1. AMAÇ

Bu prosedür, Karamanoğu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesindeki bilgilere erişimin için kullanılacak yöntemleri ve kuralları oluşturulmasını amaçlar.

2. KAPSAM

Bu prosedür, Karamanoğu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesindeki bilgilere erişimi kapsar.

3. SORUMLULAR

- Bilişim Kullanıcılara
- Bilgi İşlem Daire Başkanlığı

4. TANIMLAR

5. UYGULAMA

5.1 Kullanıcı Hesap Yönetimi

5.1.1 Yeni Kullanıcı Hesabı Açılması

İşe yeni başlayan personelin seçme ve yerleştirme süreci İK bölümünde tamamlandıktan sonra, İK bölümünden gelen talebe istinaden ilgili personeli bilgilendirir. Bir çalışanın iş tanımının gerektirdiği sistemler dışında bir sisteme erişimi gerektiğinde, bu çalışanın yöneticisi ya da kendisi yöneticisini de bilgilendirerek, erişim talebinde bulunur. İlgili personel iş uygulamaları ara yüzleri üzerinden çalışanın iş tanımına uygun önceden belirlenmiş ya da çalışanın yöneticisi tarafından talep edilen sistemlere erişimini tanımlar. Kullanıcılara verilecek bilgisayarlara "Bilgisayar Kurulum Uygulamaları Listesi"ne göre olması gereken ve kişinin rol ve sorumluluklarına göre opsiyonel izinli uygulamalar kurulur. Üçüncü tarafların kurum bilgi sistemlerine erişmesi gerektiğinde üçüncü taraf ile koordinasyonu sağlayan ilgili personel, kendi bölüm yöneticisinin de onayına istinaden ilgili erişim formunu doldurarak ıslak imzalı halini gönderir ve erişim talebinde bulunur. Talep, Bilgi Güvenliği yöneticisi ile ağ ve sistem yönetmeni tarafından değerlendirilir ve onaylanır. Sözleşmeli çalışanlar ve danışmanlar için kullanıcı hesapları kurumdan ayrılana kadar geçerli olacak şekilde yaratılır. Bu tarih sonrasında da bu kullanıcı hesabına ihtiyaç duyulması halinde, bölüm yöneticisinin onayıyla kullanıcı hesabı aktif hale getirilir. Üçüncü taraflar için kullanıcı hesabı yaratılmasında Sistem Yöneticisinin onayı gereklidir. Sistem yöneticisi, üçüncü taraflara sistemlerde kullanıcı tanımlar. İşletim sisteminde açılacak yeni kullanıcı hesaplarını Sistem Yöneticisi, uygulamalarda açılacak yeni kullanıcı hesaplarını ilgili bölüm yöneticisi ve veritabanında açılacak yeni kullanıcı hesaplarını Bilgi İşlem Müdürü onaylar. Ağ donanımları veya ağ hizmetlerine erişim talebinde bulunan yeni kullanıcılar OTRS üzerinden çağrı açar. Ortak kullanıcı hesaplarına erişim hakkı, bireysel hesapların yaratılmasının teknik olarak elverişli olduğu durumlarda, birden fazla kişiye verilemez. Ortak bir kullanıcı hesabının kullanımını

gerektiren durumlarda, bu erişimin verildiği kullanıcıların ve erişim gereksiniminin detayları sunularak, Sistem yöneticisi ve Bilgi Güvenliği Yöneticisi'nden özel izin ve onay alınır. Ortak kullanıcı hesabı kullanımı, kayıt altına alınır. Bilgi Güvenliği Yöneticisi ayda bir defa erişim denetim izlerini (log) gözden geçirir. Yapılan incelemede ortak kullanıcı hesaplarına hangi terminallerden girildiği ve bu terminallerin sahibi olan çalışanlar değerlendirilir. Eğer ortak kullanıcı hesabı, bu hesaba ulaşmasına onay verilmeyen bir çalışan tarafından kullanılıyorsa, önce şifresi değiştirilir. Daha sonra bu durum ilgili birimin Bilgi Güvenliği Yöneticisine bildirilir. Sistem yöneticileri, kullanıcıların aynı anda, birden fazla terminalden sisteme giriş yapamaması için gerekli parametreleri uygun şekilde ayarlar.

5.1.2 Kullanıcı Hesaplarının Bakımı

Yılda en az iki defa, Bilgi Güvenliği Yöneticisi veya Sistem Sorumlusu, işletim sistemi, veritabanı ve ağ elemanlarındaki/hizmetlerindeki kullanıcı hesaplarını gözden geçirir. Bilgi Güvenliği Yöneticisi veya Sistem Sorumlusu, mümkün olan durumlarda, bu hesapların iptal edilmesini sağlar. Bilgi İşlem yöneticisi, sadece belirli kullanıcılardan gelen talep ve kullanıcının kimliğinin doğrulanması üzerine, sistem yöneticilerini bu hesabı tekrar aktif hale getirmeleri için yetkilendirir. Eğer bir kullanıcı 60 günden fazla bir süre için ayrılacaksa, IK veya bölüm sorumlusu Bilgi Güvenliği Yöneticisine bunu bildirir. Bilgi Güvenliği Yöneticisi ise bu bilgi üzerine kullanıcı hesabının bu süre zarfında sistemlerin kullanılması söz konusu değil ise bu süre için kapatılmasını sağlar. IK birimi aynı zamanda kuruluş ile ilişkisini kesen kullanıcıların listesini, erişim haklarının silinebilmesi için Bilgi Güvenliği Yöneticisine sunar. Gözden geçirme sırasında ya da ilk defa yeni bir yazılım yükleneceği zaman, Bilgi Güvenliği Yöneticisi, kurulumla gelen tüm kullanıcı hesaplarının kaldırılmasını veya bu hesaplara tanınmayacak hesap isimleri verilmesini veya şifrelerinin karmaşık olacak şekilde değiştirilmesini sağlar.

5.1.3 Tayin Olan ve İşten Ayrılan Kullanıcıların Hesaplarının Kaldırılması

İK birimi veya işten ayrılan/transfer edilen çalışanın bölüm yöneticisi bu çalışan hakkında Bilgi Güvenliği Yöneticisi'ni derhal bilgilendirir. Bilgi Güvenliği Yöneticisi, ilgili çalışanın kullanıcı hesaplarının kaldırılmasını veya erişim haklarının geri alınmasını onaylar ve bu talebi ilgili sistem yöneticisine bildirir. Sistem yöneticileri, çalışanların işten ayrılmaları üzerine Bilgi İşlem kimlik yönetim sistemi üzerinde kullanıcı hesabının pasif hale getirilmesini veya sorumluluklarının değişmesi durumunda erişim yetkilerinin uygun şekilde değiştirilmesini sağlar. Bilgi Güvenliği Yöneticisi kullanıcı listelerini, kullanıcı hesaplarının işten ayrılma tarihinde kapatıldığına veya erişim yetkilerinin güncellendiğine dair gözden geçirir. Ortak bir kullanıcı hesabının kullanılması ya da işten ayrılan çalışanın kullanıcı hesabının denetim amacıyla açık tutulması gerektiğinde veya uygulamanın kullanıcı hesabının kaldırılmasına imkân vermediği durumlarda, bu hesapların şifreleri, çalışanın son iş gününde değiştirilir. Bölüm yöneticisi, işten ayrılan personelin tüm sorumlulukların başka bir çalışana aktarılmasını sağlar. Bölüm yöneticisi ayrıca işten ayrılan çalışanın, işten ayrılmak için başvurduğu andan itibaren faaliyetlerini yakın takipte izler. İK birimi, işten ayrılan çalışanın, üzerindeki bilgisayar, anahtar, kimlik kartı, geçiş kartı, yazılım, veri, doküman, kılavuz gibi tüm donanımları kurum ilgili birim yöneticisine teslim edilmesini sağlar. Çalışanın işten

ayrılması sonrasında tesis dışına çıkarmak istediği tüm malzemeleri güvenlik personeli incelemeye alır ve Güvenlik personeli kurumla ilişiği kesilmesi esnasındaki tüm süreçte çalışana refakat eder. Yukarıdaki prosedürler çalışanların kendi rızaları dışında işten ayrılmaları veya kurum içinde gerçekleşen transfer ve görev değişiklik durumlarında da geçerlidir.

5.2 Ayrıcalıklı Yetkilerin Yönetimi

5.2.1 Rol-Yetki Matrisi

Sistem ve ağ yöneticileri, uygulama yöneticileri ve kimlik yöneticileri, Bilgi Güvenliği Yöneticisi ve bölüm yöneticilerinin yardımıyla her bir iş birimi için işletim sistemi, uygulama, veritabanı ve ağ elemanları üzerinde tanımlı tüm erişim haklarını belirler. Rol-Yetki matrisinin oluşturulması ve dokümante edilmesi için, bu erişim hakları, kurumun personel iş tanımlarıyla (rol ve sorumlulukları) eşleştirilir. İş sorumluluğu için gereken çoğu uygulama, işletim sistemi ve veritabanı erişim hakları belirlenerek, erişim haklarının etkin ve güvenli yönetimi için bir uygulama rolüne atanır. Mümkün olduğu durumda, birim içerisindeki ilgili her bir iş tanımı için ayrı bir uygulama rolü yaratılır. Bilgi İşlem Müdürü, bu rollerin ve bunlara sağlanacak yetkilerin yönetimi için oluşturulan Rol-Yetki Matrisi'ni gözden geçirir, inceler ve herhangi bir olumsuz durum oluşturmadığında gerekli onayı verir. Bu işlem, bir uygulama, işletim sistemi, veritabanı veya ağ donanımının ilk kullanımında gerçekleştirilir.

Sistem yöneticileri / uygulama yöneticileri / ağ yöneticilerinin desteğini alarak Rol-Yetki matrisini aşağıdaki senaryolar söz konusu olduğunda değiştirir:

- Bir uygulama, İşletim Sistemi, Veritabanı veya ağ donanımında önemli bir değişiklik gerçekleştiğinde veya yeni bir modül veya fonksiyon eklendiğinde
- Yeni bir iş tanımı veya rol oluşturulduğunda
- İş tanımında veya rolde değişiklik yapıldığında

Bilgi Güvenliği Yöneticisi ya da Rol-Yetki Matrisi'nin görevler ayrılığı ilkesini ihlal etmediğini kontrol eder ve görev ayrılıklarının yılda bir gözden geçirilmesini sağlar. İlgili Birim yöneticisi Rol-Yetki Matrisi'nin eksiksiz ve gereksinimlere uygun olduğunu kontrol eder.

5.2.2 Erişim Hakkı Verilmesi

İki durum için bir kullanıcıya erişim hakkı tanımlanır. Birinci durum, kullanıcı hesabının oluşturulmasıdır. Diğeri ise bir kullanıcının, görev değişikliği ya da sorumluluklarının değişmesinden ötürü ek erişim hakları talep etmesidir. Özel bir nedenden ötürü yüksek erişim yetkisine sahip kullanıcılar, normal işleri için ayrı bir kullanıcı hesabı kullanır (örn. bir uygulama çalıştırmak için sorumlu personel kendi kullanıcı hesabı ile sisteme giriş yaptıktan sonra bu hesabı üzerinden "sistem yöneticisi - System Administrator" kullanıcı hesabına geçiş yapar). Yeni bir kullanıcı yaratıldığında, erişim hakları, onay ve yetkinin alınmasının ardından talebe göre verilir. Bir kullanıcının ek erişim haklarına ihtiyaç duyması durumunda, bu kişi bu formu Bölüm Yöneticisine onaylattıktan sonra talepte bulunur ve bu formu onay için Bilgi Güvenliği Yöneticisine, Sistem ve Ağ Yönetmenine ve Bilgi

İşlem Müdürüne iletir. Kullanıcılara erişim hakkı verilmeden önce, erişim hakkı talebinin, bölüm yöneticisi tarafından onaylanması gerekir. Bölüm yöneticisi bu kişinin, verilecek ek erişim hakkına sorumluluklarını yerine getirmek için gereksinim duyduğunu kontrol eder ve talep edilen erişim yetkisinin, o kişinin görevlerini yapabilmesi için minimum yeterliliğe sahip olup olmadığı inceledikten sonra talebi onaylar. Sistem/Ağ/Uygulama Yöneticileri herhangi bir olumsuz durum ortaya çıkmayacağını ön görmeleri halinde ve gerekli onayların alındığını kontrol ederek sistem, ağ ve uygulamalarda talep edilen erişim haklarını Bilgi İşlem Müdürünün onayına istinaden tanımlar. Kurum bünyesinde çalışan personelin görev tanımlarına istinaden, erişim sağlanan sistemlerde roller ve yetkiler tanımlıdır.

5.2.3 Erişim Haklarının Gözden Geçirilmesi

Bilgi Güvenliği Yöneticisi erişim yetkilerini kendi bölümü için yılda en az iki defa gözden geçirir. Bilgi Güvenliği Yöneticisi çeşitli bilişim sistemlerindeki kullanıcıları, erişim yetkileriyle birlikte her sene gözden geçirir. Bilgi Güvenliği Yöneticisi, bilişim sistemlerindeki kullanıcıların erişim yetkilerinin onaylarını ve dokümante edilen ile uygulamadaki yetkilerin aynı olduklarını kontrol eder. Bilgi Güvenliği Yöneticisi, geçerlilik tarihinden sonra erişim yetkilerinin kaldırıldığını kontrol eder. Bilgi Güvenliği Yöneticisi, ayrıca onay olmadan erişim hakkı verilip verilmediğini kontrol eder.

5.3 Şifre Yönetimi

İşletim Sistemi, uygulama, veritabanı ve ağ donanımlarının şifre parametreleri aşağıdaki şekilde yapılandırılır:

- Minimum şifre uzunluğu: 8 karakter
- Şifre bileşimi: alfa nümerik, büyük ve küçük harfler ve en az bir özel karakter (bunlardan en az üçü sağlanmalıdır)
- İzin verilen hatalı giriş sayısı: 5

Belirli kısıtlardan ötürü şifre politikaları ayarlanamadığında, bu ayarlar dokümante edilir ve Güvenlik Kurulu tarafından onaylanır.

5.3.1 Kritik Şifrelerin Saklanması ve Yönetimi

Aşağıdaki tablo hangi tip şifrelerin kritik şifre olduğunu göstermektedir. Bu şifreler, kaybolma ve unutulma riskine karşı dikkatli bir şekilde muhafaza edilmelidir.

Kritik şifreler Bilgi İşlem Daire Başkanınca muhafaza edilir.	Şifre Tipi
Bilgi İşlem Sistemi / İş Uygulaması	Super User Şifresi (mevcut olduğu durumlarda) Yönetici (Administrator) Şifresi/Şifreleri Sistem Şifresi (Veritabanı bağlantısı için)

	mevcut olduğu durumda
Veritabanı	Veritabanı Super User Şifresi Veritabanı Yönetici (Administrator) Şifresi Veritabanı Security Officer Şifresi

5.4 İşletim Sistemleri, Uygulamalar &Veritabanları

Bilgi Güvenliği Yöneticisi, Bilgi İşlem ekip üyeleri ile beraber, İşletim Sistemi, Uygulama ve Veritabanları için Asgari Güvenlik Standartları (AGS) geliştirilmesini ve bu standartların uygulanmasını sağlar. Bilgi Güvenliği Yöneticisi AGS'nin geliştirilmesi sırasında şunlara dikkat eder:

- İşletim sistemi, uygulama ve yönelik, Erişim Kontrolü Politikası'nda detaylarıyla açıklanan tüm politika gereksinimleri
- Kullanıcı hesaplarının çeşitli tiplerinin kullanımı üzerindeki kısıtlar
- Gelişmiş erişimli yazılım ve hizmet programları üzerindeki kısıtlamalar
- İşletim Sistemi komutlarına erişim üzerindeki kısıtlamalar

Ayrıca, Bilgi Güvenliği Yöneticisi tüm İşletim Sistemi, Uygulama ve Veritabanı kurulumlarının AGS'ye göre yapılmasını sağlar. Eğer yeni bir sistem veya uygulama canlıya alınacaksa, canlıya geçilmeden önce, Bilgi İşlem Müdürü, gerek duyulduğunda sistem yöneticisinin uygun güvenlik eğitimlerini almasını sağlar. Güvenlik yönetimi fonksiyonları tesis edilmeden sistemlere erişim hakkı verilemez. Bilgi Güvenliği Yöneticisi, en son güvenlik konfigürasyonlarını standartlara ekleyebilmek veya bunu ilgili sistem yöneticisine uygulatmak amacıyla AGS'yi yılda bir defa gözden geçirir ve gerektiğinde günceller. Bilgi Güvenliği Yöneticisi tüm konfigürasyonların AGS'ye göre yapıldığını kontrol etmek için, tüm İşletim Sistemi, Uygulama ve Veritabanı kurulumlarını her sene gözden geçirir. Bilgi Güvenliği Yöneticisi, gözden geçirme sonucunda tespit edilen bulguları Bilgi İşlem yöneticisi ve diğer Güvenlik Kurulu üyelerine raporlar. Sistem, iş istasyonları ve üretim sistemlerine yüklenen işletim sistemleri için uygun lisanslar edinilir. İşletim sisteminin yüklenmesinden sonra, kullanıma geçilmeden önce, canlı sunucularında işletim sisteminin tam yedeği alınır. Yapılan her değişiklik için uygun sürümün yedeği bulunmalıdır. İşletim sistemi komutlarına doğrudan ya da hassas programlar üzerinden erişim, iş tanımlarından dolayı bu erişime sahip olması gereken kullanıcılarla kısıtlanır. Her sistem yöneticisi, kendi sorumluluğundaki veri dosyalarının ve temel programların bir kaydını tutmakla yükümlüdür. Sistem yöneticisi bu dosyalara erişimi ve bu dosyalardaki değişiklikleri takip eder. Düzenli olarak işletim sistemi güncellenir, örneğin yeni çıkan bir sürümü ya da yamayı yüklemek için güncelleme yapılır. Değişiklikler meydana geldiğinde, operasyon veya güvenlik üzerinde zararlı bir etki

oluşmaması için uygulama sistemleri gözden geçirilir ve test edilir. Değişiklikler, değişiklik yönetimi sürecine göre Bilgi İşlem Müdürünün onayıyla hayata geçirilir. Bu süreç şunları kapsar: İşletim sistemi değişikliklerinin uygulama kontrollerine ve bütünlük prosedürlerine zarar vermediğini Bilgi Güvenliği Yöneticisi kontrol eder. İlgili sistem yöneticileri, uygulamaya geçilmeden önce uygun gözden geçirmelere imkân vermek için, Bilgi İşlem yöneticisini işletim sistemi değişikliklerinden zamanında haberdar eder. Bilgi İşlem Müdürü tüm güvenlik ve sistem denetim araçlarının ana sahibidir. Bu araçlar sadece Bilgi İşlem Müdürü veya Bilgi İşlem Müdürü tarafından atanmış Bilgi Güvenliği Yöneticisi veya Bilgi Güvenliği Yöneticisi tarafından atanmış kimseler tarafından kullanılır. Bu yazılımlara erişim, bu dokümanda açıklanan Erişim Kontrolü prosedürlerine göre verilir.

5.5 Kullanıcı Erişim ve Faaliyetlerinin İzlenmesi

- Tüm kullanıcı faaliyetlerinin, işletim sistemi, uygulama, veritabanı ve ağ bileşenleri seviyesinde denetim izi tutulur. Eğer denetim izi alınması sistem performansını düşürüyorsa, sistem/ağ/uygulama yöneticileri, Bilgi İşlem yöneticisi ile beraber denetim izi tutulması gereken kritik komutlar veya faaliyetleri belirler veya hutta performansı artırmak için gerekli ilave yatırım planı hazırlarlar. Bilgi İşlem Yöneticisi seçilen denetim izi kriterlerini onaylar.
- Sistem, ağ ve uygulama yöneticileri, sistemler üzerinde raporlanması gereken kritik işlemleri ve bunlarla ilgili tanımlanması gereken alarmları) belirleyerek, bunları Bilgi İşlem yöneticisine onaylatır.
- Sistem ve ağ yöneticileri, sistemden gelen alarmları inceler ve gerekli durumlarda vaka/olay kaydı açar.

5.5.1 Uygulama ve İşletim Sistemi Seviyesinde Denetim Kaydı Tutulması

Tüm uygulama, işletim sistemi ve ağ donanımlarının denetim kaydı konfigürasyonu açık olur. Denetim kaydı dosyaları şu kayıtları içerir:

- Sisteme giriş denemesi (başarısız / başarılı)
- Kilitlenen kullanıcı hesapları
- Tüm sistem veya uygulama yöneticilerinin gerçekleştirdiği işlemler
- Bir sistem veya uygulamanın başlatılması, sonlandırılması, yeniden başlatılması (kullanıcı kimliği ve gerçekleştirme zamanıyla birlikte)

İzlenmesi gereken diğer faaliyetler, uygulama, işletim sistemi ve ağ donanımları üzerinde tanımlanan belirli risklere göre tanımlanır. İzlenen olayların seçimi, her olayın ürettiği denetim kaydı miktarına ve denetim kaydı tutmasından ötürü uygulamada oluşan yüke bağlıdır.

Denetim kayıtları şunları içerir:

- Kullanıcı kimlikleri
- Sisteme giriş ve sistemden çıkış tarih ve saatleri
- Varsa terminal veya lokasyon bilgisi

- Başarılı veya başarısız sistem erişimi denemelerinin kayıtları
- Başarılı veya başarısız veri ve diğer kaynak erişimi denemelerinin kayıtları

İşletim sistemi, uygulama ve ağ donanımları denetim kayıtlarını üst üste kaydetmeyecek veya silmeyecek şekilde yapılandırılır. Denetim kaydı dosyalarının yedeklenmesi, yedekleme sorumlularınca, günlük/ haftalık yedekleme işlemlerine dâhil edilir.

5.5.2 Denetim Kayıtlarının Gözden Geçirilmesi

Denetim kayıtları ve sistemin raporladığı alarmlar, ayda bir defa ilgili Bilgi Güvenliği Yöneticisi tarafından örneklem bazlı gözden geçirilir. Ayrıca, her ay, Bilgi Güvenliği Yöneticisi ilgili sistem yöneticileri tarafından gerçekleştirilen gözden geçirmeleri gözden geçirir. Sistem tarafından oluşturulan alarmlar her gün sistem yöneticisi tarafından incelenir ve gerekli olduğunda vaka/olay kaydı açılır.

5.5.3 Sistem Saatlerinin Senkronizasyonu

Sistem saatlerinin doğru ayarlanması, denetim izlerinin doğruluğu için önemlidir. Denetim izlerinin doğruluğu, hukuki durumlarda ya da disiplin davalarında kanıt teşkil etmelerinden ötürü ya da soruşturmalar için gereklidir. Hatalı denetim izleri, soruşturmaları aksatabilir ve kanıtın güvenilirliğine zarar verebilir. Tüm sunucu, ağ donanımları, kamera sistemleri ve masaüstü bilgisayarlarının saatlerinin aynı olmasını sağlayan bir sistem kullanılır. Ağ yöneticileri, kullanıcıların bu ayarları değiştirememesini sağlar.

5.5.4 Çevrimiçi Uçbirimlerinin Bağlantısının Otomatik Zaman Aşımı

Teknik olarak mümkün olan yerlerde, işletim sistemi, terminalleri/ masaüstü bilgisayarları/ dizüstü bilgisayarları, beş dakika çevrimdışı kaldıklarında zaman aşımına uğratacak şekilde yapılandırılır. Tüm işletim sistemleri için ekran koruyucu şifresi kullanılır.

6. İLGİLİ DOKÜMAN

- Erişim Kontrol Politikası
- Bilgi Güvenliği Politikası
- Kabul Edilebilir Kullanım Politikası
- Ağ Güvenliği Politikası