YÖNETİM KURALLARI

Veri Sınıflandırma Kuralları

1.1 Veri Sınıflandırması Yapın

Kural: Tüm değerli, hassas ya da önemli iş bilgileri ilgili bilgi sahibi ya da vekili tarafından bir sınıflandırmaya tutulmalıdır.

1-2 Sınflara Göre Kullanma Süreçleri Çıkarın

Kural: Şirket her sınıf bilginin verilmesine yönelik süreçler oluşturmalıdır.

1-3 Tüm Ögeleri İşaretleyin

Kural: Gizli, özel ya da dahili bilgi iöeren hem basılı malzemeleri, hem de bilgisayar saklama ortamlarını ilgili veri sınıflandırmasını gösterecek açık bir şekilde işaretleyin.

Bilginin Verilmesi

2-1 Çalışan Kimliğinin Tespiti Süreci

Kural: Gizli ya da hassas bilgilerin verilmesini ya da herhangi bir bilgisayar donanımının ya da yazılımının kullanılmasını içeren bir işin yapılmasından önce kişinin kimliğinin, iş durumunun ve yetkilerinin kontrol edilebilmesi için çalışanların kullanabileceği kapsamlı süreçler şirket tarafından oluşturulmalıdır.

2-2 Bilginin üçüncü şahıslara verilmesi

Kural: Bir dizi kendini kanıtlamış bilgi verme süreci yürürlüğe konmalı ve tüm çalışanlar bu süreçleri izlemeleri konusunda eğitilmelidirler.

2-3 Gizli bilgilerin dağıtımı

Kural: Yetkisiz kişilerin eline geçtiğinde büyük zararlara neden olabilecek şirket bilgileri olan gizli bilgiler ancak almaya yetkili bir güvenilir kişiye verilebilir.

2-4 Özel bilgilerin dağıtımı

Kural:Açığa çıktıkları taktirde çalışanlara ya da şirkete zarar vermek üzere kullanılabilecek,çalışan ya da çalışanlarla ilgili kişisel bilgileri ifade eden özel bilgiler, yalnızca onu almaya yetkili bir güvenilir kişiye teslim edilebilir.

2-5 Dahili bilgilerin dağıtımı

Kural: Dahili bilgiler, yalnızca şirket içinde dağıtılabilecek ya da gizlilik anlaşması imzalamış güvenilir kişilere verilebilecek bilgilerdir.Dahili bilginin dağıtımına yönelik yönergeler hazırlamanız gerekir.

2-6 Hassas bilgilerin telefon üzerinden görüşülmesi

Kural: Genel sınıfında tanımlanmış herhangi bir bilgiyi telefon üzerinde görüşmeden önce, bilgiyi verecek kişinin, karşı tarafın sesini daha önceden şahsen duymuş olması ya da şirket telefon sisteminin aramanın istek sahibine ait dahili bir numaradan yapıldığını tespit etmiş olması gerekmektedir.

2-7 Girişte ya da danışmada görevli personel süreçleri

Kural: Giriş görevlileri, şirkette çalışıp çalışmadığını bilmedikleri herhangi birine herhangi bir paketi verirlerken resimli kimlik kontrolü yapmalıdırlar. Kişinin adının, ehliyet numarasının, doğum tarihinin,alınan paketin ve alımın gerçekleştiği gün ve saatin işlendiği bir kayıt defteri tutulmalıdır.

2-8 Üçüncü şahıslara yazılım aktarımı

Kural: Herhangi bir yazılım, program ya da bilgisayar açıklamalarının verilmesinden ya da aktarılmasından önce istek sahibinin doğru kişi olduğu belirlenmeli ve bu aktarımın, söz konusu bilginin veri sınıfıyla tutarlı olup olmadığı kesinleştirilmelidir. Şirket bünyesinde kaynak kodu biçiminde yapılmış yazılımlar çoğunlukla şirket mülkü sayılır ve gizli olarak sınıflandırılırlar.

2-9 Satış ve pazarlamanın müşteri önerilerinin incelemesi

Kural: Satış ve pazarlama personeli, dahili geri arama numaralarını, ürün planlarını, ürün grubu iletişim sorumlularını ya da diğer hassas bilgileri olası bir müşteriye vermeden önce verilen önerileri incelemelidir.

2-10 Dosya ve verilerin aktarımı

Kural: İstek sahibi, kimliği belirlenmiş ve veriyi ilgili taşınabilir ortamda alması gerektiği anlaşılmış bir güvenilir kişi olmadığı sürece dosyalar ya da diğer elektronik veriler hiçbir taşınabilir ortama aktarılmamalıdır.

Telefon İdaresi

3-1 Bilgisayar bağlantısı ya da faks numaralarında aramaların yönlendirilmesi

Kural: Aramaları dış hat telefon numaralarına yönlendiren arama yönlendirme hizmetleri şirket içindeki herhangi bir modem ya da faks numarasına sağlanmamalıdır.

3-2 Arayan kimliği

Kural: Şirket telefon sistemi, tim dahili telefonlara arayan hat tanımlama(arayan kimliği) hizmetini sağlamalıdır ve eğer mümkünse, dışarıdan gelen aramalarda farklı bir çalma sesi kullanılmalıdır.

3-3 Nezaket telefonları

Kural: Ziyaretçilerin şirket çalışanı gibi davranmalarını önlemek için her nezaket telefonunun nereden edildiği(örneğin, "Danışma") arananın telefon göstergesinde açıkça görülebilmelidir.

3-4 Telefon sistemleri ile gelen üretici parolaları

Kural: Sesli mesaj yöneticisi, şçrket çalışanları tarafından kullanılmadan önce telefon sistemiyle birlikte gelen parolalar değiştirilmelidir.

3-5 Bölüm sesli mesaj kutuları

Kural: Dışarıyla bağlantısı olabilecek her bölüme için bir sesli mesaj oluşturun.

3-6 Telefon sistem satıcısının onaylanması

Kural: Satıcı firmadan gelen hizmet teknisyenlerinden hiçbirine, satıcı firma bilgileri ve gelenlerin yetkileri onaylanmadan, şirket telefon sistemine erişim hakkı tanınmamalıdır.

3-7 Telefon sisteminin ayarlanması

Kural: Sesli mesaj yöneticisi, telefon sisteminde ilgili güvenlik ayarlamalarını yaparak güvenlik gerekliliklerinin yerine getirilmesini sağlar.

3-8 Arama izleme özelliği

Kural: İletişim hizmetleri veren firmanın sınırlamalarına göre, çalışanların, arayanın saldırgan olduğundan kuşkulandıkları durumda kıstırıp kovalayan bu işlevi çalıştırabilmeleri sağlanabilecek şekilde, arama izleme özelliği devreye sokulmalıdır.

3-9 Otamatik telefon sistemleri

Kural: Eğer şirket otamatik bir yanıt verme sistemi kullanıyorsa, sistem bir çalışana ya da bölüme aramayı aktarırken dahili numarayı söylemeyecek şekilde programlanmalıdır.

3-10 Birbiri ardına başarısız girme denemesinden sonra sesli mesaj kutularının kapatılması

Kural: Peşpeşe belirli bir sayıda başarısız girme denemesi olduğunda sesli mesaj hesaplarını kilitleyecek şekilde şirket telefon sisteminin programlanması.

3-11 Sınırlandırılmış dahili telefonlar

Kural: Çoğu zaman dışarıdan gelen aramaları kabul etmeyen bölüm ve iş gruplarına ait tüm dahili telefonlar(yardım masası, bilgisayar odası, çalışan teknik destek vb.) yalnızca diğer dahili telefonların ulaşabileceği şekilde programlanmalıdır. Diğer bir seçenek ise parola korumalı olması ve dışarıdan arayan çalışanların doğru parolayı girmeleridir.

Çeşitli

4-1 Personel kartı tasarımı

Kural: Personel kartları uzaktan tanınabilecek büyük bir fotoğraf içerecek şekilde tasarlanmalıdır.

4-2 Konum ya da sorumluluk değiştirirken erişim haklarının gözden geçirilmesi

Kural: Ne zaman bir şirket çalışanının konumu değişir ya da sorumlulukları azalır veya çoğalırsa, çalışanın yöneticisi, gerekli güvenlik profilinin oluşturulması için değişimden Bİ'yi haberdar eder.

4-3 Şirket çalışanı olmayanlar için özel kimlik

Kural: Şirketiniz, düzenli olarak içeride işi olan ama şirket çalışanı olmayan kişiler ve güvenilir kuryeler için özel fotoğraflı şirket kartı çıkarmalıdır.

4-4 Taşeronların bilgisayar hesaplarını kapatmak

Kural: Kendisine bir bilgisayar hesabı açılmış bir taşeron işini bitirdikten ya da sözleşmesi sona erdikten sonra, sorumlu yönetici derhal bilgi teknolojileri bölümünü haberdar ederek uzaktan erişim için telefon bağlantısı ya da internet erişimleri ve veri tabanı erişim hesapları da dahil olmak üzere taşeronun bilgisayar hesaplarını kapattıracaktır.

4-5 Olay bildirme merkezleri

Kural: Bir olay bildirme merkezi kurulmalı ya da daha küçük şirketlerde, olası güvenlik olaylarına yönelik uyarıları alıp duyuracak bir olay bildirme sorumlusu ve yardımcısı seçilmelidir.

4-6 Olay bildirme hattı

Kural: Olay bildirme merkezine hatırlaması kolay bir dahili numarası olan bir hat açılabilir.

4-7 Hassas alanlar kapatılmalıdır

Kural: Bir güvenlik görevlisi hassas ya da güvenli alanları gözetim altında tutacak ve bu alanlara giriş iki kademeli tanıtım gerektirecektir.

4-8 Ağ ve telefon kutuları

Kural: Ağ kabloları, telefon kabloları ya da ağ erişim noktaları bulunan kutular, dolaplar ya da odalar her zaman kapalı tutulmalıdır.

4-9 Şirket içi posta kutuları

Kural: Şirket içi posta kutuları herkese açık yerlere konmamalıdır.

4-10 Şirket bülten panosu

Kural: Şirket çalışanları yararına olan bülten panoları dışarıdan gelenlerin erişebileceği yerlere asılmamalıdır.

4-11 Bilgisayar merkezi girişi

Kural: Bilgisayar odası ya da veri merkezi her zaman kilitli tutulmalı ve çalışanların içeri girerken kimlik göstermeleri zorunlu olmalıdır.

4-12 Hizmet sağlayıcılardaki müşteri hesapları

Kural: Şirkete önemli hizmetler sağlayan satıcılara sipariş veren şirket çalışanları yetkisiz kişilerin şirket adına sipariş vermelerini önlemek için parolalı bir hesp açmalıdırlar.

4-13 Bölüm bağlantı sorumlusu

Kural: Şirketiniz, her bölümden ya da iş grubundan bir kişiye bağlantı kurulacak kişi sorumluluğunu verdiği biir program tesis edebilir. Böylece herhangi bir çalışan, o bölümden olduğunu iddia eden bilinmeyen kişilerin gerçekliğini kolaylıkla doğrulayabilir. Örneğin, yardım masası destek isteyen bir çalışanın kimliğini onaylatmak için ilgili bölümün bağlantı kişisini arayabilir.

4-14 Müşteri parolaları

Kural: Müşteri hizmet temsilcilerinin müşteri hesap parolalarını alma yetkileri olmayacaktır.

4-15 Açıklık testleri

Kural: Güvenlik bilinçlendirme ve çalışan intibak eğitimleri sırasında güvenlik açıklarını test etmek için şirketin toplum mühendisliği taktikleri kullanacağını bildirilmesi gerekmektedir.

4-16 Şirket Gizli bilgilerinin gösterilmesi

Kural: Halka açıklanması düşünülmeyen şirket bilgileri herkesin görebileceği yerlere asılmamalıdır.

4-17 Güvenlik bilinçlendirme eğitimi

Kural: Şirketin tüm çalışanları, çalışan intibak eğitimleri sırasında bir güvenlik bilinçlendirme eğitimini de tamamlamalıdırlar. Dahası, her çalışan, oniki ayı geçmemek koşuluyla güvenlik eğitimlerini yürüten bölümün belirlediği düzenli aralıklarla güvenlik bilincini tazeleme eğitimleri almalıdır.

4-18 Bilgisayar erişimi için güvenlik eğitimi dersleri

Kural: Çalışanlar herhangi bir şirkette, bilgisayar sistemine erişim hakkı elde etmeden önce bilgi güvenliği derslerini başarıyla tamamlamış olmalıdırlar.

4-19 Çalışan kartı renkli baskılı olmalıdır

Kural: Kimlik kartları, kart sahibinin, çalışan, taşeron, geçici satıcı, danışman, ziyaretçi ya da stajyer olduğunu gösterecek şekilde renklendirilmiş olmalıdır.

BİLGİ İŞLEM TEKNOLOJİLERİ KURALLARI

Genel

5-1 Bİ bölümü çalışan iletişim bilgileri

Kural: Bİ bölümü çalışanlarının telefon numaraları ve e-posta adresleri, bilme gereği olmayan herhangi birine verilmemelidir.

5-2 Teknik destek talepleri

Kural: Tüm teknik destek talepleri bu tarz talepleri değerlendiren gruba yönlendirilmelidir.

Yardım Masası

6-1 Uzaktan erişim süreçleri

Kural: Yardım masası çalışanları, harici ağ erişim noktaları ya da bağlantı numaraları da aralarında olmak üzere uzaktan erişimle ilgili bilgileri ve ayrıntıları açıklamamalıdırlar.Ancak, istek sahibi aşağıdaki koşullardan birine uyuyorsa durum değişebilir:

- Dahili bilgi alabileceğine dair yetkili olduğunun onaylanmış olması

- Harici bir kullanıcı olarak şirket ağına bağlanmaya yetkili olduğunun onaylanmış olması. Kişi şahsen tanımadığı sürece bu bölümde anlatılan Onay ve Yetkilendirme Süreçlerine uygun olarak istek sahibinin kimlik tespiti kuşku bırakmayacak şekilde yapılmalıdır.

Kural: Bir kullanıcı hesabına ait parola yalnızca hesap sahibinin isteği doğrulyuda yenilenebilir.

6-3 Yetkilerin değişimi

Kural: Bir kullanıcının yetkilerini erişim hakalrını artırmaya yönelik tüm talepler hesap sahibinin yöneticisi tarafından yazılı olarak onaylanmış olmalıdır. Ayrıca bu tarz taleplerin Onay ve Yetkilendirme Süreçlerine uygun olarak ge**ç**erlilikleri onaylanmalıdır.

6-4 Yeni hesap yetkisi

Kural: Çalışanlar, taşeronlar ya da diğer yetkili kişilerin kullanımı için açılacak yeni hesap talepleri çalışanın yöneticisi tarafından imzalanmış yazılı bir belgeyle ya da dijital olarak imzalanmış elektronik postayla yapılmalıdır. Bu istekler şirekt içi posta aracılığıyla teyit edilmelidir.

6-5 Yeni parolaların teslimi

Kural: Yeni parolalar şirket gizli bilgileri olarak ele alınmalı ve şahsen, taahütlü posta gibi imzalı teslimatla ya da güvenilir kargo şirketleri gibi güvenli yöntemler kullanarak teslim edilmelidirler.

6-6 Bir hesabın kapatılması

Kural: Bir kullanıcı hesabını kapatmadan önce talebin yetkili birinden geldiğinin doğrulanması gerekmektedir.

6-7 Ağ bağlantı noktalarının ve araçlarının devre dışı bırakılması

Kural: Hiçbir çalışan kim olduklarını bilmedikleri bir teknik destek çalışanı için herhangi bir ağ aracını ya da bağlantı noktasını kapatmamalıdır.

6-8 Telsiz erişimi süreçlerinin açıklanması

Kural: Hiçbir çalışan telsiz ağına bağlanmaya yetkili olmayan kimselere telsiz ağı üzerinden şirket ağına bağlanma süreçlerini açıklamamalıdır.

6-9 Kullanıcı gizliliği

Kural: Bilgisayarla ilgili sorun olduğunu bildiren çalışanların adları bilgi işlem bölümü dışından kimseye açıklanmamaladır.

6-10 Komut girmek ya da program çalıştırmak

Kural: Bİ bölümünde ayrıcalıklı hesapları olan çalışanlar, şahsen tanımadıkları birinin isteği üzerine herhangi komut ya da program çalıştırmamalıdırlar.

Bilgisayar İdaresi

7-1 Genel erişim haklarının değiştirilmesi

Kural: Bir elektronik iş profiliyle ilgili genel erişim haklarını değiştirme talebi şirket ağında erişim haklarını yöneten gurup tarafından onaylanmalıdır.

7-2 Uzaktan erişim talepleri

Kural: Uzaktan bilgisayar erişimi yalnızca şirket dışı noktalardan bilgisayar sistemlerine girme gerekliliği olduğunu gösteren çalışanlara verilecektir.

7-3 Ayrıcalıklı hesap parolalarının ilk duruma getirilmesi

Kural: Yetkili bir hesaba ait parolanın ilk durumuna getirilmesi talebi, hesabın bulunduğu bilgisayardan sorumlu sistem yöneticisi tarafından onaylanmalıdır. Yeni parola, şirket içi postayla gönderilmeli ya da şahsen iletilmelidir.

7-4 Dışarıdan gelen destek personelinin uzaktan erişimi

Kural: Hiçbir dışarıdan destek personeline (yazılım ya da donanım satan firmadan gelen personel gibi) ilgili hizmetleri vermeye yetkili olup olmadıkları kontrol edilmeden ve kimlik tespiti yapılmadan şirket bilgisayar sistemlerine ya da ilgili araçlara uzaktan erişme hakkı ya da bilgisi verilmemelidir. Eğer destek hizmeti vermek üzere satıcı firma yetkili erişim talep ediyorsa, verilen hizmet sona erdiğinde satıcı firmanın kullandığı hesabın parolası zaman değiştirilmeden değiştirilmelidir.

7-5 Şirket sistemlerine uzaktan erişim için güçlü tanımlama

Kural: Şirket ağına uzaktan erişim için kullanılan tüm bağlantı noktaları değişken parolalar ya da biyometrikler gibi güçlü tanımlama araçlarıyla korunmalıdırlar.

7-6 İşletim sistemi ayarları

Kural: Sistem yöneticileri mümkün olan her noktada işletim sistemlerinin tüm geçerli güvenlik kural ve süreçleriyle tutarlı bir şekilde ayarlanmış olduğundan emin olmalıdırlar.

7-7 Zorunlu süre aşımı

Kural: Tüm bilgisayar hesapları bir yıl içerisinde kapanmaya ayarlanmalıdır.

7-8 Genel e-posta adresleri

Kural: Bİ bölümü dışarıyla sürekli iletişimi olan her bölüm için genel bir e-posta adresi oluşturacaktır.

7-9 Alan tescilleri için iletişim bilgileri

Kural: İnternet adres alanları ya da alan adları almak için kayıt olurken sağlanan iletişim bilgileri idari, teknik ya da diğer çalışanların bireysel olarak adlarını vermemelidir. Onun yerine oraya genel bir e-posta adersi ve ana şirket numarası girilmelidir.

7-10 Güvenlik ve işletim sistemi güncellemelerinin yüklenmesi

Kural: İşletim sistemi ve uygulama yazılımlarına yönelik tüm güvenlik yamaları, çıktıkları zaman en kısa sürede yüklenmelidirler. Eğer bu kural görev-kritik üretim sistemlerinin işleyişiyle çatışıyorsa bu tarz güncellemeler uygun oldukları zaman yapılmalıdırlar.

7-11 İnternet sayfalarındaki iletişim bilgileri

Kural: Şirketin harici internet sayfası, şirket yapısı ile ilgili hiçbir bilgi vermemeli ya da çalışanları isim isim göstermemelidir.

7-12 Ayrıcalıklı hesapların oluşturulması

Kural: Sistem yöneticisi tarafından onaylanmadığı sürece hiçbir ayrıcalıklı hesap açılmamalı ya da herhangi bir hesabın sistem yetkileri arttırılmamalıdır.

7-13 Misafir hesapları

Kural: Herhangi bir bilgisayar sisteminde ya da ilgili ağ araçlarında bulunan misafir hespları, yönetimin onayladığı adsız erişimli FTP (dosya aktarım protokolu) sunucusu hariç, devre dışı bırakılmalı ya da kaldırılmalıdır.

7-14 Şirket dışında tutulan yedeklerin şifrelenmesi

Kural: Şirket dışında tutulan herhangi bir veri yetkisiz erişimi engellemek için şifrelenmelidir.

7-15 Ağ bağlantılarına ziyaretçi erişimi

Kural: Herkese açık tüm ethernet erişim noktaları dahili ağa yetkisiz ulaşımı engellemek için parçalı ağda(segmented network) bulundurulmalıdır.

7-16 Bağlantı modemleri

Kural: Aramalara açık bağlantı modemleri dördüncü çalıştan önce açılmayacak şekilde ayarlanmalıdırlar.

7-17 Virüs koruma modemleri

Kural: Her bilgisayar sistemine virüs koruma yazılımlarının son sürümleri yüklenmeli ve çalıştırılmalıdır.

7-18 Gelen e-posta ekleri (yüksek güvenlik gereksinimi)

Kural: Yüksek güvenlik ihtiyaçları olan bir kuruluşta şirket güvenlik duvarı tüm e-posta eklerini eleyecek şekilde ayarlanmalıdır.

7-19 Yazılım onayı

Kural: Tüm yeni yazılımlar, yazılım çözümleri ya da güncellemeleri, ister fiziksel ortamda olsun ister internet üzerinden elde edilmiş olsun yüklenmeden önce güvenilirlikleri doğrulanmalıdır. Bu kural, özellikle sistem yetkileri gerektiren yazılımlar yüklenirken bilgi işlem bölümünü ilgilendirir.

7-20 Varsayılan parolalar

Kural: Varsayılan bir parolaya sahip olan tüm işletim sistemi yazılımlarının ve donanımlarının şirket parola kuralları doğrultusunda parolaları değiştirilmelidir.

7-21 Başarısız erişim denemeleri sonucu kilitlenme

Kural: Özellikle düşük ve orta düzey güvenlik gereksinimleri olan bir kurumda aynı hesaba birbiri ardına belirli bir sayıda girme girişimi olursa hesap bir süreliğine kilitlenmelidir.

7-22 Başarısız erişim girişimleri sonucu hesabın kapatılması

Kural: yüksek güvenlik gereksinimleri olan bir kurumda aynı hesaba birbiri ardına belirli sayıda başarısız girme girişimi olursa hesap, desteği veren grup tarafından düzeltilene kadar kesilmelidir.

7-23 Ayrıcalıklı hesapların parolalarının düzenli olarak değiştirilmesi

Kural: Tüm ayrıcalıklı hesap sahiplerinin en çok otuz günde bir parolalarını değiştirmeleri zorunluluğu getirilecektir.

7-24 Kullanıcı parolalarının düzenli olarak değişimi

Kural: Tüm hesap sahipleri en çok altmış günde bir parolalarını değiştirmelidirler.

7-25 Yeni hesap parolası oluşturmak

Kural: Yeni bigisayar hesapları, süresi dolmuş bir parolayla oluşturulmalı, böylece hesap sahibine ilk kullanım için yeni bir parola belirleme zorunluluğu getirilmelidir.

7-26 Açılış parolaları

Kural: Tüm bilgisayar sistemleri açılışta parola isteyecek şekilde ayarlanmalıdır.

7-27 Ayrıcalıklı hesaplar için parola zorunlulukları

Kural: Tüm ayrıcalıklı hesapların güçlü parolaları olmalıdır. Parola aşağıdaki özelliklere uymalıdır.

- Herhangi bir dildeki sözlüklerde bulunmamalıdır.
- Büyük ve küçük harflerden oluşmalı ve en az bir harf, bir simge ve bir sayı içermelidir.
- En az 12 karakter uzunluğunda olmalıdır.
- Şirkete ya da bireye herhangi bir nedenle verilmemelidir.

7-28 Telsiz erişim noktaları

Kural: Bir telsiz ağına erişimi olan tüm kullanıcılar şirket ağlarını korumak için VPN (virtual private network – sanal özel ağ) teknolojisi kullanmalıdırlar.

7-29 Virüs şablon dosyalarının güncellenmesi

Kural: Her bilgisayar sistemi virüs koruma yazılımları için virüs/Truva Atı şablon dosyalarını otomatik olarak güncellemek üzere programlanmalıdır.

Bilgisayar İşlemleri

8-1 Komut girmek ve program çalıştırmak

Kural: Bilgisayar işlemlerinden sorumlu personel, tanımadıkları birinden gelen talep üzerine komut girmemeli ve program çalıştırmamalıdır. Onaylanmamış bir kişinin istekte bulunmak için geçerli bir nedeni varmış gibi görünen durumlar ortaya çıkarsa öncelikle yöneticinin onayı alınmadan bu istek yerine getirilmemelidir.

8-2 Ayrıcalıklı hesabı olan çalışanlar

Kural: Ayrıcalıklı hesapları olan çalışanlar onaylanmamış kişilere destek ve bilgi vermemelidirler. Özellikle de bilgisayar yardımı (bir uygulamanın kullanımı konusunda eğitim gibi), herhangi bir şirket veritabanına erişim, yazılım indirme ya da uzaktan erişim yeteneğine sahip çalışanların adlarının açıklanması gibi durumlar söz konusu olduğunda bu geçerlidir.

8-3 Dahili sistem bilgileri

Kural: Bilgisayar işlemleri personeli, istek sahibine kimlik tesbiti yapmadan, şirkat bilgisayar sistemleri ya da ilgili donanımlarlailgili değerli bilgileri kesinlikle açıklamamalıdır.

8-4 Parolaların açıklanması

Kural: Bilgisayar işlemleri personeli hiçbir zaman kendilerine ait olan ya da onlara emanet edilmiş parolaları bir bilgi işlem yöneticisinin onayı olmadan açıklamamalıdır.

8-5 Elektronik ortam

Kural: Dışarı verilmek üzere sınıflandırılmamış bigiler içeren tüm elektronik ortamlar fiziksel olarak güvenli bir yerde kilitlenmelidirler.

8-6 Yedekleme ortamları

Kural: Bilgisayar işlemleri personeli yedekleme ortamlarını şirket kasasında ya da başka bir güvenli yerde saklamalıdır.

TÜM ÇALIŞANLAR İÇİN GEÇERLİ KURALLAR

Genel

9-1 Şüpheli aramaların kontrol edilmesi

Kural: Herhangi bir şüpheli bilgi ya da bilgisayar işlemi talebinde bulunulması durumu da dahil olmak üzere bir güvenlik ihlaline maruz kaldıklarından kuşkulanan çalışanlar hemen olayı şirketin olay bildirme grubuna bildirmelidirler.

9-2 Şüpheli aramaları belgelemek

Kural: Bir toplum mühendisliği saldırısı gibi görünen şüpheli bir aramada, çalışan, uygun olduğu ölçüde, saldırganın ne başarmaya çalıştığını anlatacak kadar ayrıntı öğrenmeye çalışmalı ve belgeleme amacıyla bu ayrıntılarla ilgili notlar almalıdır.

9-3 Bağlantı numaralarının verilmesi

Kural: Şirket çalışanları şirket modem telefon numaralarını açıklamamalı ve bu tarz istekleri herzaman yardım masasına yada teknik destek personeline yönlendirmelidir.

9-4 Şirket kimlik kartları

Kural: İçinde bulundukları ofis bölgesi haricinde, üst ve orta yönetim de dahil, tüm şirket çalışanları herzaman personel kartlarını takmalıdırlar.

9-5 Kimlik kartı ihlallerinin sorgulanması

Kural: Tüm çalışanlar şirket kimlik kartı yada ziyaretçi kartı takmayan tanımadıkları kişileri hemen sorgulamalıdırlar.

9-6 Peşpeşe geçmek

Kural: Binaya giren çalışanlar, içeri girmek için manyetik kartı gibi güvenli araçlar kullandıklarında tanımadıkları hiç kimsenin hemen arkalarından gelmesine izin vermemelidirler.

9-7 Hassas belgelerin kağıt öğütücüden geçirilmesi

Kural: Atılacak hassas belgeler çapraz öğütücüden geçirilmelidir. Herhangi bir zamanda hassas bilgiler yada malzemeler içermiş olan sabit sürücüler de dahil tüm taşınabilir ortamlar bilgi güvenliğinden sorumlu grup tarafından belirlenen süreçler gereğince yok edilmelidir.

9-8 Kişisel tanımlayıcılar

Kural: Kimlik numarası dahil, sosyal güvenlik numarası, ehliyet numarası, doğum tarihi ve yeri ve annenin kızlık soyadı gibi kişisel tanımlayıcılar kimlik tespiti amacı ile kullanılmamalıdırlar. Bu tanımlayıcılar sır değildir ve sayısız yöntem ile elde edilebilirler.

9-9 Kuruluş şemaları

Kural: Şirketin kuruluş şemasında gösterilen ayrıntılar şirket çalışanları dışında kimseye verilmemelidir.

9-10 Çalışanlar ile ilgili özel bilgiler

Kural: çalınaların özel bilgilerine yönelik tüm talepler insan kaynaklarına yönlendirilmelidir.

Bilgisayar Kullanımı

10-1 Bilgisayara komut girmek

Kural: İstek sahibinin bilgi işlem bölümünün bir çalışanı olduğu onaylanmadığı sürece şirket çalışanları, başka birinin isteği üzerine bilgisayara ya da bilgisayarlarla ilgili donanıma hiçbir zaman komut girmemelidirler.

10-2 Dahili adlandırma standartları

Kural: İstek sahibinin şirkette çalıştığı onaylanmadan çalışanlar bilgisayar sistemlerinin ya da veri tabanlarının adlarını açıklamamalıdırlar.

10-3 Program çalıştırma talepleri

Kural: Şirket çalışanları, başka birinin isteği üzerine herhangi bir bilgisayar uygulamasını ya da programını çalıştırmamalıdırlar.

10-4 Yazılım indirmek ya da yüklemek

Kural: İstek sahibinin bilgi işlem bölümünün bir çalışanı olduğu onylanmadığı sürece şirket çalışanlarıbaşka birinin isteği doğrultusunda hiçbir zaman yazılım indirmemeli ya da yüklememelidir.

10-5 Düz metin parolaları ve e-posta

Kural: Şifreli olmadıkları sürece parolalar e-postayla gönderilmemelidirler.

10-6 Güvenlikle ilgili yazılımlar

Kural: Şirket çalışanları hiçbir zaman virüs/Truva Atı koruma, güvenlik duvarı ya da diğer güvenlikle ilgili yazılımları bilgi işlem bölümünden alınmış bir onay olmadan devre dışı bırakmamalı ya da kaldırmamalıdırlar.

10-7 Modemlerin yüklenmesi

Kural: Bİ bölümünden onay alınmadan herhangi bir bilgisayara modem bağlanamaz.

10-8 Modemler ve otomatik yanıt verme ayarları

Kural: Birilerinin bilgisayar sistemine modem bağlantısından girmesini önlemek amacıyla Bİ onaylı tüm bilgisayarların, modem otomatik yanıt verme özellikleri kapatılmalıdır.

10-9 Kırma araçları

Kural: Çalışanlar yazılım koruma mekanizmalarını alt etmek üzere tasarlanmış yazılım araçları indirmemeli ya da kullanmamalıdırlar.

10-10 Çevrimiçi şirket bilgileri

Kural: Çalışanlar herhangi bir herkese açık haber grubuna, foruma ya da bültene şirkete ait donanım ya da yazılımlarla ilgili ayrıntılar yazmamalı ve kurallara uygun olanlar dışında iletişim bilgileri vermemelidirler.

10-11 Disketler ve diğer elektronik ortamlar

Kural: Eğer bilgisayar bilgilerini saklamak için kullanılan disket ya da CD-ROM gibi ortamlar, çalışma alanında ya da çalışanın masasında bırakılmışsa ve bilinmeyen bir kaynaktan geliyorsa bilgisayar sistemine sokulmamalıdır.

10-12 Taşınabilir ortamların atılması

Kural: Bilgi silinmiş bile olsa herhangi bir zaman aralığında hassas şirket bilgilerinin tutulduğu bir elektronik ortamı çöpe atmadan önce ortam manyetik olarak silinmeli yada kurtarılamayacak şekilde zarar görmüş olmalıdır.

10-13 Parola korumalı ekran koruyucular

Kural: Tüm bilgisayar kullanıcıları bir ekran koruyucusu parolası oluşturmalı ve belli bir süre kullanılmadığı zaman bilgisayarı kilitleyen bir zaman aşımı süresi belirlemelidir.

10-14 Parola gizlilik taahhüdü

Kural: Yeni bir bilgisayar hesabı açılmadan önce çalışan ya da taşeron, parolaların hiçbir zaman herhangi birine açıklanmaması ya da paylaşılmaması gerektiğini ve bu kurallara uymayı kabul ettiğini gösteren yazılı bir beyan imzalamalıdır.

E-Posta Kullanımı

11-1 E-Posta ekleri

Kural: E-posta ekleri güvenilir bir kişiden gelmediği ya da işle ilgili olarak beklenmediği sürece açılmamalıdır.

11-2 Harici adreslere otomatik yönlendirme

Kural: Gelen e-postaların otomatik olarak harici bir e-posta adresine yönlendirilmesi yasaktır.

11-3 E-postaların yönlendirilmesi

Kural: Onaylanmamış bir kişiden gelen herhangi bir başka onaylanmamış kişiye e-posta aktarma talebi, talep sahibine kimlik tespiti yapılmasını gerektirir.

11-4 E-postaların onaylanması

Kural: Genel olarak sınıflandırılmamış bir bilgi talebi içeren ya da bilgisayarlarla ilgili donanımlara yönelik bir işlem yapılmasını isteyen ve güvenilir bir kişiden geliyor gibi görünen bir e-posta mesajı için ek bir tanımlama şekli daha gereklidir.

Telefon Kullanımı

12-1 Telefon anketlerine katılmak

Kural: Çalışanlar, başka kuruluşların ya da kişilerin soru sorma yoluyla yaptığı anketlere katılamazlar.Bu tarz talepler halkla ilişkiler bölümüne ya da diğer sorumlu kişilere yönlendirilmelidir.

12-2 Dahili telefon numaralarının verilmesi

Kural: Eğer onaylanmamış bir kişi çalışana telefon numarasını sorarsa, çalışan, şirket işlerinin yönetilmesi ile ilgili olarak numarayı vermenin gerekli olup olmadığı doğrultusunda uygun bir karar verebilir.

12-3 Sesli mesaj parolaları

Kural: Herhangi birinin sesli mesaj kutusuna parola bilgileri içeren mesajlar bırakmak yasaktır.

Faks Kullanımı

13-1 Faks gönderilmesi

Kural: İstek sahibinin kimlik tespiti yapılmadan kimseden faks alınamaz ve kimseye faks gönderilemez.

13-2 Faksla gönderilmiş talimatların onaylanması

Kural: Faksla gelen talimatları yerine getirmeden önce, gönderenin şirketin bir çalışanı ya da bir güvenilir kişi olduğu onaylanmalıdır.

13-3 Faksla hassas bilgilerin gönderilmesi

Kural: Başka çalışanların da erişebileceği bir yerde duran bir faks makinasına hassas bilgi göndermeden önce, gönderen, bir kapak sayfası göndermelidir. Alıcı kapak sayfasını alır almaz karşılık olarak bir sayfa gönderir ve faks başında olduğunu gösterir. Gönderici, daha sonra faksın tümünü gönderir.

13-4 Parola fakslamak yasaktır

Kural: Parolalar hiçbir koşulda faks aracılığıyla gönderilmemelidir.

Sesli Mesaj Kullanımı

14-1 Sesli mesaj parolaları

Kural: Sesli mesaj parolaları hiçbir nedenle başkalarına verilmemelidirler. Buna ek olarak sesli mesaj parolaları en çok doksan günde bir değiştirilmelidir.

14-2 Çoklu sistemlerde parolalar

Kural: Sesli mesaj kullanıcıları ister dahili isterse harici,telefon ya da bilgisayar sistemlerinde kullandıkları parolayı kullanmamalıdırlar.

14-3 Sesli mesaj parolalarının ayarlanması

Kural: Sesli mesaj kullanıcıları ve yöneticiler tahmin edilmesi zor olan sesli mesaj parolaları kullanmalıdırlar. Parolalar herhangi bir şekilde kullanan kişiyle ya da şirketle ilişkilendirilmemeli ve tahmin edilme olasılığı olan öngörülebilir bir düzende olmamalıdır.

14-4 “Eski” olarak işaretlenmiş mesajlar

Kural: Dinlenmemiş sesli mesajlar yeni mesaj olarak işaretlenmediğinde sesli mesaj yöneticisi, olası bir güvenlik ihlaline karşı uyarılmalı ve sesli mesaj parolası hemen değiştirilmelidir.

14-5 Harici sesli mesaj açılış notları

Kural: Şirket çalışanları dışarıya yönelik sesli mesaj açılış notlarında verdikleri bilgiyi sınırlamalıdırlar. Genel olarak, çalışanın günlük işleri ya da yolculuk tarihleriyle ilgili bilgiler verilmemelidir.

14-6 Sesli mesaj parola düzenleri

Kural: Sesli mesaj kullanıcıları bir bölümü sabit kalan, kalanı öngörülebilir bir şekilde değişen parolalar seçmemelidirler.

14-7 Gizli ya da özel bilgiler

Kural: Gizli ya da özel bilgiler sesli mesajlarla aktarılmamalıdır.

Parolalar

15-1 Telefon güvenliği

Kural: Parolalar hiçbir zaman telefonda verilmemelidir.

15-2 Bilgisayar parolalarının verilmesi

Kural: Bilgi işlem yöneticisinin yazılı onayı olmadan bilgisayar kullanıcıları hiçbir koşulda parolalarını başkalarına vermemelidir.

15-3 İnternet parolaları

Kural: Çalışanlar, şirket sisteminde kullandıkları parolanın bir benzerini ya da aynısını internet sitelerinde de kullanmamalıdırlar.

15-4 Çoklu sistemlerde parolalar

Kural: Şirket çalışanları aynı ya da benzeri bir parolayı birden fazla sistemde kullanmamalıdırlar.Bu kural çeşitli araçları (bilgisayar ya da sesli mesaj); çeşitli konumları (ev ya da); çeşitli sistemleri, araçları (yönlendirici ya da güvenlik duvarı) ya da programları (veritabanı ya da uygulama) kapsayabilir.

15-5 Parolaların yeniden kullanılması

Kural: Hiçbir bilgisayar kullanıcısı on sekiz aylık süre içerisinde aynı ya da benzer bir parola kullanmalıdır.

15-6 Parola yapısı

Kural: Çalışanları, bir bölümü sabit kalan diğer bölümü öngörülebilir bir değişen parolalar seçmemelidir.

15-7 Parola seçimi

Kural: Bilgisayar kullanıcıları aşağıdaki koşulları sağlayan bir parola yaratmalı ya da seçmelidir.

- Standart kullanıcıları hesapları için en az sekiz karakter ve ayrıcalıklı hesaplar için en az on iki karakter uzunluğunda olmalıdır.
- En az bir sayı, bir simge ($, -,I ,& gibi) ,bir küçük harf ve bir büyük harf (işletim sisteminde bulunan farklı yazı şekillerinin el verdişi ölçüde) içermelidir.
- Aşağıdakilerden herhangi birini de içermelidir: herhangi bir dildekisözlükte bulunabilecek bir kelime, çalışanın soyadı, hobileri, plaka numarası, Sosyal Güvenlik Numarası, adresi, telefon numarası, evcil hayvanının adı, doğum günü ya da bu kelimeleri içeren kelime grupları.
- Daha önce kullanılmış bir parolanın bir tarafı sabit bir tarafı değişmiş türden farklı bir şekli de olmamalıdır, kevin, kevin1, kevin2 ya ad kevinocak, kevinşubat gibi.

15-8 Parolaları not etmek

Kural: Çalışanlar parolalarını yalnızca bilgisayardan ya da başka parola korumalı donanımdan uzakta güvenli bir yere koyacaklarsa bir yere not edebilirler.

15-9 Bilgisayar dosyalarındaki şifrelenmemiş parolalar

Kural: Şifrelenmemiş parolalarherhangi bir bilgisayar dosyasında saklanmayacak ya da bir işlev tuşuyla çağrılabilecek şekilde programlanmayacaktır. Gerekli olduğu durumda parolalar, Bİ bölümünün yetkisiz erişimleri engellemek için onayladığı bir şifreleme yazılımı kullanılarak saklanmalıdır.

DIŞARIDAN ÇALIŞANLAR İÇİN KURALLAR

16-1 Küçük istemciler

Kural: Uzaktan erişim yetkisine sahip tüm şirket çalışanları şirket ağına bağlanmak için küçük istemci kullanmalıdırlar.

16-2 Dışarıdan çalışanların bilgisayarları için güvenlik yazılımları

Kural: Şirket ağına bağlanmak için kullanılan herhangi bir harici bilgisayar sisteminde virüs ve Truva Atı koruma programları ve (donanımdan ya da yazılımdan gelen) kişisel bir güvenlik duvarı bulunmalıdır. Virüs ve Truva Atı tanım dosyaları en azından haftalık olarak yenilenmelidir.

İNSAN KAYNAKLARI KURALLARI

17-1 Ayrılan çalışanlar

Kural: Ne zaman bir çalışan şirketten ayrılır ya da ilişkisi kesilirse, insan kaynakları hemen aşağıdaki işlemleri yerine getirmelidir:

- Çevrimiçi telefon rehberinden kişinin adını çıkartmalı ve sesli mesajlarını iptal etmeli ya da yönlendirmelidir.
- Bina girişlerinde ya da şirket lobilerinde görevli personeli bilgilendirmelidir.
- Çalışanın adını ayrılan çalışanlar listesine eklemeli ve bu liste, sıklığı bir haftadan az olmayacak şekilde tüm çalışanlara gönderilmelidir.

17-2 Bİ bölümünün uyarılması

Kural: Şirkette çalışan bir kişi işten ayrıldığında ya da işine son verildiğinde insan kaynakları, eski çalışanın, aralarında veri tabanı erişimi, uzaktan bağlantı ya da uzak noktalardan internet erişimi hesaplarının da bulunduğu tüm bilgisayar hesaplarını üptal etmesi için bilgi işlem bölümünü hemen haberdar etmelidir.

17-3 İşe alma sürecinde kullanılan gizli bilgiler

Kural: İlanlar ve iş boşluklarını doldurmak için uygun aday bulmaya yönelik diğer herkese açık davetler mümkün olduğu ölçüde şirketin kullandığı bilgisayar donanım ve yazılımları konusunda bilgi vermemelidir.

17-4 Çalışanların kişisel bilgileri

Kural: İnsan kaynakları bölümü, çalışanın ya da insan kaynakları yöneticisinin yazılı onayı olmadan halen çalışan ya da çalışmayan hiçbir personel, taşeron, danışman, geçici işçi ya da stajyerin kişisel bilgilerini açıklamamalıdır.

17-5 Sicil taramaları

Kural: Kendilerine bir iş önerilmeden ya da sözleşmeye dayanan bir iş ilişkisine girmeden önce tüm yeni işe başlayanlar, taşeronlar, danışmanlar, geçici işçiler ya da stajyerler için bir sicil taraması zorunlu olmalıdır.

FİZİKSEL GÜVENLİK KURALLARI

18-1 Personel olmayan kimlik tespiti

Kural: Kuryeler ve düzenli olarak şirket binalarına girmeleri gereken, şirket dışından kişilerin şirket güvenliğinin belirlediği kurallara uygun olarak düzenlenmiş özel yaka kartları ya da benzeri bir kimlikleri olmalıdır.

18-2 Ziyaretçi kimlik tespiti

Kural: Tüm ziyaretçiler içeri alınabilmeleri için geçerli sürücü ehliyeti ya da başka bir resimli kimlik belgesi göstermelidirler.

18-3 Ziyaretçilere eşlik edilmesi

Kural: Ziyaretçiler her zaman bir çalışanın eşliğinde olmalı ya da yanlarında refakatçi bulunmalıdır.

18-4 Geçici kimlikler

Kural: Başka bir tesisten gelen ve yanlarında personel kartları bulunmayan şirket çalışanları geçerli bir sürücü ehliyeti ya da benzeri resimli bir kimlik göstermeli ve onlara geçici bir ziyaretçi kartı verilmelidir.

18-5 Acil tahliye

Kural: Acil durumlarda ya da birtalim sırasında güvenlik görevlileri herkesin binalaı terkettiğinden emin olmalıdır.

18-6 Posta odasında ziyaretçiler

Kural: Bir şirket çalışanının gözetiminde olmadan hiçbir ziyaretçinin posta odasına girmesine izin verilmemelidir.

18-7 Araç plaka numaraları

Kural: Eğer şirketin bekçili bir otoparkı varsa, güvenlik görevlileri bu alana giren tüm araçların plakalarını not etmelidirler.

18-8 Çöp bidonları

Kural: Çöp bidonları her zaman şirket alanının içinde bulunmalı ve dışarıdan erişilebilir olmamalıdır.

DANIŞMA GÖREVLİLERİ İÇİN KURALLAR

19-1 Dahili telefon rehberi

Kural: Dahili telefon rehberinde açıklanan bilgilere yalnızca şirket çalışanları erişebilmelidir.

19-2 Belirli bölümlerin/ grupların telefon numaraları

Kural: Çalışanlar, arayanın geçerli bir nedeni olup olmadığını kontrol etmeden, şirket yardım masasının, telekomünikasyon bölümünün, bilgi işlemin ya da sistem yöneticisinin dış hat telefon numaralarını vermemelidirler. Danışma

görevlisi, bu gruplardan birine bir telefon aktarırken arayanın adını mutlaka açıklamalıdır.

19-3 Bilgi aktarımı

Kural: Santral memurları ve danışma görevlileri, çalışan olup olmadığını şahsen bilmedikleri kişiler adına not almamalı ya da bilgi aktarmamalıdır.

19-4 Alınmak üzere bırakılmış malzemeler

Kural: Bir kuryeye ya da tanımlanmamış başka bir kişiye herhangi bir şey verirken, danışma görevlisi ya da güvenlik görevlisi resimli bir kimlik görmeli ve kimlik bilgilerini kuralların öngördüğü şekilde kayıt defterine işlemelidir.

OLAY BİLDİRME GRUBU İÇİN KURALLAR

20-1 Olay bildirme grubu

Kural: Bir kişi ya da grup bu iş için görevlendirilmeli ve çalışanlar güvenlikle ilgili olayları onlara iletmek üzere bilgilendirilmelidir.

20-2 Sürmekte olan saldırılar

Kural: Olay bildirme grubuna, sürmekte olan bir toplum mühendisliği saldırısı bildirildiğinde grup, hedeflenen bölümlerde görevli ve bu iş için belirlenmiş çalışanları uyarmak üzere süreçleri başlatacaktır.