KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ

BİLGİ İŞLEM DAİRE BAŞKANLIĞI

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Hazırlayan		Onaylayan

İçindekiler

1. KAPSAM

Karamanoğlu Mehmetbey Üniversitesi Kabul Edilebilir Kullanım Politikası, tüm Kurum çalışanlarını kapsar. Politika maddeleri hem Kurum içindeki hem de Kurum dışındaki kullanım için geçerlidir.

1.1 Kişisel Bilgisayar Tahsisi Politikası

Kurum çalışanlarına, görev tanımları gereği Bilgi Teknoloji donanımı tahsis edilir, kullandırılır ve yenilenir. Bilgisayar tahsisinde satın alma yöntemi ve donanım kullanım yönetmeliği tercih edilir.

Tahsis edilecek donanım, her çalışana İlk Biriminden gelen onaya istinaden görev tanımına veya Kurum tarafından belirlenmiş donanım kullanım kriterlerine uygun olarak verilir. Her seviyedeki çalışana normal kullanım ihtiyaçları çerçevesinde standart uygulamaların bulunduğu donanım tahsis edilir.

Masaüstü ve dizüstü bilgisayarların satın alma tarihinden itibaren en az beş yıl kullanılması hedeflenir. Beş yıllık kullanım süresi içinde kişinin kullanıcı profilindeki herhangi bir değişiklik sebebiyle bilgisayarının değiştirilmesi gündeme gelirse, mevcut bilgisayar kuruluş veya topluluk bünyesinde başka bir uygun kullanıcıya verilir.

Fotoğraf makinesi, video kamera, projeksiyon cihazı veya perdesi, harici disk ünitesi, harici CD yazıcı, tarayıcı vb. diğer çevre birimleri ile görsel ve işitsel dijital cihazlar, Bilgi İşlem Daire Başkanlığı onayı ile alınır.

1.2 Kişisel Kullanım Politikası

Kurum bilgisayar ve iletişim sistemlerinin kişisel kullanımı gerekli olduğu durumlarda kısıtlama yapılır. Kişisel kullanım, e-posta zincirlerinin yayılmasına yardımcı olmak veya oluşturmak, uygunsuz veri ve resim alışverişi yapmak, iş aramak, kumar oynamak ve politik aktivitelere katılmak gibi hareketleri içermez. İş ile ilgisi olmayan kişisel dosyalar lisans ihlaline ve Bilgi İşlem Daire Başkanlığının belirlemiş olduğu kapasite sınırlarının aşımına neden olmadığı sürece Kurum bilgi sistemlerinde saklanabilir.

1.3 Kurum Kaynaklarının Yasalara ve Etik Prensiplerine Uygun Kullanımı

Kurum personeli, internet kullanımı ve sesli haberleşme aktiviteleri dâhil olmak üzere, tüm bilgi sistemleri ve iletişim imkânlarının kullanımında ve bu imkânların sağlanmasında, başta 5651 numaralı yasa olmak üzere ilgili Türkiye Cumhuriyeti yasalarına, uluslararası hukuka ve genel etik kurallarına uymakla yükümlüdür. Kullanıcılar, bilgisayarlarında bulunabilecek standart iş ve ofis uygulamaları dışındaki yazılımlar (Kurum Bilgi İşlem Daire Başkanlığı tarafından kurulmuş işletim sistemi, virüs koruma, ofis uygulamaları, iş uygulamaları vb. dışındaki yazılımlar) için telif hakkı koruma düzenlemelerine uymakla şahsen sorumludur.

Diğer kullanıcıların kimlik doğrulama ve erişim kontrol araçlarını (VPN, fiziksel geçiş kontrol kartı vb.) ele geçirmeye çalışmak, Kurum kaynaklarına zarar vermek ya da üçüncü taraflara Kurum kaynaklarını kullanarak zarar vermek etik kurallarına ve yasalara aykırı olup kabul edilemez. Kullanıcılar teknik olarak mümkün olsa bile iş sorumlulukları gereği erişim ihtiyacı olmayan kaynaklara erişmemelidirler. Kullanıcılar bu hususlarda bir zafiyet fark ederse Bilgi Güvenliği Yöneticisini bilgilendirmekle yükümlüdür.

Tüm iletişimde genel prensip olarak Kurumsal ve genel etik ve nezaket kurallarına uyulmalıdır. Ayrıca iletişim sırasında Kurum çalışanlarına, müşterilere ve diğer taraflara zarar verecek hakaret içeren ifadeler kullanılamaz. Kurum, bilgi kaynaklarının personel tarafından yasal olmayan şekilde kullanımı halinde yasa uygulayıcılar ile işbirliği yapacaktır.

Kullanıcılara Bilgi Güvenliği Yöneticisi ve Bilgi İşlem Daire Başkanı onayı ile "yerel yönetici (local Kurumun)" yetkisi geçici süre için verilir.

Kullanıcılar bilgisayarlarında kurulu olan ve Kurum güvenlik politikalarında yer almayan yazılımların lisanslarının tam olmasından sorumludur.

1.4 Konfigürasyon ve Güvenlik Ayarları

Kullanıcılar teknik olarak mümkün olsa bile bilgisayarlarındaki güvenlik ayarlarının düzeyini düşürmemelidir. Güvenlik ayarlarına örnek olarak; MS Internet Explorer, MS Outlook'u etkileyen güvenlik alanları ayarları (Internet Explorer Security ZoneSettings), işletim sistemi güncelleme ayarları, virüs programı ayarları, BIOS ayarları ve diğer donanımsal ve yazılım güvenlik ayarları sayılabilir. Kullanıcılar bilgisayarlar üzerinde yeni kullanıcı oluşturamaz ve mevcut kullanıcıların hakları ve kullanıcı gruplarını değiştiremez. Eğer iş ihtiyaçları gereği yapılandırma ve güvenlik ayarlarının değiştirilmesi gerekiyor ise Bilgi İşlem Daire Başkanlığı'nın onayına başvurulur. Konfigürasyon ve güvenlik ayar değişiklikleri Bilgi İşlem Daire Başkanlığı tarafından yapılır.

Virüslere ve zararlı yazılımlara karşı güvenliğin sağlanabilmesine yönelik olarak aşağıdaki önlemler alınır.

- Kullanılan bilgisayarda hazırlanmamış her tür bilgi teknolojisi medyası (CD, disket, teyp vb.) virüs kontrolü yapıldıktan sonra kullanılır.
- Güncel virüs yazılımı Bilgi İşlem Daire Başkanlığı tarafından sağlanmakla beraber Kurum kullanıcıları, bilgisayarlarındaki anti virüs yazılımının aktif olmasından sorumludur.
- İlgisiz ya da şüpheli mesajlar açılmamalı ve bilgisayardan silinmelidir. Şüpheli durumlarda Bilgi İşlem Daire Başkanlığı bilgilendirilir.

1.5 Kuruma Ait Olmayan Bilgisayarlar

Kuruma ait olmayan bilgisayarlar sadece iş gereği ve Bilgi İşlem Daire Başkanlığı'nın ve Bilgi Teknolojileri Yöneticisinin onayı ile Kurum ofis ağına bağlanabilirler. Bilgi Teknolojileri Personeli 3. Parti çalışanları Kurum ofis bilgi ağına izinli olarak bağlar. Kuruma ait olmayan bilgisayarlarda Bilgi İşlem Daire Başkanlığı teknik kontroller uygulama ve ayar değişiklikleri yapma / yaptırma hakkına sahiptir.

1.6 Ofis Araç Gereçlerinin Fiziksel Güvenliği

Sistem odası içerisindeki cihazların yakınında yiyecek, içecek gibi gıda maddeleri tutulamaz. Kritik sunucular sistem odasında, kritik ofis ekipmanları güvenli alanlarda barındırılır. Kullanıcıların doğrudan sorumluluğunda veya ortak kullanımda olan bilgisayarlar ve diğer ofis araçlarını olumsuz etkileyebilecek çevresel etkenler (sıcaklık, nem, aşırı toz, vb. gibi) Bilgi Güvenliği Yöneticisine bildirilir.

1.7 Güvenlik Olay ve Zafiyetlerinin Raporlaması

Kullanıcılar günlük işlerini yaparken güvenlik olaylarına ve zafiyetlerine karşı duyarlı olmalıdır. Fark edilen her zafiyet, riskin gerçekleşmesi zayıf bir olasılık olsa bile en kısa zamanda Bilgi Güvenliği Yöneticisine raporlanmalıdır. Bu duruma örnek olarak, kullanıcı bilgisayarlarında virüs bulunmasından şüphelenmesi, kullanıcı parolasının başkaları tarafından öğrenilmiş olmasından şüphelenilmesi veya erişim araçlarının (VPN, fiziksel geçiş kontrol kartı vb. gibi) kaybedilmesi/çalınması, dizüstü veya avuç içi bilgisayar kaybedilmesi/çalınması, erişim kontrollerindeki zafiyet, davetsiz ve şüpheli misafir, kullanıcı girişinin reddedilmesi ve hizmet kesintisi gibi beklenmeyen durumlar verilebilir. Dizüstü ve avuç içi bilgisayarların, kritik öneme sahip dokümanların ve veri saklama cihazlarının kaybı veya çalınması durumunda en kısa zamanda Bilgi İşlem Daire Başkanlığı bilgilendirilir.

2. HESAP VEREBİLİRLİK

2.1 Hesap Verebilirlik

Kullanıcıya atanmış erişim araçları hiçbir şart altında teknik personel dâhil kimseyle paylaşılamaz. Erişim araçlarına örnek olarak; parola, VPN, fiziksel geçiş kontrol kartı vb. verilebilir. Bilgi İşlem Daire Başkanlığı hiçbir zaman kullanıcılardan şifrelerini ve PIN kodlarını söylemelerini, yazılı iletmelerini, fiziksel araçlar için vermelerini (görevden ayrılma durumu hariç) isteyemez. Eğer kullanıcılar erişim ile ilgili konularda destek için telefon ile iletişim kuruyorsa, özellikle karşı tarafın araması durumunda, arayan kişinin kimlik doğrulamasını yapar. Şüpheli telefon aramaları veya mesajlar, edinilmesi mümkün olan detay bilgiyle birlikte Bilgi Güvenliği Yöneticisine raporlanır.

2.2 Kullanıcı Kimliği

Kullanıcıların Kurum sistemleri üzerinde kendilerine ait olmayan kullanıcı kodlarını (veya genel anlamıyla kimliklerini) kullanmaları, kullanıcı kimliklerini çeşitli yöntemlerle gizlemek amacıyla jenerik kullanıcı olarak sisteme erişmeleri acil durumlar dışında yasaktır. Bu çerçevede e-posta iletilerindeki gönderen kısmında bir kimlik bilgisi bulunmaktadır ve bu alanın yanıltıcı biçimde değiştirilmesi yasaktır. Kullanıcılar (Bilgi İşlem Daire Başkanlığı Personeli dahil) jenerik / ortak hesap kullanımından kaçınmalı, kişiye özel kullanıcı hesabı kullanımında teknik kısıtlar olması durumunda Bilgi İşlem Daire Başkanlığına çözüm talebiyle başvurmalıdır. Jenerik / ortak kullanıcı hesabı kullanımı sadece teknik imkânsızlık

veya çözüm maliyetlerinin uygun olmaması durumunda, izleme kontrollerinin uygulanması şartı ve Bilgi Güvenliği Yöneticisinin onayı ile mümkündür.

2.3 Parola (Şifre) Kriterleri

Kurum sistemleri teknik olarak mümkün olan durumlarda parola karmaşıklık ve değişiklik kontrollerini teknik olarak uygulayacak biçimde yapılandırılmıştır. Kullanıcılar parola kriterlerinin teknik olarak zorlanmasının mümkün olmadığı durumlarda aşağıdaki belirtilen kriterlere uymakla yükümlüdür.

- Minimum şifre uzunluğu 8 karakterdir
- Şifre bileşimi; alfa nümerik, büyük ve küçük harfler ve en az bir özel karakter (bunlardan en az üçü sağlanmalıdır)
- 5 hatalı giriş denemesinden sonra kullanıcı hesabının kilitlenmesi
- Kullanıcı adı ve şifrelerinde İngilizce karakter harici kullanılmaz.
- Şifre girişi sırasında başkalarının izlemediğinden emin olunur.
- Kullanıcı şifresi kişiye özeldir ve başkaları ile paylaşılamaz.
- Bilgisayar başında bulunulmayacağı durumlarda şifre korumalı ekran kilitleme sistemleri aktif duruma getirilir veya bilgisayar kapatılır.

Bkz Parola Politikası

3. İNTERNET KULLANIMI

3.1 Kurumsal ve Kişisel Bilgilerin İnternet Üzerindeki Web Sitelerine Verilmesi

Kullanıcılar İnternet üzerindeki tartışma gruplarına, sohbet odalarına ve diğer forumlara Kurum adres ve telefon bilgilerini, personel isimlerini, unvanlarını, e-posta adreslerini ve diğer kişisel bilgilerini iş gerekleri ve kanuni gereklilikler dışındaki durumlarda aktarmamalıdır.

3.2 İnternet'ten Dosya İndirme

Kullanıcılar iş gereksinimleri için İnternet'ten veri dosyaları indirebilir, ancak bu işlemden önce anti-virüs imzaları ve işletim sistemi yamalarının güncelliğini kontrol eder.

4. MESAJLAŞMA KULLANIMI

4.1 E-Posta Kullanımı

Elektronik Mesajlaşma kuralları yazılı ve yüz yüze olmak üzere aynı özellikleri taşırlar. Yüz yüze iletişimin mümkün olmadığı durumlarda elektronik mesajlaşma kullanılır. Adres listesinde yer alan gruplara mesaj gönderilirken alıcıların tamamının gönderilecek mesajı almak isteyeceğinden emin olunur. Mesajın doğrudan muhatabı ve gerekiyor ise

aksiyon alması gereken kişiler KİME (TO) alanına, bir aksiyon alması gerekmeyen ve sadece bilgilendirme amacı ile mesaj gönderilen kişiler BİLGİ (CC) alanına yazılır. Mesajlara iliştirilecek dosyaların büyüklükleri önemlidir. Özellikle grafikler ve resimler çok yer alacağından dikkat edilmeli ve mümkünse göndermeden önce sıkıştırılmalıdır. Elektronik mesajlar için belirlenmiş sınır 20MB'dır. Bu büyüklüğü geçen elektronik mesajlar yollanamayacak ve alınamayacaktır.

4.2 Mesajlaşma Mahremiyeti

Kurum içerisinde kullanılan bir anlık mesajlaşma sistemi bulunmamakla birlikte yapılan tüm elektronik iletişimin kişiye özel olacağı garantisi verilmez. Kullanıcılar elektronik ortamdaki her türlü iletişimlerinin kötü niyetli kişilerin saldırılarına maruz kalabileceğini bilmelidir. Bu nedenle kritik Kurum bilgilerini içeren iletişimin, hem iletişim hattında hem de ulaştığı alıcı noktasında gizlilik ve bütünlüğünün korunabilmesi için şifreleme yöntemleri ile yapılması gereklidir. Kullanıcılar gizlilik ihtiyacı olan iletişimleri için teknik çözüm konusunda Bilgi İşlem Daire Başkanlığına başvurabilirler. Teknik olanaksızlık veya karşı taraftan kaynaklanabilecek uyumsuzluk nedeniyle şifrelemenin mümkün olmadığı kritik iletişimin yapılması Bilgi Teknolojileri Yöneticisinin onayı ile gerçekleştirilir.

4.3 Kimlik Hırsızlığı (Phishing) Saldırıları, Mesaj Ekleri Politikası ve İstenmeyen (Spam) E-Postalar ve Yasak kullanımlar

Kurum, çalışanların e-posta adreslerine gelen istenmeyen e-posta ve virüs eklentilerine karşı teknik önlemler uygulamaktadır. Buna rağmen son kullanıcılar saldırı yöntemlerinin yeni olması, ya da korunma yöntemlerinin hatalı çalışabilmesi veya bazı durumlarda bu yöntemlerin bazı saldırılara karşı yetersiz kalmaları sebebi ile genel e-posta güvenlik kurallarına uymalıdır. Kullanıcıların;

- Kişileri rahatsız edici, müstehcen, politik ve dini propaganda yapan veya Kurumsal değerlere aykırı içerikler taşıyan elektronik mesajları oluşturmak veya dağıtmak ve bu sitelerdeki diyaloglarda yer almak.
- İnternet aracılığı ile rastgele, tehdit edici ve saldırgan yazı/mesaj göndermek.
- Şans mektupları veya zincir mektuplarını içeren mesajları oluşturmak veya dağıtmak.
- Telif hakkı yasalarına uygun olmayan bilgileri içeren mesajları ve eklerini oluşturmak veya dağıtmak.
- Kaynağının izni olmadan bir mesajı ve ekini değiştirerek veya kopyalayarak dağıtmak.
- Şifre güvenliğine aykırı olarak şifrelerin herkes tarafından görülmesini sağlamak gibi aktivitelerde bulunmaları yasaktır.

Bunlara ek olarak e-posta içinde gelen bağlantılara tıklayarak (kullanıcı kodu ve parolası başta olmak üzere) hiçbir kişisel bilgilerini girmemeli, HTML formatında gelen e-postalardaki resimleri görüntülemek için indirmemeli, e-posta içindeki herhangi bir bağlantıya tıklamamalı, güvenilir kaynaklardan gelmeyen e-postalardaki eklentileri indirmemeli ve gönderen kısmındaki bilginin yanıltıcı olabileceğini unutmamalıdır.

E-posta içindeki herhangi bir bağlantıya tıklamak veya e-posta içindeki resimleri görüntülemek üzere indirmek istenmeyen e-postanın var olan bir kullanıcıya ulaştığı bilgisini saldırgana verir. Ayrıca resim indirme veya linki ziyaret etme işlemi resim işleyici uygulamalardaki açıklardan dolayı bilgisayarınızın zarar görmesine veya "Cross Site Scripting – XSS" adı verilen istemci tarafında çalışan betiklerin kötü niyetle kullanılmasına ve oturum hırsızlığı saldırılarına imkân verebilir.

5. OFİS EKİPMANLARI, BASILI DOKÜMANLAR VE TAŞINABİLİR VERİ SAKLAMA ARAÇLARI

5.1 Yazıcılar ve Fotokopi Makineleri

Kullanıcılar gizlilik gereksinimi yüksek bir dokümanı yazdırırken, bilginin yetkisi olmayan kişiler tarafından görülmesini veya ele geçirilmesini engellemek için yazdırma esnasında yazıcının yanında bulunmalıdır. Kullanıcılar gizlilik gereksinimi olsun veya olmasın makineye sıkışmış dahi olsa orijinal ve kopya doküman nüshalarını yazıcı ve fotokopi makinelerinde terk edemez. Telif hakkı Kuruma ait olmayan dokümanların, Kurumun yazıcı ve fotokopi makinelerinde çoğaltılması yasaktır. Yazıcı ve fotokopi makinelerinin aşırı kişisel kullanımı yasaktır.

5.2 İhtiyaç Kalmayan Basılı Dokümanların İmha Edilmesi

İmha edilecek tüm hassas dokümanlar, doküman parçalayıcı makine (shredder) ile parçalanır. Gizlilik gereksinimi olmayan diğer dokümanlar ofis içi veya dışında rastgele bölgelerde bırakılmaz ve kâğıt atık geri dönüşüm kutularına atılır.

5.3 Faks Makineleri

Faks makineleri ile iletilen doküman/verilerde şifreleme olmadığı ve karşı tarafta çıktının iletilmek istenen kişiden farklı bir kişi tarafından alınabilecek olması nedeniyle; kullanıcılar yüksek düzeyde gizlilik gereksinimi olan bilgilerin gönderiminde verinin açıkta gönderildiği ve hedef noktaya ulaştığında açık olarak görüntülenen teknolojileri tercih etmemelidir. Bu tür gereksinimlerin doğması durumunda kullanıcılar Bilgi Güvenliği Yöneticisi ve Bilgi İşlem Daire Başkanlığı Yetkilisi 'ne başvurur. Faks kullanımına imkân tanıyan veya faks kullanımını zorunlu kılan durumlarda şu kontroller uygulanır:

- Hassas dokümanlar (Kişilere Özel ve Gizli) alıcı tarafından alıcı cihazın başında beklenmesi durumunda gönderilir, otel veya postane gibi yerlerden mümkünse gönderilmez. Eğer gönderilmesi gerekiyorsa hizmet personeline teslim edilmez.
- Hassas bilginin iletildiği bilgisi en kısa zamanda teyit edilir.
- İmza içeren veya talimat nitelikli dokümanların kabulü durumunda mutlaka orijinal nüshaları alınır (orijinal nüshaların takibi gereksinimi elektronik olarak taranmış dokümanlar için de geçerlidir).

5.4 Taşınabilir Veri Saklama Araçları

Taşınabilir olmaları nedeniyle çalınma tehdidiyle karşı karşıya olan taşınabilir veri saklama araçlarının, özellikle kritik veri barındırmaları durumunda fiziksel güvenliği kullanıcıların sorumluluğundadır. Verinin saklanma ihtiyacı sona erdiğinde veriler saklama cihazından(hard disk, USB bellek, vb.) silinir.

6. İZLEME VE KAYIT AKTİVİTELERİ, MAHREMİYET

6.1 Kurum Sistemlerinde Saklanan veya Kurum Sistemleri Aracılığı ile İletilen Verinin Mahremiyeti

Kurum, kendi sistemleri üzerinde saklanan ve kendi sistemleri aracılığı ile iletilen tüm bilgileri inceleme hakkını saklı tutar.

6.2 Kayıtlar

Kurum, iç ve dış saldırılara karşı katmanlı güvenlik anlayışı gereği geliştirdiği loglama (denetim izi tutma) stratejisini uygulamaktadır. Bu loglama stratejisi özellikle kullanıcı faaliyetlerini izleme amacına yönelik olmamakla birlikte, kullanıcıların uygulamalar ve Kurum bilgi ağı üzerinde gerçekleştirdiği faaliyetler kayıt altına alınmaktadır. Kullanıcıların, Kurum sistemleri üzerinde veya Kurum sistemlerini kullanarak yasal mevzuata veya Kurum içi kurallara aykırı davranışlarından şüphe edilmesi halinde Kurum yönetiminin resmi talebi üzerine kullanıcılar, bilgi sistemleri üzerindeki faaliyetlerinin izlenebileceğinin bilincinde olmalıdır.

7. GENEL VERİ KORUMA VE SINIFLANDIRMA SORUMLULUKLARI

7.1 Bilgi Paylaşımı, Veri Sahipliği ve Sınıflandırılması

Kurum içi bilgi paylaşımı sadece görev gereği ilgili veriye ulaşması gereken kullanıcılar arasında olabilir. Kamu Kurumları ve üyeler ile bilgi paylaşımı bu irtibat görevini yerine getirmek üzere atanmış personel tarafından gerçekleştirilir.

Kullanıcılar kendileriyle ilgili iş verilerinin sahibi olup, bu varlıkların korunmasından nihai olarak sorumludur. Veri sahipleri kendileriyle ilgili iş verilerinin sınıflandırılmasından ve gerektiğinde yeniden sınıflandırılmasından sorumludur. Verinin çevrim içi saklanabileceği gibi, çevrim dışı ve basılı doküman halinde de saklanabileceği unutulmamalıdır. Veri sınıflandırma hakkında daha detaylı bilgi almak için Kurum bünyesinde bulunan Bilgi Güvenliği Yöneticisine danışılır.

7.2 Kurum Verisinin Saklanması

Kullanıcılar sahibi oldukları iş verilerinin yasal yükümlülükler veya iş gereklerinden doğan saklanma süre ve şart ihtiyaçlarını Bilgi Güvenliği Yöneticisine bildirmekle yükümlüdür. Basılı dokümanlar üzerinde bulunan veriler de bu maddenin kapsamı içindedir. Genel prensip olarak üzerinde çalışılan dosyalar ve kritik olmayan dosyalar kişisel bilgisayarlarda saklanabilir. Ancak kritik dosyalar üzerinde çalışılmadığı durumlarda kişisel bilgisayarlardan silinir ve sunucularda saklanır. Kullanıcılar veri saklama konusunda Kurumun merkezi veri saklama prosedür ve/veya yöntemlerini kendi yöntemlerine tercih etmeli ve sahibi oldukları kritik verilerin Kurumsal yedekleme prosedürlerine dâhil olduğundan emin olmalıdır. Kullanıcılar ortak paylaşım alanları dışındaki verilerinin güvenliğinden ve yedeklenmesinden sorumludur.

7.3 Dizüstü Bilgisayarları ve Avuç İçi Bilgisayarlar Kullanımı

Kullanıcılar, hassas Kurum verilerini Kurumun diz üstü bilgisayarlarında ve avuç içi bilgisayarlarda saklamaktan kaçınmalıdır. Bu cihazların kullanıcıları özellikle halka açık mekânlarda cihazlarını terk edemez ve cihazların fiziksel güvenliğini sağlamakla yükümlüdürler. Kullanıcılar kendilerine tahsis edilen dizüstü bilgisayarları kullanmadıkları durumlarda kilitli dolap veya çekmecelerde saklamalılardır. Uçak, otobüs gibi halka açık ulaşım araçlarında taşınabilir cihazlar kafa üstü bagajlarına değil koltuk altına konulmalıdır. Havaalanı, tren ve otobüs garlarında taşınabilir cihazları güvenlik kontrollerinden geçirilirken sürekli olarak izlenmeli ve göz teması kesilmemelidir. Taşınabilir cihazlar Kuruma uzaktan erişim için kullanılıyorsa, erişim için kullanılan kullanıcı adı ve parola bilgileri bilgisayar üzerinde herhangi bir dosya içinde saklanmamalıdır.

7.4 Ofis Dışına Gönderilen Bilgisayarlar ve Veri Saklama Araçları

Eğer kişisel bilgisayarlar veya bu bilgisayarlara ait depolama birimleri tamir veya hibe amacı ile Kurum dışına gönderilecekse, bu bilgisayarların kullanıcıları ve Bilgi İşlem Daire Başkanlığı bilgisayar üzerinde bulunan hassas verilerin silinmesi ve gerekiyorsa yedeklenmesinden nihai olarak sorumludur.

7.5 Kurum Ağına Uzaktan Erişim

Kurum ağına uzaktan erişmesi gereken kullanıcılar erişim için, sıra dışı bir neden yoksa Kurumun dizüstü bilgisayarlarını kullanır. Kullanıcılar uzaktan erişim araçlarını (VPN) koruma konusunda diğer erişim araçlarının korunmasına nazaran daha üstün hassasiyet göstermelidir. Uzaktan erişim kimlik doğrulama için kullanılan cihazların üzerine Kurum veya kullanıcıyla ilgili bir erişim bilgisi (telefon numarası, sunucu adı, IP adresi, kullanıcı kodu, vb. gibi) yazılmaz / yapıştırılmaz. Eğer sıra dışı bir durum için Kurum bilgisayarı dışında bir bilgisayardan uzaktan erişim yapılması gerekiyorsa Bilgi İşlem Daire Başkanlığının onayı alınır. Halka açık bilgisayarların uzaktan erişim için kullanımı her koşulda yasaktır (E-Posta erişimleri hariç). Kullanıcılar, Kurum bilgisayarı dışında bir

bilgisayar kullanmak zorunda olduklarında Bilgi İşlem Daire Başkanlığının önereceği kontrolleri uygulamakla yükümlüdür (çalışılan bilgisayar üzerinde iz bırakmamak için sanallaştırma (virtualization) yazılımı kullanmak, kullanılan bilgisayarın kişisel koruma duvarının olması, şifre hatırlama seçeneğinin seçilmemiş olması, anti-virüs imzalarının ve işletim sisteminin güncel olması gibi).

Kurum dışından, Kurum sistemine herhangi bir üçüncü partinin uzaktan erişmesi gerekiyor ise Bilgi İşlem Daire Başkanlığının onayı dâhilinde süreli ve sadece ilgili sunuculara ait VPN erişimi tanımlanır ve gizlilik sözleşmesi imzalanmış olmalıdır.

7.6 Temiz Masa, Temiz Ekran Politikası

Kullanıcılar masaları başında olmadıklarında hassas bilgi içeren basılı dokümanları masa üstünde bırakmamalıdırlar ve bilgisayar ekranlarını açık terk etmemelidirler. Hassas bilgi içeren basılı dokümanlar kullanılmadıklarında masadan kaldırılır ve gerekiyorsa kilit altında tutulur. Kullanıcılar Kurum dışında basılı doküman, bilgisayarlar ve veri saklama cihazlarının fiziksel güvenliği konusunda Kurum içerisine göre daha hassas davranmalı, asla kontrolsüz biçimde açıkta bırakmamalıdır. Kurum dışında bilgisayar ekranından veya basılı dokümanlardan hassas bilgilerin başkalarınca izlenme riskinin daha yüksek olduğu unutulmamalı, halka açık mekânlarda hassas bilgiler görüntülenmemelidir ya da bu gibi durumlarda ekran koruyucu filtreler kullanılmalıdır. Restoranlar ve bina içerisindeki ortak alanlar gibi halka açık mekânlarda iş ile ilgili konular konuşulurken dikkat edilmeli ve başka kişilerin duyabileceği durumlarda konuşma yapılmamalıdır.

7.7 Telefon Görüşmeleri

Kurum çalışanları özellikle Kurum dışında hassas bilgileri içeren telefon görüşmesi yapmamaya gayret etmelidir. Hassas bilgilerin telefon üzerinden konuşulmasının zorunlu olduğu durumlarda, telefon görüşmesi sırasında konuşmanın başka insanlar tarafından duyulması güç yerlerde yapılması, açık ve kalabalık mekânlarda yapılmaması gerekmektedir. Gelen aramalarda arayanın kimliğinden emin olunmaması halinde, kritik bilgilerin dağıtımını güvence altına almak için geri arama yapılarak arayanın kimlik doğrulaması yapılmalıdır.

Bu politikalara uyulmaması durumunda ilgili kişi ve yöneticileri Kurum Bilgi Güvenliği Yöneticisi tarafından uyarılır ve tekrarı halinde de kişi hakkında idari işlem yapılır.

8. DİĞER HUSUSLAR

8.1 Daha Fazla Bilgi İçin

Kullanıcılar gerektiğinde bu politikada belirtilen konular hakkında daha fazla bilgi / destek almak için Bilgi Güvenliği Yöneticisine danışmalıdır.

Bu politikaya aykırı davranışlar İnsan Kaynakları Çalışan El Kitabı'nda tanımlanan disiplin prosedürüne göre değerlendirilir.

9. TANIMLAR VE KISALTMALAR

Ağ Servisi; Bilgisayarlar bilgi ağı üzerinden diğer bilgisayarlara bir takım servisleri sunabilir. Bu mimariye istemci – sunucu mimarisi adı verilir. Bu mimariye göre istemci bilgisayar ağ üzerinden belli protokollere göre sunucu makineye ulaşacak bir istek mesajı gönderir. Ağ servisi ile bu isteği karşılayan sunucu gerekli işlemi yaptıktan sonra istemci bilgisayara ağ üzerinden yanıt döner. Ağ servislerinin güvenlik açıkları bulunabilir, bu nedenle genel güvenlik yaklaşımı, gerekli olmayan ağ servislerinin her zaman kapalı tutulmasıdır.

Betik (Script); Uygulamaları denetlemek için kullanılan bir programlama dilidir. Betikler doğrudan kaynak kodundan çalıştırılır. İlk betik dilleri genelde yığın dilleri veya iş denetim dilleri olarak adlandırılırdı. İlk betik dilleri geleneksel düzenle, derle, bağla, çalıştır işlemlerini kısaltmak için yaratılmıştı. Bu şekilde oluşturulmuş bir dosya doğrudan işletim sistemi komut satırından çağrılarak tek adımda ardışık komutlar çalıştırılabilir. Bu tür dosyalarda güvenlik açısından kullanıcı adı ve parola bilgisinin kayıtlı olmaması gerekir.

BIOS; Bilgisayarın yazılımlarını ve donanımlarını hazır hale getirir. Bu işleme booting denir. BIOS (Basic Input/OutputSystem; Temel Giriş/Çıkış Sistemi), bilgisayarın ilk açılma işlevini yerine getiren yazılımdır. BIOS yazılımı bilgisayarda kuruludur ve bilgisayar açılırken bilgisayar tarafından işletilen ilk koddur (“önyükleme bellenimi- boot firmware”). BIOS’ un temel işlevi işletim sistemini yüklemek ve başlatmak ve bilgisayarı diğer donanım ve yazılımların çalışmasına hazır hale getirmektir. Bilgisayar başlatıldığında BIOS’ un ilk işi klavye, hard disk, CD/DVD sürücüsü, fare gibi sistem aygıtlarını tanımlamak ve kullanıma hazırlamaktır.

Cross Site Scripting – XSS; Bilgisayar güvenlik açığıdır. HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır. Genelde cross site scripting açıkları, saldırganın sistemi deneme-yanılma yaparak bulması ile ortaya çıkmaktadır. Açığın bulunması ile saldırgan, başka bir alan adından, açığın bulunduğu alan adı ve sayfanın bilgilerini, oturum ayrıntılarını ve diğer nesne değerlerini çalabilir.

Çipli Kart; Kredi kartı büyüklüğünde olan genellikle plastik bir yapının içine gömülmüş olan elektronik sistemlerdir. İçinde işlemci barındıran kartlar akıllı kart olarak adlandırılır.

Elektronik İmza; Sayısal imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir. Elektronik ortamlarda imza yerine kullanılabilen yasal kimlik doğrulama sistemidir.

P2P Ağ; Peer-to-peer ya da P2P olarak tanımlanır. Peer eş, denk demektir. İki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür. Eşler, sunucuları veya sabit bilgisayarlar tarafından merkezi koordinasyon ihtiyacı olmadan, işlemci gücü, disk

depolama veya ağ bant genişliği gibi kendi kaynaklarının bir kısmını, doğrudan diğer ağ katılımcıları için kullanılabilir yapabilir. Sadece sunucuların tedarikçi ve istemcilerin tüketici olduğu geleneksel istemci-sunucu modelinin aksine eşler, hem tedarikçi hem de tüketicidir.

Güvenli Silme; Standart silme işleminde sadece o verinin adres bilgisi silinir ancak verinin kendisi silinmez bu neden ile silinmiş olarak gözüken veriye farklı araçlar kullanılarak yeniden erişilebilir. Normal silinme işleminden sonra veriler bazı programlar aracılığı ile tekrar görülür hale getirilebilir. Güvenli Silme sırasında veri geri getirilemeyecek şekilde tahrip edilerek silinir. Güvenli silme için kullanılabilecek örnek uygulamalar; Active@KillDisk - Hard Drive Eraser, Eraser, Shreditfor Windows, Disk Wipe vb.

Güvenlik Alanları (Security Zones); Internet, Yerel intranet, Güvenilen Siteler ve Yasak Siteler. Bir web sitesine atanan bölge, bu site için kullanılan güvenlik ayarlarını gösterir. İnternet sitelerinin dinamik içerik sunma ihtiyacı ve tarayıcıların daha fonksiyonel olmaları amacıyla Applet, ActiveX, VBScript, Java Script vb. teknolojiler geliştirilmiştir. Ancak bu fonksiyonellik zaman içinde ortaya çıkan zayıflıklar kullanılarak kötüye kullanılmış / kullanılmaktadır.

İstenmeyen (Spam) E-posta; İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi Spam olarak adlandırılır. Spam çoğunlukla ticari reklam niteliğinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacına yöneliktir. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajın alıcıları veya taşıyıcı, servis sağlayıcı Kurumlar tarafından karşılanmak zorunda kalınır.

Jenerik / Ortak Hesap; Sistem yazılımları ve bazı sunucu ve uygulama yazılımları varsayılan kurulumları ile belli jenerik kullanıcıları erişim kontrolü için yaratır. Bu kullanıcı hesaplarına jenerik hesaplar denir. Genellikle yönetsel hakları olan bu tür kullanıcı kodları bazı durumlarda değiştirilebilir ve yönetsel haklar farklı kullanıcılara gerektiği ölçüde dağıtılabilir. Ancak bazı yazılımlar için bu mümkün değildir. Ortak hesap kullanımı aynı kullanıcı hesabının farklı kullanıcılar tarafından kullanılmasıdır. Bu durum hesap verebilirliğe zarar verir.

Koruma Duvarı (Firewall); Ağ servisleri belli protokoller üzerinden, bu protokollerden ikisi olan TCP/UDP servisleri de belli portları kullanarak hizmet verir. Genel güvenlik prensibi olarak sadece gerekli sunucuların ve gerekli servislerin (protokol ve port tanımlarıyla) sunulması gerekir. Sadece gerekli servislerin sunulması, ağların güvenlik ihtiyaçlarına göre bölümlenmesi, sadece gerekli sunucuların (teknik olarak IP adreslerinin) hizmetlerine sadece istenen kullanıcılar tarafından ulaşımın sağlanması için bir kontrol cihazı (veya yazılımı) olarak koruma duvarları kullanılır. Koruma duvarları üzerlerinde diğer koruma önlemlerini de barındırabilmektedir (hizmet kesinti saldırılarına karşı koruma, saldırı tespit sistemlerini

yanıltmaya yönelik yöntemleri bertaraf etme gibi). Koruma duvarları derinlemesine güvenlik yaklaşımına göre sadece bir katmanı oluşturur ve asla tek başına yeterli güvenliği sağlamaz.

Kriptoloji; Bilgi alışverişini emniyetli olarak yapmasını sağlayan veya saklanan bilginin emniyetini korumak için uygulanan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür. Kriptolamanın içinde genel olarak algoritmalar ve anahtar bulunur. Kriptolama yöntemleri şu servislerden bir veya birden fazlasını sağlamak amacıyla kullanılır: Gizlilik, Bütünlük, Kimlik Doğrulama, İnkâr Edilemezlik.

Parola (Şifre); Kimlik doğrulamada kullanıcı adına ek olarak kullanılan ve sadece kullanıcısı tarafından bilinmesi gereken karakterler bütünüdür.

Phishing (Yemleme); Phishing (Yemleme) saldırısında amaç (kimlik bilgileri, kart numarası gibi) kişisel bilgilerin ele geçirilebilmesi olup, temelde bir sosyal mühendislik yöntemi olan sahte e-posta ve Web sayfalarının kullanılmasıyla gerçekleştirilir. Phishing'de dolandırıcılar, tüketicilere tanınmış bir firmadan geliyormuş izlenimi verilmiş bilgi güncelleme talebi vb. içeren e-postalar göndermektedir. Bu e-postalarda genellikle cevap için e-postanın içindeki linkin (Web sayfası için kısa yol) tıklanarak gerekli siteye geçilebileceği belirtilmektedir. Ancak, verilen talimat uygulandığında gidilen site dolandırıcılar tarafında hazırlanmış ve gerçeğini taklit eden sahte bir Web sayfası olmaktadır. Bu sahte sitede elde edilen bilgiler mahiyetine göre daha sonra çeşitli dolandırıcılık faaliyetlerinde kullanılabilmektedir. Phishing yönteminde bankaların kimliğinin kullanmasının yanında mağazalar veya e-ticaret Kurumlarının ve İnternet servis sağlayıcıların kimliklerinin de kullanıldığı görülmektedir. Pharming adı verilen ve aynı amacı taşıyan bir diğer saldırı türü de DNS (İsim Sunucusu) sunucularının veya isim sorgularının yanıtlarının manipüle edilmesiyle kullanıcıların saldırgan tarafından düzenlenen bir siteye (kullanıcının bilgisi olmadan) yönlendirilerek kandırılması ve kişisel bilgilerinin çalınması şeklinde gerçekleştirilir.

Sanallaştırma (Virtualization) Yazılımları; Sanallaştırma yazılımları bir işletim sistemi yazılımını veya bir uygulamayı üzerinde çalıştığı donanım veya işletim sisteminden soyutlar. İşletim sisteminin soyutlanmasındaki temel amaç aynı anda tek donanımın kaynakları kullanılarak birden fazla işletim sisteminin ve doğal olarak hizmetlerinin kullanılmasıdır. Ancak bir yan etki olarak konuk (guest) işletim sisteminde meydana gelen değişiklikler sadece onun tarafından kullanılan bir ev sahibi (host) işletim sistemi dosyasında sınırlandırıldığından, zarara yol açabilecek testlerin veya güvenlik riski taşıyan aktivitelerin konuk sistemde yapılması ile ev sahibi sistemin korunması da sağlanmış olur. Teknik olarak işletim sistemi sanallaştırma yöntemi ile aynı yöntem kullanılmamakla birlikte sanallaştırma desteği sağlayan uygulamalar da o uygulama ile yapılan işlemlerin geri kalan sistem dosyalarına etki etmesini engeller ve uygulama kapatıldığında kullanım sırasında gerçekleşen tüm değişiklikler yok olur. Bu alandaki en çok kullanılan uygulamalar web tarayıcılarına sanallaştırma desteği sağlayan uygulamalardır. Böylece o bilgisayar üzerinde yapılan işlemlerin başkaları tarafından öğrenilmesine yol açacak kalıntıların bulunmaması sağlanmış olur.

Sosyal Mühendislik; Bilgi güvenliği terminolojisine sosyal mühendislik adıyla giren saldırı veya gerçek saldırı öncesi aktiviteler insani duyguları (korku, acili yet hissi, minnet, itaat, güven hissi, yardımcı olma güdüsü, vb. gibi) kullanarak bilgiye erişim yetkisi olan kişilerin yönlendirilmesi ve kullanılmasını içerir. Saldırgan farklı kimliklere bürünerek kurguladığı senaryo adımları ile kurbanını beklenen tepkileri vermeye yönlendirir. En temel sosyal mühendislik araçları telefon ve e-postadır.

Virüs, Trojan, Worm, Spyware, Adware, Anti-Virüs ve Virüs İmzaları; Genel olarak kötü niyetli yazılım (malware) olarak adlandırılan virüs, trojan, worm, spyware ve adware yazılımlarının ortak noktası bilgisayar kullanıcılarının (veya daha genel tanımıyla sistem sahiplerinin) bilgi ve onayı olmadan sistemlere girme, bilgi çalma veya zarar verme amacına yönelik olarak yaratılmış olmalarıdır. Virüsler kendilerini kopyalamak için başka bir çalıştırılabilir dosyaya kendini eklemeye ihtiyaç duyarken worm kendi başına ağ üzerinden diğer bilgisayarlara bulaşabilir. Trojan, genel olarak farklı ve kullanıcının isteyerek yüklediği bir uygulamaya eklenip, istenen uygulamanın çalıştırılması ile bulaşır. Spyware bulaştığı bilgisayarda yapılan aktiviteleri kaydedip, başka bir sisteme kullanıcının bilgi ve onayı olmadan gönderir. Adware bulaştığı bilgisayara istenmeyen pazarlama materyallerini indirir ve gösterir. Diğer kötü niyetli yazılımlar arasında rootkit'ler, backdoor'lar, bot'lar, keylogger'lar ve dialer'lar sayılabilir. Anti-virüs yazılımları bu tür yazılımları erişim sırasında veya taramalar sırasında saptar ve günümüzde vazgeçilmez bir güvenlik katmanı oluşturur. Anti-virüs yazılımları kötü niyetli yazılımları tespit etmek için birer virüs imza veri tabanı kullanır. Sürekli olarak yeni kötü niyetli yazılımlar ortaya çıktığından bu imzaların güncelliği son derece önemlidir.

	Kabul Edilebilir Kullanım Politikası	Doküman No	PR.06
		İlk Yayın Tarihi	20.02.2018
		Revizyon No	0
		Revizyon Tarihi	
		Sayfa No	

Hazırlayan		Onaylayan