularda veya şifre kontrolleriyle korunan taşınabilir ortamlarda tutulur
Dizüstü Bilgisayar	Özel bir ihtiyaç yok	Güçlü ve karmaşık Şifre kullanımı Dizüstü bilgisayarlar kullanılmadığı zaman kabinetlere kilitlenir	Şifreleme Güvenli bir kimlik doğrulama mekanizması Kullanımı minimum	Şifreleme Güvenli bir kimlik doğrulama mekanizması Kullanımı minimum	Şifreleme Güvenli bir kimlik doğrulama mekanizması Kullanımı minimum

Bilginin bulunduğu Ortam	Kamuya Açık	Kurum İçi	Hizmete Özel	Gizli	Çok Gizli
			seviyede tutulur Dizüstü bilgisayarlar kullanılmadığı zaman dolaplara kilitlenir	seviyede tutulur Dizüstü bilgisayarlar kullanılmadığı zaman dolaplara kilitlenir	seviyede tutulur Dizüstü bilgisayarlar kullanılmadığı zaman dolaplara kilitlenir
Taşınabilir ortam (Örn: CD, Flash bellek)	Özel bir ihtiyaç yok	Taşınabilir cihazlar bilgisayarlar kullanılmadığı zaman dolaplara kilitlenir	Şifreleme Taşınabilir cihazlar bilgisayarlar kullanılmadığı zaman dolaplara kilitlenir	Şifreleme Taşınabilir cihazlar bilgisayarlar kullanılmadığı zaman dolaplara kilitlenir	Şifreleme Taşınabilir cihazlar bilgisayarlar kullanılmadığı zaman dolaplara kilitlenir
Hardcopy (Kağıt, Film, Video vb)	Özel bir ihtiyaç yok	Ön sayfaya etiketleme yapılır“Kurum İçi” Basılı dokümanlar kullanılmadıklarında dolaplara kilitlenir.	Bütün sayfalara “Hizmete Özel” etiketi yapıştırılır. Alıcının geri bildirimi alınır Basılı dokumanlar kullanılmadıklarında dolaplara kilitlenir	Bütün sayfalara “Gizli” etiketi yapıştırılır. Alıcının geri bildirimi alınır Ödünç alan kişinin kaydı tutulur. Basılı dokumanlar kullanılmadıklarında dolaplara kilitlenir	Bütün sayfalara “Çok Gizli" etiketi yapıştırılır Ödünç alan kişinin kaydı tutulur. Kopyalanamaz. Basılı dokümanlar kullanılmadıklarında dolaplara kilitlenir

5.8.4 İmha Kontrol Matrisi

Bilginin Bulunduğu Ortam	Kamuya Açık	Kurum İçi	Hizmete Özel	Gizli	Çok Gizli
Taşınabilir ortam (Örn: CD, Flash bellek)	Özel bir ihtiyaç yok	Dosya silinir Taşınabilir cihazlar bilgisayarlar kullanılmadığı zamanlarda dolaplara kilitlenir.	Bilgi İşlem dosyaları siler Taşınabilir cihazlar bilgisayarlar kullanılmadığı zamanlarda dolaplara kilitlenir	Bilgi İşlem dosyaları siler Taşınabilir cihazlar bilgisayarlar kullanılmadığı zamanlarda dolaplara kilitlenir	Bilgi İşlem dosyayı kurtarılmaya olanak vermeyecek şekilde siler Taşınabilir cihazlar bilgisayarlar kullanılmadığı zamanlarda dolaplara kilitlenir
E-posta	Özel bir ihtiyaç yok	Eski e-postalar periyodik olarak silinir	E-posta 3 ay sonra silinir	E-posta 3 ay sonra silinir	E-posta 3 ay sonra silinir
Kağıt, Film veya Video vb.	Özel bir ihtiyaç yok	Kağıt öğütücü cihazlardan geçirilmeli ya da geri dönülemeyecek şekilde silinir.	Kağıt öğütücü cihazlardan geçirilmeli ya da geri dönülemeyecek şekilde silinir.	Dosya sahibi ya da onun atayacağı biri tarafından kağıt öğütücü cihazlardan geçirilir ya da geri dönülemeyecek şekilde silinir.	Orijinal dosyanın sahibi tarafından imha edilir.

6. İLGİLİ DOKÜMAN

- Varlık Yönetimi Politikası
- Kabul Edilebilir Kullanım Politikası

Hazırlayan		Onaylayan