1. AMAÇ

Bu politika, Karamanoğu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesindeki bilgilere ve sistemlere erişimin kural ve ilkelerini oluşturmak amaçlanmıştır.

2. KAPSAM

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

3. SORUMLULAR

- Tüm Bilişim Kullanıcıları
- Bilgi İşlem Daire Başkanlığı ve Birimleri

4. TANIMLAR

5. UYGULAMA

5.1 Erişim Kontrolü için İş Gereksinimi

Kurum bilgilerine ve bilişim sistemlerine (işletim sistemleri, uygulamalar, veritabanları, ağ donanımları ve diğerleri) erişim hakkı "en düşük erişim hakkı" ve "bilmesi gereken" ilkelerine bağlı kalınarak verilir. Her bir uygulama veya sistemin yetkisiz erişim, değişiklik, gizliliğinin ihlali veya zarar görmeye karşı korunması için uygun seviyede erişim kontrolü içeren prosedürler uygulanır. Bu şekilde, bilginin doğru, gizli ve erişilebilir olması sağlanır. (Bilgi Güvenliği Prosedürleri "Kullanıcı Hesap Yönetimi")

5.2 Kullanıcı Erişimi Yönetimi

5.2.1 Kullanıcı Kaydının Yapılması ve Silinmesi

Bilişim sistemlerine ve hizmetlerine ait tüm erişimler, erişim verilmeden önce erişim hakkının onaylanmasını sağlayan Erişim Kontrolü Prosedürü üzerinden sağlanır. Bilişim sistemlerine ve hizmetlerine erişimlerin kaldırılmasına yönelik otomatik veya zamanında bildirmeyi de sağlayacak resmi bir erişim silme süreci izlenir. (Bilgi Güvenliği Prosedürleri "Erişim Kontrolü Prosedürleri ")

5.2.2 Mantıksal Erişim Yetki Yönetimi

İşletim sistemi, iş uygulamaları, veritabanları ve ağ donanımları gibi her tip bilişim sistemine erişim yetkileri tanımlanır ve dokümante edilir. Erişim yetkileri, kişilerin iş tanımlarına ve görevlerine göre ve gerekli onayların ardından verilir. Kişinin iş tanımının gerektirdiği erişim yetkilerinin dışındaki ek erişimler için ilgili birim müdürünün ve bilgi işlem müdürünün onayı alınır.

5.2.3 Kullanıcı Şifre Yönetimi

Tüm kullanıcı şifreleri (kullanıcı şifreleri ya da yönetici "administrator" şifreleri) gizli tutulur, kesinlikle paylaşılmaz, e-posta yoluyla bir başkasına iletilmez ya da herhangi bir şekilde deşifre edilemez. Kullanıcı oluşturma süreci esnasında kullanıcıya güvenli yollardan bir ilk şifre sunulur. Ayrıca sistem kullanıcının ilk girişinde kullanıcıyı hemen şifresini değiştirmeye zorlayacak şekilde yapılandırılır. Kritik bilişim sistemleri için yönetici (administrator) şifrelerinin saklanması ve yönetilmesine yönelik uygun prosedürler uygulanır.

Sistem kısıtları ya da iş gereksinimlerinden ötürü herhangi bir şifre ya da kullanıcı hesap politikası uygulanamıyorsa, bu duruma özel onay mekanizmaları ve bu durumdan kaynaklanacak riskin azaltılması için özel kontroller oluşturulur. Kişiye özel kullanıcı kimliği ve şifresinin oluşturulamadığı uygulamalar için, erişim yetkilerinin kısıtlanması ve denetlenmesi için alternatif çözümler uygulanır. Kurumda ortak kullanıcı hesabı ve şifresinin kullanılması ancak, Sitem Yöneticisi ve talep eden kullanıcının birim yöneticisinin onayına istinaden açılır. Ortak kullanıcı hesabı ve şifresinin kullanılması durumları kaydedilir ve ancak belli aralıkta kullanıma açılabilir.

5.3 Kullanıcı Sorumlulukları

Bkz. Kabul Edilebilir Kullanım Politikası

5.4 İşletim Sistemi Erişim Kontrolü

Tüm işletim sistemleri ve kritik uygulamalar için Asgari Güvenlik Standartları (AGS) veya sistem güvenliği sıkılaştırma standartları (hardening standards) oluşturulur ve uygulanır. Tüm işletim sistemleri ve uygulamalar AGS' ye göre yapılandırılır. İşletim sistemlerine erişim güvenli bir sistem giriş prosedürü ile kontrol edilir. Çeşitli sistemlere erişilmesi için gerekli kullanıcı bilgileri bir kullanıcı kimliğinden (ID) ve şifresinden veya kullanıcıya özel diğer bilgilerden (dijital sertifikalar, belirteç (token) vb.) oluşturulur. Kullanıcıların aynı işlem ortamında birden fazla kullanıcı hesabı olmaz. Zorunlu bir durum değilse, ortak kullanıcı kimlikleri kullanılamaz. Ortak kullanıcının gerekli olduğu durumlarda, erişim sağlanmadan önce ilgili yöneticilerden onay alınır. Ayrıca, kullanıcı kimlikleri kullanıcılar arasında hiçbir koşulda paylaşılmaz. İşletim sistemi seviyesinde şifre gereksinimlerine bağlı kalınması için gerekli kısıtlamalar oluşturulur. Uygulanabilir yerlerde, sistemin üzerine yazma işlemi gerçekleştirebilecek sistem yardımcı programlarına ve uygulama kontrollerine erişim, kullanıcıların iş tanımlarını gerçekleştirebilmek için gerekli olandan daha fazla bilgi elde edemediklerinin kontrol edilmesi gereklidir. Sistem programlarına erişim, son kullanıcıların problemlerini çözmeye yardımcı olmaları için yalnızca yönetici görevindeki (administrator) kullanıcılarla sınırlı tutulur. İşletim sistemleri, uygulamalar, veritabanları ve terminaller veya sunucular inaktif kaldıkları durumlarda belirli bir süre sonra zaman aşımına uğrar ve/veya ekran koruyucusu otomatik olarak devreye girer. (Bilgi Güvenliği Prosedürleri "İşletim Sistemleri, Uygulamalar & Veritabanları")

5.5 İşletim Sistemi, Uygulamalar ve Veritabanları

Kullanıcıların ve destek personelinin bilgi ve uygulama sistem fonksiyonlarına erişimi, erişim kontrolü politika ve prosedürlerine göre kısıtlanır. Bilgi Güvenliği Yöneticisi veya onun bu görevi atayacağı kişi yılda en az bir defa uygulama güvenliğinin sağlanıp

sağlanmadığını denetler. Kurumun üçüncü kişi uygulamaları kullanması durumunda, üçüncü kişi tedarikçilerin sistemlere yeni uygulama kurarken Asgari Güvenlik Standartları'na uydukları denetlenir. Sistemler üzerinde kurulu olan uygulamalar yılda en az bir defa gözden geçirilir. Uygulamalar ve hassas sistemler varlık envanterinde belirlenmiştir ve gerekli görülen kritik uygulamalar normal bilgi işlem ortamlarından ayrılmıştır.. Paylaşımda olan bir ortamda hassas bir uygulama çalıştırılacağı zaman, uygulamanın sahibi ve Bilgi Güvenliği Yöneticisi ile uygulamanın kaynak paylaşımında bulunduğu uygulama sistemleri belirlenir. Çalışanlar, hiçbir uygulama sisteminin veritabanına doğrudan erişemez. (Bilgi Güvenliği Prosedürleri "İşletim Sistemleri, Uygulamalar & Veritabanları") Bkz Varlık Envanteri

5.6 Ağ Erişimi Kontrolü

Bkz. Ağ Güvenliği Politikası

6. İLGİLİ DOKÜMAN

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