TÜRK STANDARDI

TS ISO/IEC 27002

Aralık 2013

ICS 35.040

Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri

Information technology - Security techniques - Code of practice for information security controls

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information

TÜRK STANDARDLARI ENSTİTÜSÜ
Necatibey Caddesi No.112 Bakanlıklar/ANKARA

Milli Önsöz

- Bu standard; kaynağı ISO/IEC 27002:2013 standardı olan TS ISO/IEC 27002:2013 Türk standardının Bilgi Teknolojileri ve İletişim İhtisas Kurulu'na bağlı TK01 Bilgi Teknolojileri ve İletişim Teknik Komitesi marifetiyle hazırlanan Türkçe tercümesidir.

- ISO resmi dillerinde yayınlanan diğer standard metinleri ile aynı haklara sahiptir.

- Bu standardda kullanılan bazı kelime ve/veya ifadeler patent haklarına konu olabilir. Böyle bir patent hakkının belirlenmesi durumunda TSE sorumlu tutulamaz.

- Bu standartta atıf yapılan standartların birebir karşılığı olarak yayınlanmış olan Türk Standartlarının numaraları aşağıda belirtilmiştir.

– Bu standardda atýf yapýlan standardlarýn milli karþýlýklarý aþaðýda verilmiþtir.

EN, ISO, IEC vb No	**Adı (İngilizce)**	**TS No**	**Adı (Türkçe)**
ISO/IEC 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary	TS ISO/IEC 27000	Bilgi Teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Genel bakış ve sözlük

ULUSLARARASI STANDARD
INTERNATIONAL STANDARD

ISO 27002

İkinci Baskı
2013-10-01

Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri

Information technology - Security techniques - Code of practice for information security controls

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information

Referans Numarası
ISO 27002:2013 (E)

TELİF HAKKI KORUMALI DOKÜMAN

ISO Telif Ofisi
Case postale 56 · CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Faks + 41 22 749 09 47
e-posta: copyright@iso.org
Web www.iso.org

İsviçre'de basılmıştır.

İçindekiler

Sayfa

Önsöz ..... **v**
0 Giriş ..... **vi**
0.1 Arka plan ve bağlam vi
0.2 Bilgi güvenliği gereksinimleri vi
0.3 Kontrollerin seçilmesi vii
0.4 Kendi kılavuzlarını geliştirme vii
0.5 Yaşam döngüsü değerlendirmeleri vii
0.6 İlgili standardlar vii
1 Kapsam **1**
2 Atıf yapılan standard ve/veya dokümanlar **1**
3 Terimler ve tarifler **1**
4 Bu standardın yapısı **1**
4.1 Maddeler 1
4.2 Kontrol kategorileri 1
5 Bilgi güvenliği politikaları **2**
5.1 Bilgi güvenliği için yönetimin yönlendirmesi 2
6 Bilgi güvenliğinin organizasyonu **3**
6.1 İç organizasyon 3
6.2 Mobil cihazlar ve uzaktan çalışma 5
7 İnsan kaynakları güvenliği **7**
7.1 İstihdam öncesi 7
7.2 Çalışma esnasında 8
7.3 İstihdamın sonlandırılması veya değiştirilmesi 10
8 Varlık yönetimi **11**
8.1 Varlıkların sorumluluğu 11
8.2 Bilgi sınıflandırma 13
8.3 Ortam işleme 14
9 Erişim kontrolü **16**
9.1 Erişim kontrolünün iş gereklilikleri 16
9.2 Kullanıcı erişim yönetimi 17
9.3 Kullanıcı sorumlulukları 20
9.4 Sistem ve uygulama erişim kontrolü 21
10 Kriptografi **23**
10.1 Kriptografik kontroller 23
11 Fiziksel ve çevresel güvenlik **25**
11.1 Güvenli alanlar 25
11.2 Teçhizat 28
12 İşletim güvenliği **32**
12.1 İşletim prosedürleri ve sorumlulukları 32
12.2 Kötücül yazılımlardan koruma 34
12.3 Yedekleme 35
12.4 Kaydetme ve izleme 36
12.5 İşletimsel yazılımın kontrolü 37
12.6 Tekniklik açıklıkların yönetilmesi 38
12.7 Bilgi sistemleri tetkik hususları 40
13 Haberleşme güvenliği **40**
13.1 Ağ güvenliği yönetimi 40
13.2 Bilgi transferi 42
14 Sistem edinimi, geliştirme ve bakımı **44**
14.1 Bilgi sistemlerinin güvenlik gereksinimleri 44
14.2 Geliştirme ve destek proseslerinde güvenlik 46
14.3 Test verisi 51
15 Tedarikçi ilişkileri **51**
15.1 Tedarikçi ilişkilerinde bilgi güvenliği 51
15.2 Tedarikçi hizmetleri sağlama yönetimi 54
16 Bilgi güvenliği ihlal olayı yönetimi **55**
16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirmelerin yönetimi 55
17 İş sürekliliği yönetiminin bilgi güvenliği hususları **58**
17.1 Bilgi güvenliği sürekliliği 58

17.2 Yedek fazlalıklar 60
18 Uyum 60
18.1 Yasal ve sözleşmeye tabi gereksinimlere uyum 60
18.2 Bilgi güvenliği gözden geçirmeleri 63
Kaynaklar 65

Önsöz

ISO (Uluslararası Standardizasyon Kuruluşu) ulusal standard kuruluşlarının (ISO ülke kuruluşları) dünya çapında federasyonudur. Uluslararası Standard hazırlama çalışması genelde ISO teknik komiteleri aracılığı ile yapılır. Teknik komitenin konusu ile ilgilenen üyelerin o teknik komitede temsil edilme hakkı vardır. ISO ile işbirliği içindeki resmi ya da sivil uluslararası kuruluşlar da, çalışmalarda yer alabilir. ISO, elektroteknik standardizasyonla ilgili tüm konularında Uluslararası Elektroteknik Komisyonu (IEC) ile yakın işbirliği içinde çalışır.

Uluslararası Standardlar, ISO/IEC Direktifleri Bölüm 2'ye göre yazılmıştır.

Teknik komitelerin ana görevi, Uluslararası Standard hazırlamaktır. Teknik komitelerin kabul ettiği Taslak Uluslararası Standardlar, oylama için üye ülke kuruluşlarına gönderilir. Bir Uluslararası Standardın yayınlanması, oy veren üye ülkelerin en az % 75'inin onayını gerektirir.

Bu dokümanın bazı kısımlarının patent haklarına konu olabileceğine dikkat edilmelidir. Böyle herhangi bir patent hakkının belirlenmesi durumunda ISO sorumlu tutulamaz.

ISO/IEC 27001, Ortak Teknik Komite ISO/IEC JTC 1, Bilgi teknolojisi Alt komitesi SC 27, BT Güvenlik teknikleri tarafından hazırlanmıştır.

Bu ikinci baskısı teknik olarak revize edilmiş olan ilk baskısı (ISO/IEC 27002:2005)'i iptal eder ve yerini alır.

0 Giriş

0.1 Arka plan ve bağlam

ISO/IEC 27001[10] standardına dayalı Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulanması sürecinde kontrolleri seçmek için kuruluşların bir referans model olarak kullanmaları ya da yaygın olarak kabul edilen bilgi güvenliği kontrolleri için kılavuz doküman olması amacıyla bu uluslararası standard hazırlanmıştır. Bu standard aynı zamanda sanayi ve kurumlara özgü bilgi güvenliği yönetim sistemi kılavuzlarının, söz konusu sektöre özgü bilgi güvenliği risk çevrelerinin de dikkate alınarak geliştirilmesi amacıyla hazırlanmıştır.

Her çeşit ve büyüklükteki kuruluş (kamu ve özel sektör, ticari ve ticari olmayan), elektronik, fiziksel ve sözel de dâhil olmak üzere çeşitli biçimlerde (örneğin; konuşmalar ve sunumlar) bilgileri toplar, işler, saklar ve iletir.

Bilginin değeri yazılı kelimeler, numaralar ve görüntülerin ötesine geçer: bilgi birikimi, kavramlar, fikirler ve marka bilginin soyut biçiminin örnekleridir. Birbirine bağlı bir dünyada, bilgi ve ilgili prosesler, sistemler, ağlar ve bunların işletilmesine katılan personel diğer önemli varlıklar gibi bir kuruluşun işi için gerekli, çeşitli tehditlere karşı ele alınması ve korunması gereken varlıklardır.

Prosesler, sistemler, ağlar ve insanların doğası gereği açıklıkları olduğundan bu varlıklar kasıtlı ve kazayla ortaya çıkan tehditlere maruz kalırlar. İş prosesleri ve sistemlerdeki değişiklikler ya da diğer dış değişiklikler (yeni yasa ve düzenlemeler gibi) yeni bilgi güvenliği risklerini oluşturabilir. Bu nedenle, tehditler birçok yoldan kuruluşa zarar vermek için zafiyetlerden faydalanır ve bilgi güvenliği riskleri her zaman mevcuttur. Etkili bilgi güvenliği, tehditlere ve zafiyetlere karşı kuruluşu koruyarak bu riskleri ve kuruluşun varlıklarına olan etkiyi azaltır.

Politikalar, prosesler, prosedürler, organizasyon yapıları ve yazılım ve donanım fonksiyonları da dâhil olmak üzere kontrollerin uygun bir kümesi uygulanarak bilgi güvenliği sağlanır. Gerektiğinde kuruluşun özel güvenlik ve iş amaçlarını karşılamak için bu kontrollerin oluşturulması, uygulanması, izlenmesi, gözden geçirilmesi ve iyileştirilmesi gerekmektedir. ISO/IEC 27001[10]'de tanımlandığı gibi bir BGYS, tutarlı bir yönetim sisteminin genel çerçevesinde bilgi güvenliği kontrollerinin kapsamlı bir kümesinin uygulanması için kuruluşun bilgi güvenliği risklerinin koordineli bir görünümünü sağlar.

Birçok bilgi sistemi ISO/IEC 27001[10] ve bu standard anlamında güvenli olacak şekilde tasarlanmamıştır. Teknik yollarla elde edilebilir güvenlik sınırlıdır ve uygun bir yönetim ve prosedürler tarafından desteklenmelidir. Hangi kontrollerin olması gerektiğini belirlemek için dikkatli bir planlama yapılması ve detaylara özen gösterilmesi gerekmektedir. Başarılı bir BGYS uygulaması kuruluştaki tüm çalışanların desteğini gerektirir. Ayrıca; hissedarların, tedarikçilerin ya da diğer dış tarafların katılımını gerektirebilir. Dış taraflardan uzman tavsiyesi de gerekebilir.

Daha genel bir anlamda, etkin bilgi güvenliği; işi mümkün kılan bir faktör olarak, yönetim ve diğer paydaşları kuruluşun varlıklarının oldukça güvenli ve zararlara karşı korumalı olmasını temin eder.

0.2 Bilgi güvenliği gereksinimleri

Bir kuruluşun güvenlik gereksinimlerini tanımlaması esastır. Güvenlik gereksinimleri ile ilgili üç ana kaynak vardır.

a) Kuruluşun genel iş stratejisi ve hedefleri dikkate alınarak kuruluşun risk değerlendirmesi. Risk değerlendirmesi aracılığıyla, varlıkların karşı karşıya oldukları tehditler tanımlanır, açıklıklar ve gerçekleşme olasılıkları değerlendirilir ve potansiyel etkileri tahmin edilir;

b) Bir kuruluşun ticari ortakları, yüklenicileri ve hizmet sağlayıcıları ile bunların sosyo-kültürel çevresinin karşılaması gereken yasal, kanuni, düzenleyici ve sözleşme ile ilgili gerekleri,

c) Kuruluşun bilgi işleme, işleme, depolama, iletişim ve arşivleme faaliyetlerini desteklemek üzere geliştirilmiş belirli ilkeler, hedefler ve iş gereksinimleri kümesi.

Kontrollerin uygulanmasında kullanılan kaynaklar, bu kontrollerin yokluğunda güvenlik sorunlarının neden olacağı muhtemel iş zararlarına karşı dengelenmelidir. Risk değerlendirmesi sonuçları, bilgi güvenliği risklerinin yönetilmesi için ve bu risklere karşı korumak amacıyla seçilen kontrollerin uygulanması için uygun yönetim eylemleri için kılavuzluk sağlar, önceliklerin belirlenmesini sağlar.

Risk değerlendirme, risk işleme, risk kabulü, risk iletişimi, risk izleme ve risk gözden geçirme konusunda tavsiyeler de dâhil olmak üzere ISO/IEC 27005[11] standardı bilgi güvenliği risk yönetimi hakkında kılavuzluk sağlar.

0.3 Kontrollerin seçilmesi

Kontroller bu standarddan ya da diğer kontrol kümelerinden seçilebilir ya da uygun biçimde özel ihtiyaçları karşılamak üzere yeni kontroller geliştirilebilir.

Kontrollerin seçimi; kuruluş kararlarında temel alınan risk kabulüne, risk işleme seçeneklerine ve kuruluşta uygulanan genel risk yönetimi yaklaşımına bağlıdır. Aynı zamanda ilgili tüm ulusal ve uluslararası yasa ve düzenlemelere tabii olmalıdır. Ayrıca kontrol seçimi, savunma derinliği sağlamak için kontrollerin birbirleriyle olan etkileşim tarzına bağlıdır.

Bu standarddaki bazı kontroller, bilgi güvenliği yönetimi için kılavuzluk sağlayabilir ve kuruluşların çoğu için uygulanabilir olarak kabul edilebilir. Kontroller, uygulama kılavuzu ile birlikte aşağıda daha ayrıntılı olarak anlatılmıştır. Kontrollerin seçimi hakkında ve diğer risk işleme seçenekleri hakkında daha fazla bilgi ISO/IEC 27005[11] standardında bulunabilir.

0.4 Kendi kılavuzlarını geliştirme

Bu standard, kuruluşa özgü kılavuz geliştirmek için bir başlangıç noktası olarak kabul edilebilir. Bu uygulama esası içindeki, kılavuz ve kontrollerin tamamı uygulanabilir olmayabilir. Ayrıca, bu standardda yer almayan ek kontroller ve kılavuzlar gerekebilir. Ek kontroller veya kılavuzlar eklendiğinde, denetçiler ve iş ortakları tarafından uyumluluk denetimini kolaylaştıracak çapraz başvuruları bu standardın hükümlerine dâhil etmek yararlı olabilir.

0.5 Yaşam döngüsü değerlendirmeleri

Bilgi; oluşturulma ve depolama, işleme, kullanım ve iletim yoluyla tekrar kullanımından nihai imha ya da bozulmaya kadar olan doğal bir yaşam döngüsüne sahiptir. Varlıkların değeri ve riski kendi yaşam döngüleri içerisinde değişebilir (örneğin; şirketin mali hesaplarına yetkisiz erişim ya da hırsızlık, bu bilgiler resmen yayınlandıktan sonra daha az önemli hale gelir) ama bilgi güvenliği tüm aşamalarda bir dereceye kadar önemini korumaktadır.

Bilgi sistemlerinin; hizmetin durdurulmasının ve yok edilmesinin sonuna kadar düşünülmüş, belirtilmiş, tasarlanmış, test edilmiş, uygulanmış, kullanılmış, sürdürülmüş yaşam döngüleri vardır. Bilgi güvenliği tüm aşamalarda göz önünde bulundurulmalıdır. Yeni sistem geliştirmeleri ve mevcut sistemlerdeki değişiklikler, kuruluşların güvenlik kontrollerinin, gerçek olaylar ve mevcut ve öngörülen bilgi güvenliği risklerinin de hesaba katılarak güncellemesi ve geliştirmesi için fırsatlar sunar.

0.6 İlgili standardlar

Bu standard, çok farklı kuruluşlarda yaygın olarak uygulanan geniş yelpazedeki bilgi güvenliği kontrollerine ilişkin kılavuzluk sağlarken, ISO/IEC 27000 ailesinde kalan diğer standardlar bilgi güvenliği yönetimi genel sürecinin diğer yönleri üzerinde tamamlayıcı tavsiye ya da şartları içerir.

Hem BGYS hem de standardlar ailesine genel bir bakış için ISO/IEC 27000 standardına bakılmalıdır. ISO/IEC 27000 standardı, ISO/IEC 27000 standard ailesinde kullanılan terimlerin çoğunu tanımlayan bir sözlüğü sağlar ve standard ailesinin her bir üyesi için kapsamı ve amacı açıklar.

ULUSLARARASI STANDARD **ISO / IEC 27002: 2013**

Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği kontrolleri için uygulama prensipleri

1 Kapsam

Bu standard, kuruluşun bilgi güvenliği risk çevresi/çevreleri dikkate alınarak kontrollerin seçilmesini, uygulanmasını ve yönetimini de içeren kurumsal bilgi güvenliği standardları ve bilgi güvenliği yönetimi uygulamaları için kılavuzluğu kapsar.

Bu standard aşağıdakileri gerçekleştirecek kuruluşlar tarafından kullanılmak üzere tasarlanmıştır:

a) ISO/IEC 27001 standardına dayalı Bilgi Güvenliği Yönetim Sistemi uygulanması sürecinde kontrollerin seçilmesi; [10]
b) Genel kabul görmüş bilgi güvenliği kontrollerinin uygulanması;
c) Kendi bilgi güvenliği yönetim kılavuzlarını geliştirilmesinde.

2 Atıf yapılan standard ve/veya dokümanlar

Aşağıda atıf yapılan dokümanlar, bu dokümanın uygulanması için mecburidir. Tarihi belirtilmiş atıflar için sadece atıf yapılan baskı uygulanır. Tarihi belirtilmemiş atıflar için, atıf yapılan dokümanın en son baskısı (tüm değişiklikleri içeren) uygulanır.

ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

3 Terimler ve tarifler

Bu dokümanın amaçları için ISO/IEC 27000 standardında verilen terimler ve tarifler kullanılır.

4 Bu standardın yapısı

Bu standard, 14 ana güvenlik kontrol maddesi altında toplamda 35 ana güvenlik kategorisi ve 114 kontrolünü içerir.

4.1 Maddeler

Güvenlik kontrollerini tanımlayan her bir madde bir veya daha fazla ana güvenlik kategorisi içerir.

Bu standardda maddelerin sırası, bu maddelerin önem derecesini göstermez. Koşullara bağlı olarak, herhangi bir güvenlik kontrolü ya da bütün maddeler önemli olabilir. Bu nedenle bu standardı uygulayan her bir kuruluş, uygulayacağı kontrolleri, bunların önem derecelerini ve bunların münferit iş proseslerine uygulanma durumunu belirlemelidir. Ayrıca, bu standardda yer alan tüm listeler öncelik sırasında değildir.

4.2 Kontrol kategorileri

Her ana güvenlik kontrol kategorisi aşağıdakileri içerir:

a) Neyin başarılacağını ifade eden bir kontrol hedefini,
b) Kontrol hedefine ulaşmak için uygulanabilecek bir veya daha fazla sayıda kontrolü.

Kontrol açıklamaları aşağıdaki şekilde yapılandırılmıştır:

Kontrol
Kontrol amacını karşılamak için özel kontrol ifadesini tanımlar.

Uygulama kılavuzu
Kontrol amacını karşılamak ve kontrollerin uygulanmasını desteklemek için daha detaylı bilgi sağlar. Bu kılavuzlar her durumda hedefe tam uygun ya da yeterli olmayabilir ve kuruluşun özel kontrol gereksinimlerini yerine getiremeyebilir.

Diğer bilgiler
Yasal hususları ve diğer standardlara atıflar gibi dikkate alınması gereken diğer bilgileri sağlar. Sağlanacak hiçbir bilgi mevcut değilse bu bölüm gösterilmez.

5 Bilgi güvenliği politikaları

5.1 Bilgi güvenliği için yönetimin yönlendirmesi

Amaç: Bilgi güvenliği için, iş gereksinimleri ve ilgili yasalar ve düzenlemelere göre yönetimin yönlendirme ve desteğini sağlamak.

5.1.1 Bilgi güvenliği politikaları

Kontrol
Bilgi güvenliği politikaları tanımlanmalı, yönetim tarafından onaylanmalı ve yayınlanarak çalışanlara ve ilgili dış taraflara duyurulmalıdır.

Uygulama kılavuzu
Kuruluşlar; en üst düzeyde, yönetim tarafından onaylanmış "bilgi güvenliği politikası"nı tanımlamalı ve bu politika, kendi bilgi güvenliği amaçlarını yönetmek için kuruluşun yaklaşımını ortaya koymalıdır.

Aşağıdakiler tarafından oluşturulan gereksinimler bilgi güvenliği politikasında ele alınmalıdır:

a) İş stratejisi,
b) Düzenlemeler, yasalar ve sözleşmeler,
c) Mevcut ve öngörülen bilgi güvenliği tehdit ortamı.

Bilgi güvenliği politikası aşağıdakiler ile ilgili ifadeler içermelidir:

a) Bilgi güvenliğinin tanımını ve bilgi güvenliği ile ilgili tüm faaliyetlerine kılavuzluk için amaçları ve ilkeleri,
b) Tanımlanmış rollere bilgi güvenliği yönetimi için genel ve özel sorumlulukların atamasını,
c) Sapmaları ve özel durumları işlemek için prosesleri.

Daha alt düzeyde; bilgi güvenliği politikası, bilgi güvenliği kontrollerini zorunlu tutan konuya özel politikalarla desteklenmelidir. Konuya özel politikalar tipik olarak, kuruluşun içinde belirli hedef gruplarının ihtiyaçlarını karşılamak ya da belirli konuları kapsayacak şekilde yapılandırılır.

Bu tür politika konuları aşağıdaki hususları içerir:

a) Erişim kontrolü (bk. Madde 9),
b) Bilgi sınıflandırma (ve işleme) (bk. Madde 8.2),
c) Fiziksel ve çevresel güvenlik (bk. Madde 11),
d) Son kullanıcı odaklı konular:
    1) Varlıkların kabul edilebilir kullanımı (bk. Madde 8.1.3),
    2) Temiz masa ve temiz ekran (bk. Madde 11.2.9),
    3) Bilgi transferi (bk. Madde 13.2.1),
    4) Mobil cihazlar ve uzaktan çalışma (bk. Madde 6.2),
    5) Yazılım kurulumu ve kullanımı ile ilgili kısıtlamalar (bk. Madde 12.6.2),
e) Yedekleme (bk. Madde 12.3),
f) Bilgi transferi (bk. Madde 13.2),
g) Kötücül yazılımlardan koruma (bk. Madde 12.2),
h) Teknik açıklıkların yönetimi (bk. Madde 12.6.1),
i) Kriptografik kontroller (bk. Madde 10),
j) Haberleşme güvenliği (bk. Madde 13),
k) Kişi tespit bilgisinin mahremiyeti ve korunması (bk. Madde 18.1.4),
l) Tedarikçi ilişkileri (bk. Madde 15).

Bu politikalar; çalışanlara ve ilgili dış taraflara duyurulmalı ve amaçlanan okuyucu için erişilebilir ve anlaşılabilir olmalıdır. Örneğin; bir "bilgi güvenliği farkındalık, eğitim ve öğretim programı" (bk. Madde 7.2.2) bağlamında.

Diğer bilgiler
Bilgi güvenliği için iç politikalara duyulan ihtiyaç kuruluştan kuruluşa değişebilir. Daha büyük ve daha karmaşık kuruluşlarda, kontrollerin beklenen düzeylerinin tanımlanmasının ve onaylanmasının uygulanan kontrollerden ayrıldığı ya da kuruluş içerisinde çok farklı insanlara ve fonksiyonlara politikaların uygulandığı durumlarda iç politikalar özellikle faydalıdır. Bilgi güvenliği için politikalar tek bir "bilgi güvenliği politikası" dokümanında ya da tek fakat ilgili dokümanların bir kümesinde verilebilir.

Bilgi güvenliği politikası kuruluş dışına dağıtılırsa, gizli bilgilerin ifşa edilmemesine dikkat edilmelidir.

Bazı kuruluşlar politika dokümanları için "Standartlar", "Direktifler" ya da "Kurallar" gibi diğer terimleri kullanmaktadır.

5.1.2 Bilgi güvenliği için politikaların gözden geçirilmesi

Kontrol
Bilgi güvenliği politikaları, belirli aralıklarla veya önemli değişiklikler ortaya çıktığında sürekli uygunluk, kesinlik ve etkinliği sağlamak amacıyla gözden geçirilmelidir.

Uygulama kılavuzu
Her politikanın; politikanın geliştirilmesi, gözden geçirilmesi ve değerlendirilmesi için yönetim tarafından onaylanmış sorumluluğa haiz bir sahibi olmalıdır. Gözden geçirme; kurumsal çevre değişikliklerinde, iş koşullarında, yasal şartlarda veya teknik ortamdaki değişimler nedeniyle kuruluşun politikasını ve bilgi güvenliği yönetimi yaklaşımını iyileştirmesi için fırsatları içermelidir.

Bilgi güvenliği politikalarının gözden geçirilmesinde yönetimin gözden geçirmesinin sonuçları dikkate alınmalıdır.

Revize edilen bir politika için yönetimin onayı alınmalıdır.

6 Bilgi güvenliğinin organizasyonu

6.1 İç organizasyon

Amaç: Kuruluş içerisinde bilgi güvenliği operasyonu ve uygulamasının başlatılması ve kontrol edilmesi amacıyla, bir yönetim çerçevesi kurmak.

6.1.1 Bilgi güvenliği rolleri ve sorumlulukları

Kontrol
Tüm bilgi güvenliği sorumlulukları tanımlanmalı ve tahsis edilmelidir.

Uygulama kılavuzu
Bilgi güvenliği sorumluluklarının tahsisi, bilgi güvenliği politikaları ile uyumlu şekilde yapılmalıdır (bk. Madde 5.1.1). Tek tek varlıkların korunması ve özel güvenlik proseslerini yürütmek için sorumluluklar açıkça belirtilmelidir. Bilgi güvenliği risk yönetimi faaliyetleri ve artık risklerin kabulü için sorumluluklar tanımlanmalıdır. Bu sorumluluklar gereken yerlerde, özel yerleşke ve bilgi işleme tesisleri için daha ayrıntılı bir kılavuz ile desteklenmelidir. Varlıkların korunması ve özel güvenlik proseslerinin yürütülmesi için yerel sorumluluklar açıkça tanımlanmalıdır.

Bilgi güvenliği sorumluluğu tahsis edilen kişiler güvenlik görevleriyle ilgili yetkilerini başkalarına devredebilirler. Ancak; hesap verme sorumlulukları devam eder ve bu kişiler tüm yetki devri yapılmış görevlerin doğru uygulandığını tespit etmelidir.

Kişilerin sorumlu oldukları alanlar belirtilmelidir. Özellikle aşağıdaki maddeler sorumluluk tanımında yer almalıdır:

a) Varlıklar ve bilgi güvenliği prosesleri tanımlanmalı ve tarif edilmelidir,
b) Her bir varlık ya da bilgi güvenliği prosesi için sorumluluk tahsis edilmeli ve bu sorumluluk detayları yazılı hale getirilmelidir (bk. Madde 8.1.2),
c) Yetkilendirme seviyeleri tanımlanmalı ve yazılı hale getirilmelidir,
d) Bilgi güvenliği alanında atanan kişiler sorumluluklarını yerine getirebilmek için alanında yetkin olmalı ve geliştirmeleri takip edebilmeler için fırsat verilmelidir,
e) Tedarikçi ilişkilerinin bilgi güvenliği hususları koordinasyonu ve izlemesi tanımlanmalı ve yazılı hale getirilmelidir.

Diğer bilgiler
Birçok kuruluşta, bilgi güvenliğinin geliştirilmesi ve uygulanması ile tanımlanan kontrollerin desteklenmesi için genel sorumluluk bilgi güvenliği yöneticisine verilmektedir.

Ancak, kaynak bulma ve uygulama kontrollerinin sorumluluğu çoğu zaman münferit olarak yöneticilere verilmektedir. Yaygın bir uygulama, her bir varlığa gün ve gün korunmasından sorumlu olacak bir sahip atanmasıdır.

6.1.2 Görevlerin ayrılığı

Kontrol
Çelişen görevler ve sorumluluklar, yetkilendirilmemiş veya kasıtsız değişiklik fırsatlarını veya kuruluş varlıklarının yanlış kullanımını azaltmak amacıyla ayrılmalıdır.

Uygulama kılavuzu
Sadece tek bir kişinin, yetkilendirme veya tespit etme imkânı olmadan varlıklara erişim, güncelleme veya kullanmasına müsaade edilmediği hususuna dikkat edilmelidir. Bir olayın başlatılması onun yetkilendirilmesinden ayrılmalıdır. Kontroller tasarlanırken atlatma amaçlı karşılıklı anlaşma olasılığı göz önünde bulundurulmalıdır.

Küçük kuruluşlar, görevlerin ayrılığını başarmakta zorlanabilirler; fakat bu prensip mümkün olduğunca ve pratikte uygulanmalıdır. Ayrım yapmak zorlaşırsa, faaliyetlerin izlenmesi, denetim kayıtları ve yönetimin gözetimi gibi diğer kontroller dikkate alınmalıdır.

Diğer bilgiler
Görevler ayrımı, bir kuruluşun varlıklarının yanlışlıkla ya da kasıtlı olarak yanlış kullanım riskini azaltmak için bir yöntemdir.

6.1.3 Otoritelerle iletişim

Kontrol
İlgili otoritelerle uygun iletişim kurulmalıdır.

Uygulama kılavuzu
Kuruluşlar, ne zaman ve hangi otoritelerle (örneğin; kolluk kuvvetleri, düzenleyici kurumlar, denetim otoriteleri) temas kurulacağına ve tespit edilen bilgi güvenliği ihlal olaylarının zamanında nasıl raporlanacağını (örneğin; yasaların ihlal edildiğinden şüphelenildiğinde) belirten prosedürlere sahip olmalıdırlar.

Diğer bilgiler
İnternet üzerinden gelen saldırılara maruz kalan kuruluşlar, saldırı kaynağına karşı harekete geçmek için yetkili otoritelere ihtiyaç duyabilir.

Bu tür teması sağlamak, bilgi güvenliği ihlal olay yönetimi (bk. Madde 16) ya da iş sürekliliği ve acil durum planlaması sürecini (bk. Madde 17) desteklemek için bir şart olabilir. Düzenleyici kuruluşlar ile temas halinde olmak kuruluşlar için yasa ya da düzenlemelerde olabilecek değişiklikleri tahmin etmek ve hazırlanmak için yararlıdır. Diğer yetkililer ile yapılacak temaslar; altyapı hizmetleri, acil servisleri, elektrik tedarikçileri ve örneğin; itfaiye (iş sürekliliği ile bağlantılı olarak), telekomünikasyon sağlayıcıları (hat yönlendirme ve erişilebilirlik ile bağlantılı olarak) ve su tedarikçileri (teçhizat için soğutma tesisleri ile bağlantılı olarak) gibi sağlık ve güvenlik hizmetlerini kapsar.

6.1.4 Özel ilgi grupları ile iletişim

Kontrol
Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel dernekler ile uygun iletişim kurulmalıdır.

Uygulama kılavuzu
Özel ilgi gruplarına veya forumlara üyelik aşağıdakiler için bir araç olarak kabul edilmelidir:

a) Sahip olunan bilgiyi geliştirmek amacıyla en iyi uygulamalar ve ilgili güvenlik bilgileri hakkında güncel bilgi sahibi olmak için,
b) Bilgi güvenliği ortamının anlaşılmasının, güncel ve eksiksiz olduğundan emin olmak için,
c) Alarmlar, öneriler, saldırılar ve güvenlik açıkları ile ilgili yamalar hakkında erken uyarı almak için,
d) Uzman bilgi güvenliği tavsiyelerine erişmek için,
e) Yeni teknolojiler, ürünler, tehdit ya da açıklıklar hakkında karşılıklı bilgi değişimi ve bilgi paylaşım için,
f) Bilgi güvenliği ihlal olaylarını ele alırken uygun irtibat noktaları sağlamak için (bk. Madde 16).

Diğer bilgiler
Bilgi paylaşım anlaşmaları, güvenlik konularında işbirliği ve koordinasyonu arttırmak için yapılabilir. Bu tür anlaşmalar gizli bilgilerin korunması için şartları tanımlamalıdır.

6.1.5 Proje yönetiminde bilgi güvenliği

Kontrol
Proje yönetiminde, proje türüne bakılmaksızın bilgi güvenliği ele alınmalıdır.

Uygulama kılavuzu
Bilgi güvenliği, bilgi güvenliği risklerinin tanımlanması ve bir projenin parçası olarak ele alınmasını sağlamak için kuruluşun proje yönetimi yöntemine/yöntemlerine entegre edilmelidir. Bu, projenin karakteri ne olursa olsun herhangi bir proje için genel olarak geçerlidir. Örneğin; çekirdek iş süreci, BT, tesis yönetimi ve diğer destek prosesleri için bir proje. Kullanımdaki proje yönetim yöntemleri aşağıdaki hususları gerektirmelidir:

a) Bilgi güvenliği amaçlarının proje amaçlarına dâhil olması,
b) Bilgi güvenliği risk değerlendirmesinin gerekli kontrollerin tanımlanması için projenin erken bir aşamasında yapılması,
c) Bilgi güvenliğinin uygulanan proje metodolojisinin her aşamasının bir parçası olması.

Tüm projelerde bilgi güvenliği etkileri düzenli olarak ele alınmalı ve gözden geçirilmelidir. Bilgi güvenliği için sorumluluklar tanımlanmalı ve proje yönetim yöntemlerinde tanımlanan rollere tahsis edilmelidir.

6.2 Mobil cihazlar ve uzaktan çalışma

Amaç: Uzaktan çalışma ve mobil cihazların güvenliğini sağlamak.

6.2.1 Mobil cihaz politikası

Kontrol
Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.

Uygulama kılavuzu
Mobil cihazlar kullanılırken, iş bilgilerinin ele geçirilmemesini temin için özel bir önem gösterilmelidir. Mobil cihaz politikası, korumasız ortamlarda mobil cihazların çalışması riskini hesaba katmalıdır.

Mobil cihaz politikası aşağıdaki hususları dikkate almalıdır:

a) Mobil cihazların kaydı,
b) Fiziksel koruma için gereksinimler,
c) Yazılım kurulum kısıtlaması,
d) Mobil cihaz yazılım sürümleri ve yamaların uygulanması için gereksinimler,

e) Bilgi hizmetlerine bağlantı kısıtlaması,
f) Erişim kontrolleri,
g) Kriptografik teknikler,
h) Kötücül yazılım koruması,
i) Uzaktan devre dışı bırakma, silme ya da kilitleme,
j) Yedekleme,
k) Web servislerinin ve web uygulamalarının kullanımı.

Halka açık yerlerde, toplantı odalarında ve diğer korumasız alanlarda mobil cihazların kullanımına dikkat edilmelidir. Bu cihazlar tarafından saklanan ve işlenen bilginin, açıklanmasına ya da yetkisiz erişimine karşı koruma bulunmalıdır. Örneğin; kriptografi teknikleri kullanmak (bk. Madde 10) ve gizli kimlik doğrulama bilgisinin kullanımını zorlamak (bk. Madde 9.2.4).

Mobil cihazlar; araba ve diğer ulaşım araçları, otel odaları, konferans merkezleri ve toplantı salonları gibi yerlerde hırsızlığa karşı fiziksel olarak da korunmalıdır. Mobil cihazların çalınması ya da kaybolması durumları için yasal, sigorta ve kuruluşun diğer güvenlik gereksinimleri dikkate alınarak özel bir prosedür oluşturulmalıdır. Önemli, hassas ya da kritik iş bilgilerini taşıyan cihazlar sahipsiz bırakılmamalı, mümkünse fiziksel olarak kilitlenmeli ya da cihazı güvenli hale getirmek için özel kilitler kullanılmalıdır.

Mobil cihaz kullanan personeller için, bu şekilde çalışmalardan kaynaklanan riskler ve uygulanması gereken kontroller ile ilgili olarak farkındalıklarının arttırılması amacıyla eğitim düzenlenmelidir.

Mobil cihaz politikası kişisel mobil cihazların kullanımına izin veriyorsa, politika ve diğer güvenlik önlemlerinde aşağıdaki hususlara dikkat edilmelidir:

a) Cihazların özel ve iş kullanımının ayrılması. Bu ayrım0 özel cihazda bulunan iş verisinin ayrılması ve korunması gibi yazılımların kullanılmasını içerir,
b) Kullanıcıların görevlerini kabul ettikleri son kullanıcı anlaşmasını imzalamalarından sonra iş bilgilerine erişim sağlanması (fiziksel koruma, yazılım güncelleme vb.), iş verilerinin sahipliğinden feragat, cihazın çalınması ya da kaybolması ya da hizmetin kullanımı yetkilendirmesi için vakit olmadığında kuruluş tarafından verilerin uzaktan silinmesine izin verilmesi. Bu politikada mahremiyet mevzuatının dikkate alınması gerekmektedir.

Diğer bilgiler
Mobil cihazların kablosuz ağ bağlantıları (wi-fi) diğer ağ bağlantısı türlerine benzer, ancak; kontrollerin tanımlanmasında önemli farklılıklara dikkat edilmelidir. Tipik farklılıklar şunlardır:

a) Bazı kablosuz güvenlik protokolleri olgunlaşmamıştır ve bilinen açıklıklara sahiptir,
b) Mobil cihazlarda depolanan bilgiler, kısıtlı ağ bant genişliği ya da yedeklemelerin planlandığı zamanlarda mobil cihazların bağlanamaması nedeniyle yedeklenemeyebilir.

Mobil cihazlar sabit kullanım cihazları ile genellikle ağ, internet erişimi, e-posta ve dosya işleme gibi ortak fonksiyonları paylaşır. Bilgi güvenliği kontrolleri mobil cihazlar için genellikle sabit kullanım cihazlarında kabul edilen kontrollerden ve bu cihazların kuruluşun tesisi dışındaki kullanımı ile gündeme gelen tehditleri ele alan kontrollerden oluşur.

6.2.2 Uzaktan çalışma

Kontrol
Uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak amacı ile bir politika ve destekleyici güvenlik önlemleri uygulanmalıdır.

Uygulama kılavuzu
Uzaktan çalışma faaliyetlerine izin veren kuruluşlar, kullanılan uzaktan çalışma için şartları ve kısıtlamaları tanımlayan bir politika hazırlamalıdır. Uygulanabilir görüldüğü ve yasalarla izin verildiği durumda, aşağıdaki hususlar dikkate alınmalıdır:

a) Binanın ve yerel çevrenin fiziksel güvenliği dikkate alınarak, uzaktan çalışma alanının mevcut fiziksel güvenliği,
b) Önerilen uzaktan çalışma ortamı,
c) Kuruluşun iç sistemlerine uzaktan erişim ihtiyacı, erişilecek ve haberleşme hattından geçirilecek bilginin hassasiyeti ve dâhili sistemin hassaslığı dikkate alınarak haberleşme güvenlik gereksinimleri,
d) Kişiye ait teçhizat üzerindeki bilgilerin işlenmesini ve saklanmasını önleyen sanal masaüstü erişim izni,

e) Aynı ikametgâhı kullanan aile ve arkadaşlar gibi kişiler tarafından bilgi ve kaynaklara yetkisiz erişim tehdidi,
f) Ev ağlarının kullanımı ve kablosuz ağ hizmetleri yapılandırmasında gereksinimler ya da kısıtlamalar,
g) Özel kişilere ait teçhizatlar üzerinde geliştirilen fikri mülkiyet hakları ile ilgili anlaşmazlıkları önlemeye yönelik politika ve prosedürler,
h) Yasalarla engellenebilen kişiye ait teçhizata erişim (cihazın güvenliğinin doğrulanması için ya da bir soruşturma esnasında),
i) Çalışanlara ve dış kullanıcılara ait özel iş istasyonları üzerinde istemci yazılımı lisanslama için kuruluş tarafından yazılım lisans anlaşması yapılması,
j) Kötücül yazılımdan koruma ve güvenlik duvarı gereksinimleri.

Dikkate alınması gereken kılavuzlar ve düzenlemeler aşağıdakileri de içermelidir:

a) Kuruluşun kontrolü altında olmayan özel mülkiyete ait teçhizat kullanımının yasak olduğu yerlerde uzaktan çalışma faaliyetleri için uygun donanım ve depolama mobilyalarının sağlanması,
b) İzin verilmiş işin bir tarifi, iş saatleri, tutulan bilginin sınıflandırılması ve uzaktan çalışan kişinin erişim yetkisi olan iç sistemler ve hizmetler,
c) Uzaktan erişimi güvenli kılmak için yöntemleri de içeren uygun haberleşme teçhizatlarının kullanılmasına izin verilmesi,
d) Fiziksel güvenlik,
e) Teçhizatlara ve bilgiye, aile üyelerinin ve ziyaretçilerin erişimiyle ilgili kurallar ve kılavuz,
f) Donanım ve yazılım destek ve bakımının sağlanması,
g) Sigorta sağlanması,
h) Yedekleme ve iş sürekliliğiyle ilgili prosedürler,
i) Kayıt bilgisi ve güvenliğin izlenmesi,
j) Uzaktan çalışma işlemleri sona erdiğinde yetki ve erişim haklarının iptali ile donanımın geri iadesi.

Diğer bilgiler
Uzaktan çalışma, geleneksel olmayan çalışma ortamları da dâhil olmak üzere ofis dışında yapılan işin her türlüsünü ifade eder. Örneğin “evden çalışma”, “esnek işyeri”, “uzak çalışma” ve “sanal iş” ortamları.

7 İnsan kaynakları güvenliği

7.1 İstihdam öncesi

Amaç: Çalışanlar ve yüklenicilerin kendi sorumluluklarını anlamalarını ve düşünüldükleri roller için uygun olmalarını temin etmek.

7.1.1 Tarama

Kontrol
Tüm işe alım adayları için ilgili yasa, düzenleme ve etiğe göre ve iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak geçmiş doğrulama kontrolleri gerçekleştirilmelidir.

Uygulama kılavuzu
Doğrulama yapılırken tüm ilgili mahremiyet, kişi tespit bilgisinin korunması ve/veya istihdama yönelik mevzuat dikkate alınmalıdır. Ayrıca doğrulama, izin verilen durumlarda aşağıdakileri içermelidir:

a) Yeterli kişisel referansların varlığı; örneğin, bir adet işle ilgili, bir adet kişisel referans,
b) Başvuru sahibinin özgeçmişinin doğrulanması (tamlık ve kesinlik açısından),
c) Beyan edilen akademik ve işle ilgili niteliklerin onaylanması,
d) Bağımsız kimlik doğrulama (pasaport ve benzeri belge),
e) Sabıka kaydı incelemesi ya da kredi incelemesi gibi daha ayrıntılı doğrulama.

Bir birey, belirli bilgi güvenliği rolü için istihdam edileceği zaman kuruluşlar adayla ilgili olarak aşağıdaki hususlardan emin olmalıdır:

a) Güvenlik rolünü gerçekleştirmek için gerekli yeterliliğe sahip olması,

b) Özellikle kuruluş için rol kritik ise, rolü üstlenmesi için güvenilir olması.

İlk görüşme veya pozisyon yükselmesinde bir iş kişinin bilgi işleme tesislerine erişim sağlamasını gerektiriyorsa ve özellikle bu tesisler, finansal bilgiler veya yüksek seviyede gizli bilgiler işliyorsa kuruluş bu durumda daha detaylı doğrulamaları dikkate almalıdır.

Prosedürler, doğrulama gözden geçirmeleri için kıstasları ve sınırları belirlemelidir. Örneğin; kimler nasıl tarama yapar, doğrulama değerlendirmelerini nasıl, ne zaman ve neden yapar.

Bir tarama sürecinin de yükleniciler için yapılması sağlanmalıdır. Bu durumlarda, kuruluş ve yüklenici arasındaki anlaşmada tarama yürütmek ve tarama tamamlanamadığında ya da sonuçları şüphe veya endişe verdiğinde izlenmesi gereken bildirim prosedürleri için sorumluluklar belirlenmelidir.

Kuruluş ile ilgili iş pozisyonu için tüm adaylar hakkında bilgi toplanması ilgili yargı çevresi uyarınca mevcut tüm yasalara uygun olmalı ve bu bilgiler işlenmelidir. Uygulanabilir yasalara bağlı olarak, adaylar tarama faaliyetleri hakkında önceden bilgilendirilmelidir.

7.1.2 İstihdam hüküm ve koşulları

Kontrol
Çalışanlar ve yükleniciler ile yapılan sözleşmeler de kendilerinin ve kuruluşun bilgi güvenliği sorumlulukları belirtmelidir.

Uygulama kılavuzu
Çalışanlar veya yüklenicilerin sözleşmeden doğan yükümlülükleri, aşağıdaki hususların açıklanması ve belirtilmesine ek olarak bilgi güvenliği için kuruluşun politikalarını yansıtmalıdır;

a) Gizli bilgilere erişim hakkı olan tüm çalışanlarına ve yüklenicilerine bilgi işleme tesislerine erişim yetkisi verilmeden önce bir gizlilik ya da ifşa etmeme anlaşması imzalattırılması (bk. Madde 13.2.4),
b) Çalışanların ya da yüklenicilerin yasal sorumlulukları ve hakları; örneğin, telif hakkı yasaları veya veri koruma yasaları (bk. Madde 18.1.2 ve Madde 18.1.4),
c) Çalışan ya da yüklenici tarafından yürütülen hizmetler ve bilgi işleme tesisleri ve bilgi ile ilişkili kuruluş varlıklarının yönetimi ve bilgi sınıflandırması için sorumluluklar (bk. Madde 8),
d) Diğer kuruluşlar ve dış taraflardan alınan bilgilerin işlenmesi için çalışanların ya da yüklenicilerin sorumlulukları,
e) Çalışanlar ya da yükleniciler kuruluşun güvenlik gereksinimlerini dikkate almadığında yürütülecek işlemler (bk. Madde 7.2.3).

Bilgi güvenliği rolleri ve sorumlulukları istihdam öncesi proseste iş adaylarına duyurulmalıdır.

Kuruluş, çalışanların ve yüklenicilerin bilgi sistemleri ve hizmetleri ile ilişkili kuruluşun varlıklarına erişim niteliğine ve kapsamına uygun bilgi güvenliği koşullarını kabul ettiğini garanti etmelidir.

Uygun olan durumlarda, istihdam koşulları ile sorumlulukları istihdam bitiminden sonra tanımlanmış belirli bir zamana kadar devam etmelidir (bk. Madde 7.3).

Diğer bilgiler
Çalışanların ya da yüklenicilerin gizlilik, veri koruma, iş ahlakı, kuruluşun teçhizat veya tesislerinin uygun kullanımı ve kuruluş tarafından beklenen bilindik uygulamalarla ilgili bilgi güvenliği sorumluluklarının ifade edilmesi için bir uygulama esasları kullanılabilir. Yüklenici ile ilişkili bir dış tarafın, sözleşmeli birey adına sözleşme yapması gerekebilir.

7.2 Çalışma esnasında

Amaç: Çalışanların ve yüklenicilerin bilgi güvenliği sorumluluklarının farkında olmalarını ve yerine getirmelerini temin etmek.

7.2.1 Yönetim sorumlulukları

Kontrol
Yönetim, çalışanlar ve yüklenicilerin, kuruluşun yerleşik politika ve prosedürlerine göre bilgi güvenliğini uygulamalarını istemelidir.

Uygulama kılavuzu
Yönetim sorumlulukları çalışanlar ve yükleniciler için aşağıdakilerin temin edilmesini içermelidir:

a) Bilgi sistemlerine veya gizli bilgilere erişim hakkı verilmeden önce, kendi güvenlik rolleri ve sorumlulukları hakkında doğru bilgilendirilmesi,
b) Kuruluş bünyesindeki rolleri ifade eden bilgi güvenliği beklentilerinin kılavuzlar ile sağlanması,
c) Kuruluşun bilgi güvenliği politikalarını yerine getirmek için motivasyon sağlanması,
d) Kuruluş içindeki görev ve sorumluluklara uygun olarak bilgi güvenliği üzerinde bir farkındalık seviyesine ulaşılması (bk. Madde 7.2.2),
e) Kuruluşun bilgi güvenliği politikası ve uygun çalışma yöntemlerini içeren istihdam koşullarına uyulması,
f) Uygun beceri ve niteliklerin sağlanmasında sürekliliğin temin edilmesi ve düzenli olarak eğitim verilmesi,
g) Bilgi güvenliği politika ve prosedürleri ihlallerinin raporlanmasının anonim bir raporlama kanalı ile sağlanması (“usulsüzlüklerin duyurulması”).

Yönetim, örnek teşkil edecek şekilde bilgi güvenliği politikalarını, prosedürlerini ve kontrollerini desteklediğini göstermelidir.

Diğer bilgiler
Çalışanların ve yüklenicilerin bilgi güvenliği sorumlulukları hakkında bilgilendirilmemesi kuruluş için büyük hasara neden olabilir. Motivasyonu yüksek olan personelin daha güvenilir olması ve daha az bilgi güvenliği ihlal olaylarına neden olması muhtemeldir.

Kötü yönetim personelin kendisini değersiz hissetmesine ve bunun sonucunda kuruluş için olumsuz bir bilgi güvenliği etkisine neden olabilir. Örneğin; kötü yönetim bilgi güvenliğinin ihmal edilmesine veya kuruluşun varlıklarının potansiyel suiistimale maruz kalmasına neden olabilir.

7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi

Kontrol
Kuruluştaki tüm çalışanlar ve ilgili olan yerlerde, yükleniciler, kendi iş fonksiyonları ile ilgili olduğunda, kurumsal politika ve prosedürlerle ilgili uygun farkındalık eğitim ve öğretimini ve düzenli güncellemeleri almalıdırlar.

Uygulama kılavuzu
Bilgi güvenliği farkındalık programı, çalışanların ve ilgili olduklarında yüklenicilerin bilgi güvenliği sorumlulukları ve bu sorumlulukları yerine getirme yöntemlerinin farkında olmalarını hedefler.

Bir bilgi güvenliği farkındalık programı, kuruluşun korunacak bilgilerini korumak için uygulanmakta olan kontrolleri dikkate alarak, kuruluşun bilgi güvenliği politikaları ve ilgili prosedürleri doğrultusunda oluşturulmalıdır. Farkındalık programı, kampanyalar (örneğin; bir “bilgi güvenliği günü”) ve mektuplar veya el kitapları gibi farkındalığı arttırıcı birkaç faaliyeti kapsamalıdır.

Bilgi güvenliği programı, kuruluşta çalışanların rollerini ve uygun olduğu durumda kuruluşun yüklenicilerden beklediği farkındalığı dikkate alarak planlanmalıdır. Farkındalık programı faaliyetleri zaman içerisinde tercihen düzenli şekilde planlanmalıdır, böylece faaliyetler tekrarlanır ve yeni çalışanlar ve yükleniciler kapsanır. Farkındalık programı düzenli olarak güncellenmelidir. Böylece, kurumsal politika ve prosedürler uygun bir çizgide devam eder. Farkındalık programı bilgi güvenliği ihlal olaylarından öğrenim üzerine inşa edilmelidir.

Farkındalık eğitimi, kuruluşun bilgi güvenliği farkındalık programının gereklerine göre yapılmalıdır. Farkındalık eğitimi, sınıf tabanlı, uzaktan eğitimi, web tabanlı, kendi kendine ve diğer yöntemler de dâhil olmak üzere farklı dağıtım ortamlarını kullanabilir.

Bilgi güvenliği eğitim ve öğretimi aynı zamanda aşağıdaki gibi genel hususları kapsar:

a) Kuruluş genelinde yönetimin bilgi güvenliğine bağlılığının belirtilmesi,
b) Politikalar, standardlar, yasalar, düzenlemeler, sözleşme ve anlaşmalarda tanımlanan uygulanabilir bilgi güvenliği kuralları ve yükümlükleri ile uyumlu olması ve uyum ile ilgili bilgi sahibi olma,
c) Kişinin kendi eylemlerinden ve eylemsizliklerinden hesap verebilirliği ve kuruluş ve dış taraflara ait bilgi güvenliğini ya da korumasına yönelik genel sorumlulukları,
d) Temel bilgi güvenliği prosedürleri (bilgi güvenliği ihlal olaylarının raporlanması gibi) ve asgari seviye kontroller (parola güvenliği, kötücül yazılım kontrolü ve temiz masalar gibi),
e) Daha fazla bilgi güvenliği içeren eğitim ve öğretim materyalleri de dâhil olmak üzere bilgi güvenliği konularında daha fazla bilgi ve tavsiye için iletişim noktalarına ve kaynaklara başvurma.

Bilgi güvenliği eğitim ve öğretimi periyodik olarak gerçekleştirilmelidir. İlk eğitim ve öğretim, sadece yeni başlayanlara değil, yeni pozisyonlarda ya da önemli ölçüde farklı bilgi güvenliği gereksinimleri olan rollerde görev alanlara rolü etkin olmadan önce verilmelidir.

Kuruluş, eğitim ve öğretimi etkin şekilde yürütmek için eğitim ve öğretim programı geliştirmelidir. Program, kuruluşun korunan bilgisi ve bilginin korunması için uygulanan kontroller göz önünde bulundurularak kuruluşun bilgi güvenliği politikası ve ilgili prosedürleri ile aynı doğrultuda olmalıdır. Program, eğitim ve öğretimin farklı şekillerini göz önünde bulundurulmalıdır. Örneğin; dersler ve bireysel çalışmalar.

Diğer bilgiler
Bir farkındalık programı oluşturulurken, sadece ‘ne’ ve ‘nasıl’a değil aynı zamanda ‘neden’e odaklanmak önemlidir. Çalışanların, bilgi güvenliği amacını ve kendi davranışlarının kuruluşa olumlu ve olumsuz potansiyel etkilerini anlaması önemlidir.

Farkındalık, eğitim ve öğretim diğer eğitim faaliyetlerinin bir parçası olabilir ya da bunlarla birlikte yürütülebilir. Örneğin; genel BT ya da genel güvenlik eğitimi. Farkındalık, eğitim ve öğretim faaliyetleri bireylerin rolleri, sorumlulukları ve becerileri ile ilgili ve uygun olmalıdır.

Çalışanların kavraması bir farkındalık, eğitim ve öğretim kursu sonunda bilgi birikiminin aktarımının test edilmesi ile değerlendirilebilir.

7.2.3 Disiplin prosesi

Kontrol
Bir bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi ve bildirilmiş bir disiplin prosesi olmalıdır.

Uygulama kılavuzu
Disiplin prosesi, bir bilgi güvenliği ihlalinin gerçekleştiğinin doğrulanmasından önce devreye girmemelidir (bk. Madde 16.1.7).

Resmi disiplin prosesi, bilgi güvenliği ihlalleri işlediği şüphesi olan çalışanlar için doğru ve adil davranışı sağlamalıdır. Resmi disiplin prosesinin; ihlalin niteliği ve büyüklüğü ile bunların işe etkisini, bu ihlalin ilk veya tekrarlanan bir suç olup olmadığını, ihlali yapan çalışanın düzgün eğitilmiş olup olmadığını, ilgili yasaları, iş sözleşmelerini ve gerektiğinde diğer faktörleri dikkate alan dereceli bir tepkiyi sağlaması gerekir.

Disiplin prosesi, kuruluşun bilgi güvenliği politikaları ve prosedürlerinin ihlal edilmesi ve diğer bilgi güvenliği ihlallerini önlemek için caydırıcı olarak kullanılmalıdır. Kasıtlı ihlallerde acil eylemler gerekebilir.

Diğer bilgiler
Disiplin prosesinde, bilgi güvenliği açısından dikkat çekici davranışlar için olumlu yaptırımlar tanımlanırsa bir motivasyon ya da teşvik haline gelebilir.

7.3 İstihdamın sonlandırılması veya değiştirilmesi

Amaç: İstihdamın sonlandırılması veya değiştirilmesi prosesinin bir parçası olarak kuruluşun çıkarlarını korumak.

7.3.1 İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi

Kontrol
İstihdamın sonlandırılması veya değiştirilmesinden sonra geçerli olan bilgi güvenliği sorumlulukları ve görevleri tanımlanmalı, çalışan veya yükleniciye bildirilmeli ve yürürlüğe konulmalıdır.

Uygulama kılavuzu
Sorumlulukların sonlandırılmasının duyurulması; devam eden bilgi güvenliği gereksinimleri ve yasal sorumluluklar ve uygun olduğu durumlarda, tüm gizlilik anlaşmalarında (bk. Madde 13.2.4) belirtilen sorumlulukları ve çalışanların ya da yüklenicilerin istihdam bitiminden sonra belirli bir süre devam eden istihdam şartlarını (bk. Madde 7.1.2) içermelidir.

Çalışan ve yüklenici sözleşmelerinde istihdamın sona ermesinden sonra da geçerli olan çalışan veya yüklenicinin istihdam hüküm ve koşulları yer almalıdır (bk. Madde 7.1.2).

Sorumluluk veya istihdam değişiklikleri, mevcut sorumluluğun sona erdirilmesi veya yeni sorumluluk ve istihdam başlaması ile birlikte işe dâhil edilmesi yönetilmelidir.

Diğer bilgiler
Genel sonlandırma prosesinden genellikle insan kaynakları fonksiyonu sorumludur ve kişi ayrılırken ilgili prosedürlerin bilgi güvenliği yönlerinin yönetilmesinde ayrılan kişinin yöneticisi ile birlikte çalışır. Dış taraf aracılığıyla sağlanan bir yüklenici olması durumunda, fesih işlemi kuruluş ile dış taraf arasındaki sözleşmeye uygun olarak dış tarafça yapılır.

Personel ve işletim düzenlemelerindeki değişikliklerin; çalışanlara, müşterilere ya da yüklenicilere bildirilmesi gerekli olabilir.

8 Varlık yönetimi

8.1 Varlıkların sorumluluğu

Amaç: Kuruluşun varlıklarını tespit etmek ve uygun koruma sorumluluklarını tanımlamak.

8.1.1 Varlık envanteri

Kontrol
Bilgi ve bilgi işleme tesisleri ile ilgili varlıklar belirlenmeli ve bu varlıkların bir envanteri çıkarılmalı ve idame ettirilmelidir.
Uygulama kılavuzu
Bir kuruluş, bilgi yaşam döngüsünde ilgili varlıkları belirlemeli ve önemini yazılı hale getirmelidir. Bilgi yaşam döngüsü oluşturma, işleme, depolama, iletme, silme ve imhayı içermelidir. Dokümantasyon mevcut envanterlere uygun olarak veya özel olarak muhafaza edilmelidir.

Varlık envanteri; güncel, tutarlı, doğru ve diğer envanterler ile uyumlu olmalıdır.

Belirlenen her bir varlık için varlık mülkiyeti tahsis edilmeli (bk. Madde 8.1.2) ve sınıfı belirlenmelidir (bk. Madde 8.2).

Diğer bilgiler
Varlık envanteri etkin korumayı sağlamak için yardımcı olur ve aynı zamanda sağlık ve emniyet, sigorta veya finansal (varlık yönetimi) sebepler gibi diğer amaçlar için gerekli olabilir.

ISO/IEC 27005[11] standardı varlıkları belirlerken kuruluş tarafından dikkate alınması gerebilecek varlıkların örneklerini sağlar. Varlık envanterini derleme süreci risk yönetimi için önemli önkoşuldur (bk. ISO/IEC 27000 ve ISO/IEC 27005[11]).

8.1.2 Varlıkların sahipliği

Kontrol
Envanterde tutulan tüm varlıklara sahip atamaları yapılmalıdır.

Uygulama kılavuzu
Varlık yaşam döngüsü için onaylanmış yönetim sorumluluğuna sahip bireyler ve diğer oluşumlar, varlık sahipleri olarak atanmaya hak kazanırlar.

Varlık sahipliğinin zamanında belirlenmesini sağlamak için bir proses genellikle kullanılmaktadır. Varlıklar oluşturulduğunda ya da varlıklar kuruluşa transfer edildiğinde sahipliği belirlenmelidir. Varlık sahibi, varlık yaşam döngüsü boyunca varlığın uygun yönetiminden sorumlu olmalıdır.

Varlık sahibi:

a) Varlık envanterinin kaydedildiğinden emin olmalıdır,
b) Varlıkların uygun sınıflandırıldığından ve korunduğundan emin olmalıdır,
c) Uygulanabilir erişim kontrol politikasını dikkate alarak önemli varlıklara erişim kısıtlamalarını ve sınıflandırmasını tanımlamalı ve periyodik olarak gözden geçirmelidir,
d) Varlıkların silinmesi ya da imha edilmesinde uygun işlemin uygulandığından emin olmalıdır.

Diğer bilgiler
Bir varlığın yaşam döngüsü boyunca kontrol edilmesi için yönetim sorumluluğu onayına sahip bir birey ya da oluşum olabilir. Tanımlanan sahibin varlık üzerinde herhangi bir mülkiyet hakkı yoktur.

Rutin görevler devredilebilir; (örneğin, bir varlığa günlük olarak bakan emanetçi gibi) fakat sorumluluk varlık sahibindedir.

Karmaşık bilgi sistemleri içinde varlık gruplarını belirlemek işlevlerin birlikte sağlanmasında faydalı olabilir. Bu durumda bu hizmet sahibi, varlıkların işleyişi de dâhil hizmetin sunumundan sorumludur.

8.1.3 Varlıkların kabul edilebilir kullanımı

Kontrol
Bilgi ve bilgi işleme tesisleri ile ilgili bilgi ve varlıkların kabul edilebilir kullanımına dair kurallar belirlenmeli, yazılı hale getirilmeli ve uygulanmalıdır.

Uygulama kılavuzu
Kuruluşun varlıklarını kullanan veya bunlara erişimi olan çalışanlar ve dış taraf kullanıcılar, bilgi ve bilgi işleme tesisleri ve kaynakları ile ilişkili kuruluşun varlıklarının bilgi güvenliği gereksinimleri hakkında farkındalıkları sağlanmalıdır. Bu kullanıcılar tüm bilgi işleme kaynaklarının kullanımından ve kendi sorumlulukları altında gerçekleşen tüm kullanımlardan sorumlu olmalıdır.

8.1.4 Varlıkların iadesi

Kontrol
Tüm çalışanlar ve dış tarafların kullanıcıları, istihdamlarının, sözleşme veya anlaşmalarının sonlandırılmasının ardından ellerinde olan tüm kurumsal varlıkları iade etmelidirler.

Uygulama kılavuzu
Sonlandırma süreci, önceden verilen tüm fiziksel ve elektronik varlıkların sahipliğinin ya da kuruluşa ait emanetlerin iadesini içerecek şekilde formüle edilmelidir.

Çalışan veya dış taraf kullanıcısı, kuruluşun ekipmanını satın aldığında veya kendi kişisel ekipmanını kullandığında tüm ilgili bilgilerin kuruluşa transfer edildiğinden ve güvenli bir şekilde ekipmandan silindiğinden emin olmak amacıyla prosedürler izlenir (bk. Madde 11.2.7).

Çalışan veya dış taraf kullanıcısının devam eden operasyonlar için önemli bilgilere sahip olduğu durumlarda, bu bilgilerin yazılı hale getirilmesi ve kuruluşa transfer edilmesi gereklidir.

Fesih bildirim süresi boyunca, kuruluş; işi fesih edilen çalışanların ve yüklenicilerin fikri mülkiyet gibi ilgili bilgilerin yetkisiz kopyalamasını kontrol etmelidir.

8.2 Bilgi sınıflandırma

Amaç: Bilginin kurum için önemi derecesinde uygun seviyede korunmasını temin etmek.

8.2.1 Bilgilerin sınıflandırması

Kontrol
Bilgi yasal gereksinimler, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre sınıflandırılmalıdır.

Uygulama kılavuzu
Bilgi için sınıflandırma ve ilgili koruma kontrollerinin de, bilgi paylaşımı ya da kısıtlaması için yasal gereklerin yanı sıra iş ihtiyaçları dikkate alınmalıdır. Bilginin saklandığı, işlendiği ya da başka türlü ele alındığı ya da korunduğu bilgi dışındaki varlıklar da bilgi sınıflandırması ile uyumlu olarak sınıflandırılabilir.

Bilgi varlıklarının sahipleri, yaptıkları sınıflandırmadan sorumlu olmalıdır.

Sınıflandırma, sınıflandırma ve sınıflandırmanın zaman içerisinde gözden geçirilmesi kriterleri için teamülleri içermelidir. Sınıflandırmadaki koruma düzeyi gizlilik, bütünlük ve erişilebilirlik ve ele alınan tüm gereksinimler analiz edilerek değerlendirilmelidir. Sınıflandırma, erişim kontrol politikası (bk. Madde 9.1.1) ile uyumlaştırılmalıdır.

Her sınıflandırma seviyesi, sınıflandırma uygulaması bağlamında mantıklı bir isme sahip olmalıdır.

Sınıflandırma, herkesin bilgi ve ilgili varlıkları aynı şekilde sınıflandırmaları, koruma gereksinimleri hususunda ortak bir anlayışa sahip olmaları ve uygun koruma uygulamaları için tüm kuruluş genelinde tutarlı olmalıdır.

Sınıflandırma, kuruluşun proseslerine dâhil edilmelidir ve kuruluş çapında tutarlı ve uyumlu olmalıdır. Sınıflandırma sonuçları, kuruluşun kendi hassasiyetine ve kritikliğine bağlı olarak varlıkların değerini belirtmelidir. Örneğin; gizlilik, bütünlük ve erişilebilirlik açısından. Sınıflandırma sonuçları, yaşam döngüsü yoluyla hassasiyete ve kritikliğe göre varlıkların değerindeki değişiklik ile uyumlu olarak güncellenmelidir.

Diğer bilgiler
Sınıflandırma, bilgi ile uğraşan kişilere onu nasıl ele alacağı ve koruyacaklarına ilişkin net bir belirtim sağlar. Benzer koruma ihtiyaçları olan bilgi grupları oluşturularak ve her gruptaki tüm bilgiler için geçerli bilgi güvenliği prosedürleri uygulanarak bu kolaylaştırılır. Bu yaklaşım, her bir durum için risk değerlendirmesi ve kontrollerin özellikle tasarlanması ihtiyacını azaltır.

Bilgi, belli bir süre sonra hassas ya da kritik olmaktan çıkabilir. Örneğin; bilgi kamuya açıklandığında. Bu hususlar dikkate alınmalıdır. Şöyle ki; yüksek sınıflandırma ek masraflarla sonuçlanan gereksiz kontrollerin uygulanmasına yol açabilir ya da tam tersine düşük sınıflandırma, iş amaçlarının başarılmasını tehlikeye atabilir.

Örneğin; bilgi gizliliği sınıflandırması aşağıdaki dört seviyeyi temel alabilir:

a) İfşa edilmesi durumunda hiç bir zarar olmaz,
b) İfşa edilmesi durumunda küçük bir mahcubiyete ya da küçük bir sıkıntıya neden olur,
c) İfşa edilmesi durumunda işlemler ya da taktik amaçlar üzerinde kısa vadeli etkiye neden olur,
d) İfşa edilmesi stratejik hedefler üzerinde uzun vadeli etkiye neden olur ya da kuruluşun hayatiyetini risk altına sokar.

8.2.2 Bilgi etiketleme

Kontrol
Bilgi etiketleme için uygun bir prosedür kümesi kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.

"Uygulama kılavuzu"
Bilgi etiketleme için prosedürlerin, fiziksel ve elektronik formattaki bilgiyi ve ilgili varlıkları kapsaması gerekir. Etiketleme Madde 8.2.1'e göre kurulan sınıflandırmayı yansıtmalıdır. Etiketler kolayca fark edilebilmelidir. Prosedürler, ortam türlerine bağlı olarak varlıkların ele alınışı ya da bilgiye nasıl erişileceği, etiketlerin nerede ve nasıl ekleneceği hususlarında kılavuzluk sağlamalıdır. Prosedürlerde etiketlemenin yapılmadığı durumları tanımlayabilirsiniz. Örneğin; iş yükünü azaltmak için gizli olmayan bilgilerin etiketlenmesi. Çalışanlar ve yükleniciler etiketleme prosedürünü bilmelidir.

Hassas veya kritik bilgiler olarak sınıflandırılmış bilgileri içeren sistemlerin çıktıları uygun sınıflandırma etiketi bulunmalıdır.

Diğer bilgiler
Sınıflandırılmış bilgilerin etiketlenmesi bilgi paylaşımı anlaşmaları için önemli bir gerekliliktir. Bilgi ve bilgi ile ilgili varlıkların etiketlenmesi bazen olumsuz etkiye neden olabilir. Dış veya iç saldırganların sınıflandırılmış varlıkları tespit etmesi ve buna göre çalması daha kolaydır.

8.2.3 Varlıkların kullanımı

Kontrol
Varlıkların kullanımı ile ilgili prosedürler, kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.

Uygulama kılavuzu
Prosedürler, sınıflandırma ile tutarlı kullanım, işleme, depolama ve iletişim bilgisi için güncellenmelidir (bk. Madde 8.2.1).

Aşağıdaki adımlara dikkat edilmelidir:

a) Her bilgi sınıflandırma düzeyi için koruma gereklerini destekleyen erişim kısıtlaması,
b) Varlıkların yetkilendirilmiş alıcılarına ait resmi kaydın devam ettirilmesi,
c) Asıl bilgilerin korunması ile tutarlı bir düzeyde geçici ya da kalıcı bilgi kopyaların korunması,
d) Üreticinin belirttiği özellikler doğrultusunda BT varlıklarının depolanması,
e) Yetkili alıcının dikkatini çekmek için ortamın tüm kopyalarının net bir şekilde işaretlenmesi.

Kuruluşta kullanılan sınıflandırma düzeni, düzey isimleri benzer olsa bile diğer kuruluşlar tarafından kullanılan düzenlerle eşdeğer olmayabilir. Ek olarak, kuruluşlar arasında taşınan bilgilerin sınıflandırma düzenleri aynı olsa bile her kuruluşun kendi içerisinde sınıflandırması farklı olabilir.

Bilgi paylaşımı dâhil diğer kuruluşlar ile yapılan anlaşmalar bilgilerin sınıflandırma tanımlanması prosedürlerini ve diğer kuruluşlardan gelen sınıflandırma etiketlerinin yorumlanmasını içermelidir.

8.3 Ortam işleme

Amaç: Ortamda depolanan bilginin yetkisiz ifşasını, değiştirilmesini, kaldırılmasını ve yok edilmesini engellemek.

8.3.1 Taşınabilir ortam yönetimi

Kontrol
Taşınabilir ortam yönetimi için prosedürler, kuruluş tarafından benimsenen sınıflandırma düzenine göre uygulanmalıdır.

Uygulama kılavuzu

Taşınabilir ortam yönetimi için aşağıdaki hususlar dikkate alınmalıdır:

a) Artık gerekmiyorsa, kuruluştan kaldırılacak herhangi bir tekrar kullanılabilir ortamın içeriği geri kazanılamaz hale getirmelidir,
b) Gerektiğinde ve pratik ise, kuruluşta taşınabilir ortamın kaldırılması için yetkilendirme gereklidir ve bu tür kaldırma işlemlerinin bir kayıt izleme logu kanıt sağlamak amacıyla saklanmalıdır,
c) Tüm ortamlar, üretici özelliklerine uyumlu olarak güvende ve güvenli ortamda saklanmalıdır,
d) Veri gizliliği veya bütünlüğü önemli mülahazalar ise taşınabilir ortamlardaki verinin korunması için kriptografik teknikler kullanılmalıdır,
e) Depolanan veriye hala ihtiyaç duyuluyorsa medya riskini azaltmak için veri erişilemez olmadan önce yeni ortama transfer edilmelidir,
f) Değerli verilerin birden fazla kopyası, veri hasarı ya da veri kaybı riskini azaltmak için ayrı bir ortamda saklanmalıdır,
g) Taşınabilir ortamın kaydedilmesi veri kaybı olasılığını sınırlandırmak amacıyla dikkate alınmalıdır,
h) Taşınabilir ortam sürücüleri sadece kullanmak için bir iş nedeni olduğunda etkinleştirilmelidir,
i) Bilgi transferi için silinebilir ortam kullanımı gerektiğinde ortam izlenmelidir.

Prosedürler ve yetkilendirme seviyeleri yazılı hale getirilmelidir.

8.3.2 Ortamın yok edilmesi

Kontrol
Ortam, artık ihtiyaç kalmadığında resmi prosedürler kullanılarak güvenli bir şekilde yok edilmelidir.

Uygulama kılavuzu
Ortamın güvenli yok edilmesi için resmi prosedürler gizli bilgilerin yetkisiz kişilere sızma riskinin en aza indirmek için gereklidir. Gizli bilgileri içeren ortamın güvenli yok edilmesi için prosedürler, bilgilerin hassasiyeti ile orantılı olmalıdır. Aşağıdaki hususlar dikkate alınmalıdır:

a) Hassas bilgileri içeren ortam güvenli bir şekilde saklanmalı ve yok edilmelidir; örneğin, yakma veya parçalama ya da kuruluşun başka bir uygulamasında kullanmak için verilerin silinmesi,
b) Güvenli yok etme gerektirebilir öğelere yönelik prosedürler olmalıdır,
c) Tüm ortam öğelerinin toplanması ve güvenli bir şekilde yok edilmesinin ayarlanması, hassas öğelerin ayrılmasına çalışmaktan daha kolay olabilir,
d) Birçok kuruluş ortamlar için toplama ve imha hizmetleri sunar, doğru kontroller ve tecrübeye sahip bir dış taraf seçimine özen gösterilmelidir,
e) Bir denetim kaydı tutmak için hassas öğelerin yok edilmesi kayıt altına alınmalıdır.

Yok edilmesi için ortam biriktirilirken, toplamanın çok sayıda hassas olmayan bilginin hassas hale gelmesine yol açan kümelenme etkisi dikkate alınmalıdır.

Diğer bilgiler
Hassas veriler içeren hasar görmüş cihazlar, bu cihazların içindeki öğelerin tamire gönderileceği veya göz ardı edileceğinin mi ya da fiziksel olarak yok edileceğinin mi belirlenmesi amacıyla bir risk değerlendirmesi gerekebilir (bk. Madde 11.2.7).

8.3.3 Fiziksel ortam aktarımı

Kontrol
Bilgi içeren ortam, aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunmalıdır.

Uygulama kılavuzu
Taşınan bilgileri içeren ortamları korumak için aşağıdaki hususlara dikkat edilmelidir:

a) Güvenilir taşımacılık ya da kuryeler kullanılmalıdır,
b) Yetkili kurye listesi yönetim tarafından kabul edilmelidir,
c) Kuryelerin kimliklerini doğrulamak için prosedürler geliştirilmelidir,
d) Paketleme, taşıma sırasında ortaya çıkabilecek herhangi bir fiziksel hasardan korumak için yeterli ve üreticinin belirlediği teknik özelliklere uygun olmalıdır. Örneğin; ısı, nem ya da elektromanyetik alanlara maruz kalma gibi ortamın yenileme etkisini azaltacak herhangi bir çevresel faktörlere karşı koruma.

e) Ortamın içeriğini tanımlayan kayıtlar ile birlikte kaç kez transfer edildiğinin, transfer sorumlularının ve alıcı tarafından alındığının kayıtları tutulmalıdır.

Diğer bilgiler
Ortamın posta hizmeti yoluyla ya da kurye ile gönderilmesi durumunda bilgi yetkisiz erişime, yanlış kullanıma ya da fiziksel taşıma sırasında hasara maruz kalabilir. Bu kontrolde, ortam kâğıt belgeleri içerir.

Ortamdaki gizli bilgi şifreli değilse, ortam için ek fiziksel koruma düşünülmelidir.

9 Erişim kontrolü

9.1 Erişim kontrolünün iş gereklilikleri

Amaç: Bilgi ve bilgi işleme tesislerine erişimi kısıtlamak.

9.1.1 Erişim kontrol politikası

Kontrol
Bir erişim kontrol politikası, iş ve bilgi güvenliği şartları temelinde oluşturulmalı, yazılı hale getirilmeli ve gözden geçirilmelidir.

Uygulama kılavuzu
Varlık sahipleri, ayrıntı miktarı ile kendi varlıklarına yönelik özel kullanıcı rolleri için ve ilişkili bilgi güvenliği risklerini yansıtan kontrolleri, erişim kontrol kurallarını, erişim haklarını ve kısıtlamaları ve sıkılığını belirlemelidir.

Erişim kontrolleri hem mantıksal hem de fizikseldir (bk. Madde 11) ve her ikisi birlikte dikkate alınmalıdır. Kullanıcılara ve hizmet sağlayıcılara, erişim kontrolleri aracılığı ile karşılanacak iş gereksinimleri hakkında bildirimler verilmelidir.

Politika aşağıdaki hususları dikkate almalıdır:

a) İş uygulamaları ile ilgili güvenlik gereksinimleri,
b) Bilgi sızıntısı ve yetkilendirme için politikalar; örneğin, ilke ve güvenlik seviyelerini ve bilgi sınıflandırmasını bilme gereksinimi (bk. Madde 8.2),
c) Sistemler ve ağlara erişim hakları ile bilgi sınıflandırılması arasındaki tutarlılık,
d) Verilere veya hizmetlere erişimin sınırlandırılmasına dair ilgili yasalar ve sözleşme yükümlülükleri (bk. Madde 18.1),
e) Dağıtılmış ve ağ oluşturulmuş çevre içindeki tüm olası bağlantı hakları için erişim haklarının yönetimi,
f) Erişim kontrol rollerinin ayrılması; örneğin, erişim talebi, erişim yetkilendirmesi, erişim yöneticisi,
g) Erişim taleplerinin resmi yetkilendirilmesi için gereksinimler (bk. Madde 9.2.1 ve Madde 9.2.2),
h) Erişim haklarının periyodik gözden geçirilmesi için gereksinimler (bk. Madde 9.2.5),
i) Erişim haklarının kaldırılması (bk. Madde 9.2.6),
j) Kullanıcı kimlik bilgileri ve gizli kimlik doğrulama bilgileri kullanımı ve yönetimi ile ilgili tüm önemli olayların kayıtlarının saklanması,
k) Ayrıcalıklı erişim rolleri (bk. Madde 9.2.3).

Diğer bilgiler
Erişim kontrol kuralları tanımlanırken aşağıdaki hususlar göz önünde bulundurulmalıdır:

a) Daha zayıf kural olan “açıkça yasaklanmadıkça her şeye izin verilir” kuralının aksine “açıkça izin verilmedikçe her şey yasaklanır” kuralı tabanlı kurallar kurmak,
b) Bilgi etiketlerinde (bk. Madde 8.2.2), bilgi işleme tesisleri tarafından otomatik olarak başlatılan ve bir kullanıcının takdiriyle başlatılan değişiklikler,
c) Bilgi sistemi tarafından otomatik olarak başlatılan ve bir sistem yöneticisi tarafından başlatılan kullanıcı yetkilerindeki değişiklikler,
d) Yürürlüğe girmeden özel onaya gerek duyan ve duymayan kurallar.

Erişim kontrol kuralları, resmi prosedürler (bk. Madde 9.2, Madde 9.3 ve Madde 9.4) ve tanımlanan sorumluluklar (bk. Madde 6.1.1, Madde 9.3) tarafından desteklenmelidir.

İş rolleri ile erişim haklarını bağlamak için rol tabanlı erişim kontrolü birçok kuruluş tarafından başarılı bir şekilde kullanılmaktadır.

Erişim kontrol politikalarını yönlendiren yaygın ilkelerden ikisi şunlardır:

a) Bilmesi gereken: sadece size, görevlerinizi gerçekleştirmek için gereken bilgilere erişim verilir. (farklı görevler/roller, farklı bilmesi gereken ve farklı erişim profili demektir.)
b) Kullanması gereken: sadece size, görevlerinizi/işinizi/rolünüzü gerçekleştirmek için gereken bilgi işleme tesislerine (BT ekipmanları, uygulamalar, prosedürler, odalar) erişim verilir.

9.1.2 Ağlara ve ağ hizmetlerine erişim

Kontrol
Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir.

Uygulama kılavuzu
Ağ ve ağ hizmetlerinin kullanımı ile ilgili bir politika oluşturulmalıdır. Bu politika aşağıdaki hususları kapsamalıdır:

a) Erişimine izin verilen ağ ve ağ hizmetleri,
b) Ağ ve ağ hizmetlerine kimlerin erişeceğini belirlemek için yetkilendirme prosedürleri,
c) Ağ bağlantılarına ve ağ hizmetlerine erişimi korumak için yönetim kontrolleri ve prosedürleri,
d) Ağ ve ağ hizmetlerine erişim için kullanılan yöntemler (örneğin; kablosuz ağlar ya da VPN kullanımı),
e) Çeşitli ağ hizmetlerine erişim için kullanıcı kimlik doğrulama gereksinimleri,
f) Ağ hizmetleri kullanımının izlenmesi.

Ağ hizmetleri kullanımı ile ilgili politika kuruluşun erişim kontrol politikası ile tutarlı olmalıdır (bk. Madde 9.1.1).

Diğer bilgiler
Ağ hizmetlerine yetkisiz ve güvensiz bağlantılar tüm kuruluşu etkileyebilir. Bu kontrol, hassas ya da kritik iş uygulamaları veya yüksek riskli yerlerdeki kullanıcılar (örneğin; kuruluşun bilgi güvenliği yönetimi ve kontrolü dışında kalan halka açık alanlarda ya da dış alanlarda) için özellikle önemlidir.

9.2 Kullanıcı erişim yönetimi

Amaç: Yetkili kullanıcı erişimini temin etmek ve sistem ve hizmetlere yetkisiz erişimi engellemek.

9.2.1 Kullanıcı kaydetme ve kayıt silme

Kontrol
Erişim haklarının atanmasını sağlamak için, resmi bir kullanıcı kaydetme ve kayıt silme prosesi uygulanmalıdır.

Uygulama kılavuzu
Kullanıcı kimlik bilgisi yönetimi için proses aşağıdaki hususları içermelidir:

a) Kullanıcıların kendi işlemleri ile bağlantılı ve bu işlemlerden sorumlu olacakları tek ve benzersiz kullanıcı kimliklerin kullanımı; paylaşılan kimliklerin kullanımına sadece iş ve işletimsel nedenler için gerekli olduğundan izin verilmelidir; Ayrıca onaylanmalı ve yazılı hale getirilmelidir,
b) Kuruluştan ayrılan kullanıcıların kullanıcı kimliklerinin hemen kaldırması veya engellemesi,
c) Periyodik olarak gereksiz kullanıcı kimliklerini belirlemek ve kaldırmak ya da engellemek,
d) Gereksiz kullanıcı kimliklerinin başka kullanıcılara verilmediğinin temin edilmesi.

Diğer bilgiler
Bilgi ve bilgi işleme tesislerine erişim sağlanması veya iptali genellikle iki aşamalı bir prosedür ile gerçekleştirilir:

a) Bir kullanıcı kimliği atama, izin verme ya da iptal,
b) Kullanıcı kimliği erişim haklarının sağlanması ya da iptali (bk. Madde 9.2.2).

9.2.2 Kullanıcı erişimine izin verme

Kontrol
Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi uygulanmalıdır.

Uygulama kılavuzu
Kullanıcı kimliklerine verilen erişim hakları atanması ya da iptali için prosedür aşağıdaki hususları içermelidir:

a) Bilgi sistemi ya da hizmetleri kullanımı için bilgi sistemi ya da hizmeti sahibi tarafından yetki verilmesi (bk. Madde 8.1.2); yönetim tarafından erişim hakları için ayrıca onay verilmesi uygun olabilir,
b) Sağlanan erişim seviyesinin erişim politikalarına uygun olduğunun doğrulanması (bk. Madde 9.1) ve bu erişim seviyesinin görevler ayrılığı gibi diğer gereksinimler ile tutarlı olması (bk. Madde 6.1.2),
c) Yetkilendirme prosedürleri tamamlanmadan önce erişim haklarının aktif edilmediğinden emin olunması (örneğin; servis sağlayıcılar tarafından),
d) Bilgi sistemlerine ve hizmetlerine erişmek için kullanıcı kimliklerine verilen erişim haklarının kaydının merkezi olarak tutulması,
e) Kuruluştan bir kişi ayrıldığında, rol ya da işi değiştiğinde kullanıcı erişim haklarının silinmesi ya da engellenmesi gibi kullanıcı erişim haklarının uyarlanması,
f) Bilgi sistemleri ve hizmetlerinin sahipleri ile erişim haklarının periyodik gözden geçirilmesi (bk. Madde 9.2.5).

Diğer bilgiler
Tipik kullanıcı erişim profilleri ile erişim haklarını özetleyen, iş gereksinimlerini temel alan kullanıcı erişim rollerinin kurulmasına dikkat edilmelidir. Erişim istekleri ve gözden geçirilmesi (bk. Madde 9.2.4), özel haklar bazından ziyade roller bazında daha kolay yönetilir.

Personel ya da yüklenici tarafından yetkisiz erişim teşebbüsü olması halinde personel sözleşmelerinde ve hizmet sözleşmelerinde yaptırımları belirten maddelerin de dâhil olmasına dikkat edilmelidir.

9.2.3 Ayrıcalıklı erişim haklarının yönetimi

Kontrol
Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımı kısıtlanmalı ve kontrol edilmelidir.

Uygulama kılavuzu
Ayrıcalıklı erişim hakları tahsisi, ilgili erişim kontrol politikası ile uyumlu resmi bir yetkilendirme prosesi vasıtasıyla kontrol edilmelidir. Aşağıdaki hususlar göz önünde bulundurulmalıdır:

a) İşletim sistemi, veri tabanı yönetim sistemi ve her uygulama ve kullanıcılar gibi her sistem ya da proses ile ilişkili ayrıcalıklı erişim haklarının kime tahsis edileceği tanımlanmalıdır,
b) Kullanım gerekliliğine ve olaydan olaya temelinde, erişim politikası (Madde 9.1.1) ile ayrılmak kaydıyla ayrıcalıklı erişim hakları bireylere tahsis edilmelidir, örneğin, fonksiyonel rolleri için asgari gereklilikler temelinde,
c) Yetki prosesinin ve ayrılmış olan tüm ayrıcalıkların kaydı tutulmalıdır. Yetkilendirme prosesi tamamlanmadan ayrıcalıklı erişim hakları verilmemelidir,
d) Ayrıcalıklı erişim haklarının sona ermesi için gerekler tanımlanmalıdır,
e) Ayrıcalıklı erişim hakları, düzenli iş faaliyetleri için kullanılan kullanıcı kimliğinden farklı bir kullanıcı kimliğine tahsis edilmelidir. Düzenli iş faaliyetleri ayrıcalıklı kullanıcı kimliğinden yapılmamalıdır,
f) Ayrıcalıklı erişim haklarına sahip kullanıcıların yetkinlikleri, söz konusu ayrıcalıklarının görevleri ile ilişkili olup olmadığının doğrulanması için düzenli olarak gözden geçirilmelidir,
g) Sistemlerin yapılandırma yeteneklerine göre, genel yönetici kullanıcı kimliklerinin izinsiz kullanımını önlemek amacıyla belirli bir prosedür oluşturulmalı ve sürdürülmelidir,
h) Genel yönetici kullanıcı kimlikleri için, gizli kimlik doğrulama bilgileri paylaşıldığında gizli kimlik doğrulama bilgilerinin gizliliği sürdürülmelidir (örneğin, parolalar sık sık değiştirilir ve ayrıcalıklı bir kullanıcı ayrıldığında ya da işi değiştiğinde parolalar değiştirilir, uygun mekanizmalarla ayrıcalıklı kullanıcılar arasında iletişim sağlanır).

Diğer bilgiler
Sistem yöneticisi ayrıcalıklarının uygunsuz kullanımı (herhangi bir özellik veya bilgi işleme tesisleri kullanıcıların sistem veya uygulama kontrollerini aşmalarına neden olan) sistemlerin ihlaline ya da hata faktörlerine büyük katkıda bulunur.

9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi

Kontrol
Gizli kimlik doğrulama bilgisinin tahsis edilmesi, resmi bir yönetim prosesi yoluyla kontrol edilmelidir.

Uygulama kılavuzu
Bu proses aşağıdaki gereksinimleri içermelidir:

a) Kullanıcıların kişisel gizli kimlik doğrulama bilgilerini gizli tutmak ve grup gizli kimlik doğrulama bilgilerini sadece grup üyeleri arasında tutmak için bir taahhütname imzalamaları gerekir, bu taahhütname çalışma hüküm ve koşullarında yer alabilir (bk. Madde 7.1.2),
b) Kullanıcıların gizli kimlik bilgilerini korumak için ilk kullanımda değiştirmek zorunda olacakları güvenli geçici gizli kimlik doğrulama bilgileri başlangıçta sağlanmalıdır,
c) Kullanıcıya yeni veya geçici gizli kimlik doğrulama bilgilerini sağlamadan önce kullanıcı kimliğini doğrulama prosedürleri kurulmalıdır,
d) Geçici gizli kimlik doğrulama bilgileri kullanıcılara güvenli bir şekilde verilmelidir, dış tarafların veya korumasız (açık metin) elektronik posta mesajlarının kullanımından kaçınılmalıdır,
e) Geçici gizli kimlik doğrulama bilgileri tek ve benzersiz olmalıdır ve tahmin edilebilir olmamalıdır,
f) Kullanıcılar gizli kimlik doğrulama bilgilerini aldıklarını onaylamalıdır,
g) Varsayılan tedarikçi kimlik doğrulama bilgileri, sistemlerin ya da yazılımın kurulumunu müteakiben değiştirilmelidir.

Diğer bilgiler
Parolalar gizli kimlik doğrulama bilgileri türünün yaygın kullanımıdır ve kullanıcı kimliğini doğrulamanın ortak bir aracıdır. Gizli kimlik doğrulama bilgisinin diğer türleri kimlik doğrulama kodları üreten kriptografik anahtarlar ve diğer veri saklanan donanım tokenları (örneğin, akıllı kartlar).

9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi

Kontrol
Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirmelidir.

Uygulama kılavuzu
Erişim haklarının gözden geçirilmesinde aşağıdaki hususlar dikkate alınmalıdır:

a) Kullanıcı erişim hakları belirli aralıklarla ve çalışanların terfii, rütbe indirilmesi ve iş feshi gibi her değişiklikten sonra gözden geçirilmelidir (bk. Madde 7),
b) Aynı kuruluş içinde bir iş rolünden diğerine geçerken kullanıcı erişim hakları gözden geçirilerek yeniden tahsis edilmelidir,
c) Ayrıcalıklı erişim hakları için yetkilendirmeler daha sık aralıklarla gözden geçirilmelidir,
d) Ayrıcalıkların tahsisi, yetkisiz ayrıcalıkların gerçekleşmediğini temin etmek için belirli aralıklarla kontrol edilmelidir,
e) Ayrıcalıklı hesapların değişiminin periyodik gözden geçirilmesinin kayıtları tutulmalıdır.

Diğer bilgiler
Bu kontrol, Madde 9.2.1, Madde 9.2.2 ve Madde 9.2.6'daki kontrollerin yürütülmesinde olası zayıflıkları dengeler.

9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi

Kontrol
Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme tesislerine erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılmalı veya bunlardaki değişiklik üzerine düzenlenmelidir.

Uygulama kılavuzu
Sonlandırma halinde, bilgi, bilgi işleme tesisleri ve hizmetleri ile ilgili varlıklara bireyin erişim hakkı kaldırılmalı ya da askıya alınmalıdır. Bu husus, erişim haklarını kaldırmanın gerekli olup olmadığını belirler. İstihdam değişiklikleri, yeni istihdam için onaylanmamış tüm erişim haklarının kaldırılmasını yansıtmalıdır. Kaldırılacak ya da yeniden ayarlanacak erişim hakları, fiziksel ve mantıksal erişim haklarını içermelidir. Kaldırma ya da ayar; anahtarların, kimlik kartlarının, bilgi işleme olanaklarının ya da aboneliklerinin kaldırılması, iptal edilmesi ya da değiştirilmesi yoluyla yapılabilir. Çalışanların ve yüklenicilerin erişim haklarını tanımlayan doküman, erişim haklarının kaldırılmasını ya da ayarlanmasını içermelidir. Ayrılan bir çalışan veya dış taraf kullanıcısı, aktif kalan kullanıcı kimliklerinin parolalarını biliyorlarsa, istihdam, anlaşma veya sözleşme feshi durumunda veya değişiminde bu parolalar değiştirilmelidir.

Bilgi ve bilgi işleme tesisleri ile ilişkili varlıklar için erişim hakları aşağıdaki gibi risk faktörlerinin değerlendirilmesine bağlı olarak istihdamın feshi veya değişiminden önce azaltılmalı veya kaldırılmalıdır:

a) Sonlandırma ya da değişikliğin yönetim, çalışan veya dış taraf kullanıcısı tarafından başlatılıp başlatılmadığı ve sonlandırma nedeni,
b) Çalışan, dış taraf veya diğer herhangi bir kullanıcısı mevcut sorumlulukları,
c) Şu anda erişilebilir varlıkların değeri.

Diğer bilgiler
Bazı durumlarda; erişim hakları grup kimlikleri gibi ayrılan çalışanlardan veya dış taraf kullanıcılardan daha fazla kişiye tahsis edilmiş olabilir. Bu gibi durumlarda, ayrılan kişiler grup erişim listelerinden kaldırılmalıdır. Tüm çalışanlara ve üçüncü taraf kullanıcılara ayrılan personel ile bu bilginin paylaşılmaması konusunda tavsiyede bulunulmalıdır.

Yönetimin sonlandırma kararı durumunda hoşnutsuz kalan çalışanlar ya da dış taraf kullanıcılar bilgi işleme tesislerini sabote edebilir veya kasten bilgileri bozabilir. İstifa edilmesi ya da görevden ayrılma durumunda, gelecekte kullanmak üzere bilgi toplamak cazip olabilir.

9.3 Kullanıcı sorumlulukları

Amaç: Kullanıcıları kendi kimlik doğrulama bilgilerinin korunması konusunda sorumlu tutmak.

9.3.1 Gizli kimlik doğrulama bilgisinin kullanımı

Kontrol
Kullanıcıların, gizli kimlik doğrulama bilgisinin kullanımında kurumsal uygulamalara uymaları şart koşulmalıdır.

Uygulama kılavuzu
Tüm kullanıcılar için aşağıdaki hususlar tavsiye edilmelidir:

a) Gizli kimlik doğrulama bilgilerinin gizli tutulması. Bu husus, yöneticiler dâhil tüm diğer taraflara bilgilerin açıklanmamasını sağlar,
b) Gizli kimlik doğrulama bilgilerinin; onaylanmış güvenli ve güçlü saklama yöntemi (örneğin; parola atlaması gibi) kullanılabilene kadar kâğıt, yazılım dosyası ya da el cihazı gibi ortamlarda tutunulmasından kaçınılması,
c) Gizli kimlik doğrulama bilgilerinin olası bir ifşası ile ilgili herhangi bir belirti olduğunda gizli kimlik doğrulama bilgilerinin değiştirilmesi,
d) Parolalar gizli kimlik doğrulama bilgisi olarak kullanıldığında, yeterli azami uzunlukta aşağıdaki hususları sağlayan kaliteli parolalar seçilmelidir,
    1) Hatırlanması kolay,
    2) Herhangi bir kişinin kolayca tahmin edebileceği veya kullanan kişi ile ilgili bilgiler kullanılarak elde edilebilir olmamalıdır (örneğin; isimler, telefon numaraları ve doğum tarihleri gibi),
    3) Sözlük saldırısına savunmasız olmamalıdır (yani, sözlüklere dâhil olan kelimelerden ibaret olmamalıdır),
    4) Ardışık, tümü sayısal ya da tümü alfabetik karakterlerden oluşmamalıdır,
    5) Geçici ise ilk oturum açmada değiştirilmelidir,
e) Bireysel kullanıcıların gizli kimlik doğrulama bilgileri paylaşılmamalıdır,

f) Otomatikleştirilmiş oturum açma prosedürleri ve depolamalarında parolalar gizli kimlik doğrulama bilgisi olarak kullanıldığında parolalara doğru bir koruma sağlanmalıdır,
g) İş ve iş dışı amaçlar için aynı gizli kimlik doğrulama bilgileri kullanılmamalıdır.

Diğer bilgiler
Tek oturum açma hususu ya da diğer gizli kimlik doğrulama bilgileri yönetim araçları, kullanıcıların koruması gereken gizli kimlik doğrulama bilgilerini azaltabilir ve dolayısıyla bu kontrollerin etkinliğini arttırabilir. Ancak; bu araçlar aynı zamanda gizli kimlik doğrulama bilgilerinin ifşa edilmesinin etkisini de arttırabilir.

9.4 Sistem ve uygulama erişim kontrolü

Amaç: Sistem ve uygulamalara yetkisiz erişimi engellemek.

9.4.1 Bilgiye erişimin kısıtlanması

Kontrol
Bilgi ve uygulama sistem fonksiyonlarına erişim, erişim kontrol politikası doğrultusunda kısıtlanmalıdır.

Uygulama kılavuzu
Erişim kısıtlaması bireysel iş uygulama gereksinimlerini temel almalı ve tanımlanan erişim kontrol politikası ile uyumlu olmalıdır.

Aşağıdaki hususların uygulanması erişim kısıtlaması gereksinimlerini desteklemek amacıyla dikkate alınmalıdır:

a) Uygulama sistem fonksiyonlarına erişimin kontrolü için menülerin sağlanması,
b) Verilere belirli kullanıcılar tarafından erişilebildiğinin kontrol edilmesi,
c) Kullanıcıların erişim haklarının kontrolü, örneğin; okuma, yazma, silme ve yürütme,
d) Diğer uygulamalara erişim haklarının kontrolü,
e) Çıktılardaki bilginin sınırlandırılması,
f) Hassas uygulamaların, uygulama verilerinin veya sistemlerin yalıtımı için fiziksel ya da mantıksal erişim kontrollerinin sağlanması.

9.4.2 Güvenli oturum açma prosedürleri

Kontrol
Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir.
Uygulama kılavuzu
Bir kullanıcının iddia edilen kimliğinin kanıtlanması için uygun kimlik doğrulama tekniği seçilmelidir.

Güçlü kimlik doğrulama ve kimlik doğrulama gerekli olduğunda, parolalara alternatif olarak kriptografik araçlar, akıllı kartlar, token ya da biyometrik araçlar gibi kimlik doğrulama yöntemleri kullanılabilir.

Bir sistem ya da uygulamaya giriş için prosedürler, yetkisiz erişim fırsatlarını asgari düzeye indirecek şekilde tasarlanmalıdır. Dolayısıyla, oturum açma prosedürü, yetkisiz kullanıcılara yardım sağlamaktan kaçınmak için sistem ya da uygulama hakkında en az bilgiyi açığa çıkarmalıdır. İyi bir oturum açma prosedürü aşağıdaki şekilde olmalıdır:

a) Oturum açma başarıyla tamamlanana kadar, sistem ve uygulama tanımlayıcılarını görüntülememelidir,
b) Bilgisayara sadece yetkili kullanıcıların erişim sağlaması gerektiğini belirten genel bir uyarı haberi görüntülemelidir,
c) Oturum açma sırasında yetkisiz kullanıcılara yardım edebilecek hiçbir yardım mesajı sağlanmamalıdır,
d) Oturum açma bilgisini, sadece tüm girdi verilerinin tamamlanması üzerine geçerli kılmalıdır. Eğer bir hata durumu ortaya çıkarsa, sistem verinin hangi kısmının doğru ve yanlış olduğunu belirtmemelidir,

e) Kaba kuvvet oturum açma girişimlerine karşı korumalıdır,
f) Başarılı ve başarısız girişimlerin kayıtları tutulmalıdır,
g) Potansiyel girişimler ya da oturum açma kontrollerinin başarılı ihlali tespit edilirse bir güvenlik olayı başlatılmalıdır,
h) Başarılı bir oturum açma prosesinin tamamlanmasının ardından aşağıdaki bilgiler görüntülenmelidir:
    1) Önceki başarılı oturum açmanın tarihi ve zamanı,
    2) En son başarılı oturum açmadan bu yana her başarısız oturum açma denemesinin detayları,
i) Girilen parolanın görüntülenmemesine dikkat edilmelidir,
j) Bir ağ üzerinden parolalar açık metin olarak iletilmemelidir,
k) Tanımlanan bir hareketsizlik süresi sonrasında aktif olmayan oturumlar sonlandırılmalıdır, özellikle halka açık alanlar ya da kuruluş güvenlik yönetimi dışındaki dış alanlarda ya da mobil cihazlar gibi yüksek riskli yerlerde,
l) Yüksek riskli uygulamalar için ek güvenliği sağlamak ve yetkisiz erişim fırsatlarını azaltmak amacıyla bağlantı süreleri kısaltılmalıdır.

Diğer bilgiler
Parolalar, sadece kullanıcılarının bildiği gizliliğe dayalı kimlik bilgilerini ve kimlik doğrulamayı sağlayan ortak bir yoldur. Bu husus, aynı zamanda kriptografik kontroller ve kimlik doğrulama protokolü ile elde edilebilir. Kullanıcı kimlik doğrulamanın gücü, erişilecek bilginin sınıflandırılmasına uygun olmalıdır.

Parolaların ağ üzerinden oturuma giriş esnasında açık metin olarak iletilmesi durumunda, bu ağ üzerinde yer alan bir 'dinleyici (sniffer)' programı ile bu parolalar elde edilebilir.

9.4.3 Parola yönetim sistemi

Kontrol
Parola yönetim sistemleri etkileşimli olmalı ve kaliteli parolaları temin etmelidir.

Uygulama kılavuzu
Parola yönetim sistemi aşağıdaki hususları sağlamalıdır:

a) Hesap verilebilirliği sürdürmek için bireysel kullanıcı kimliklerinin ve parolalarının kullanımını zorunlu kılması,
b) Uygun olan yerlerde, kullanıcılara kendi parolalarını seçme ve değiştirme hakkının tanınması ve girdi hataları için teyit prosedürü içermesi,
c) Nitelikli parola seçiminin zorlaması,
d) Kullanıcıların kendi parolalarını ilk oturum açmada değiştirmeye zorlamalıdır,
e) Düzenli parola değiştirme gerektirmesi ve zorlaması,
f) Önceki parolaların bir kaydını saklamalı ve tekrar kullanımını engellemeli,
g) Giriş yapılırken parolaları ekranda görüntülememeli,
h) Parola dosyalarını, uygulama sistem verilerinden ayrı bir yerde saklamalı,
i) Parolaları korumalı formda saklamalı ve iletmeli.

Diğer bilgiler
Bazı uygulamalarda kullanıcı parolalarının bağımsız bir otorite tarafından verilmesi gerekir. Bu durum, yukarıda belirtilen maddelerden b), d) ve e)'de uygulanamaz. Çoğu durumda parolalar kullanıcılar tarafından seçilir ve korunur.

9.4.4 Ayrıcalık destek programlarının kullanımı

Kontrol
Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir.

Uygulama kılavuzu
Sistem ve uygulamaların kontrolleri geçersiz kılma yeteneğine sahip olabilen destek programlarını kullanımı için aşağıdaki hususlar dikkate alınmalıdır:

a) Destek sistem programları için kullanıcı tanımlama, kimlik doğrulama ve yetkilendirme prosedürleri,
b) Uygulama yazılımından destek programlarının ayrılması,

c) Destek programlarının kullanımının en az sayıda güvenilir ve yetkili kullanıcılarla sınırlandırılması (bk. Madde 9.2.3),
d) Destek sistem programlarının geçici kullanımı için yetkilendirme,
e) Destek programlarının kullanılabilirliğinin sınırlanması, örneğin; yetkilendirilmiş değişim süresince,
f) Destek programlarının kullanım kayıtları,
g) Destek programları için yetkilendirme düzeyleri tanımlanması ve yazılı hale getirilmesi,
h) Tüm gereksiz yardımcı programların kaldırılması ya da devre dışı bırakılması,
i) Sistemlerde uygulamalara erişimi olan kullanıcılar için görevden ayrılık gerektiğinde yardımcı programların kullanılamaz yapılması.

Diğer bilgiler
Çoğu bilgisayar kurulumu bir veya daha fazla destek programlarına sahiptir. Bu durum sistem ve uygulama kontrollerini geçersiz kılabilir.

9.4.5 Program kaynak koduna erişim kontrolü

Kontrol
Program kaynak koduna erişim kısıtlanmalıdır.

Uygulama kılavuzu
Program kaynak kodu ve ilgili öğelere (tasarımlar, özellikler, doğrulama planları ve geçerleme planları gibi) erişim, yetkisiz işlevsellik girişini ve istenmeyen değişiklikleri önlemenin yanı sıra değerli fikri mülkiyet haklarının gizliliğini sağlamak için sıkı bir şekilde kontrol edilmelidir. Program kaynak kodu için bu, tercihen program kaynak kütüphanelerinde kod kontrollü merkezi depolama ile elde edilebilir. Bilgisayar programlarının çökme ihtimalini azaltmak amacıyla bu tür program kaynak kütüphanelerine erişimi kontrol etmek için aşağıdaki hususlara dikkat edilmelidir:

a) Mümkün olduğu sürece, program kaynak kütüphanesi işletimdeki sistemler içinde tutulmamalıdır,
b) Program kaynak kodu ve program kaynak kütüphanesi oluşturulmuş prosedürler ile yönetilmelidir,
c) Destek personeli, program kaynak kütüphanesine sınırsız erişim yetkisine sahip olmamalıdır,
d) Programcılar, program kaynak kütüphanesinin ve ilişkili öğelerin güncellenmesi ve program kaynaklarının yayınlanmasını sadece uygun yetki alındıktan sonra yapmalıdır,
e) Program listeleri güvenli bir ortamda saklanmalıdır,
f) Program kaynak kütüphanelerine yapılan tüm erişimlerin denetim günlüğü tutulmalıdır,
g) Program kaynak kütüphanelerinin sürdürülmesi ve kopyalanması sıkı değişim kontrol prosedürlerine (bk. Madde 14.2.2) tabi olmalıdır.

Program kaynak kodunun yayınlanması amaçlanıyorsa bütünlüğü hakkında güvence sağlamaya yardımcı olmak için ek kontroller (örneğin; sayısal imza) dikkate alınmalıdır.

10 Kriptografi

10.1 Kriptografik kontroller

Amaç: Bilginin gizliliği, aslına uygunluğu ve/veya bütünlüğü' nün korunması için kriptografi' nin doğru ve etkin kullanımını temin etmek.

10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika

Kontrol
Bilginin korunması için kriptografik kontrollerin kullanımına dair bir politika geliştirilmeli ve uygulanmalıdır.

Uygulama kılavuzu
Kriptografi politikası geliştirilirken aşağıdaki hususlara dikkat edilmelidir:

a) İş bilgilerinin korunacağı genel esasları de içeren, kuruluş içerisinde kriptografik kontrollerin kullanımına yönelik yönetim yaklaşımına,
b) Bir risk değerlendirmesine dayanılarak, gereken koruma düzeyi; gerekli şifreleme algoritmasının türü, gücü ve kalitesi de hesaplanarak tanımlanmalıdır,

c) Mobil aygıtlar ya da taşınabilir ortam aygıtları veya iletişim hatları tarafından iletilen hassas bilginin korunması için şifreleme kullanılmalıdır,
d) Anahtarların kayıp, tehlike altında ya da zarar görmüş olması söz konusu olduğunda, şifrelenmiş bilgilerin kurtarılması ve kriptografik anahtarların korunması ile ilgili yöntemlerde dâhil olmak üzere anahtar yönetimi yaklaşımı,
e) Roller ve sorumluluklar, örneğin; aşağıdakilerden kimlerin sorumlu olduğu,
    1) Politikanın uygulanması,
    2) Anahtar üretimi dâhil anahtar yönetimi (bk. Madde 10.1.2),
f) Kuruluş çapında etkin uygulamanın sağlanması için kabul edilen standartlar (hangi iş prosesleri için hangi çözümlerin kullanılacağı),
g) İçerik inceleme ile şifrelenmiş bilgilerin kullanımının etkisinin kontrolü (örneğin, kötücül yazılım tespit etme),

Kuruluşun kriptoloji politikası uygulanırken, dünyanın farklı yerlerinde kullanılan kriptografi teknikleri ve şifrelenmiş bilgilerin sınır ötesine akış sorunları için geçerli yasalara ve ulusal kısıtlamalara dikkat edilmelidir (bk. Madde 18.1.5).

Kriptografik kontroller, farklı bilgi güvenliği amaçlarını elde etmek için kullanılabilir. Örneğin;

a) Gizlilik: saklanan ya da iletilen hassas veya kritik bilgilerin korunması için bilgilerin şifrelenmesi amacıyla kullanımı,
b) Bütünlük/doğruluk: saklanan ya da iletilen hassas veya kritik bilgilerin bütünlüğünü ve doğruluğunu doğrulamak için sayısal imzaların ve mesaj doğrulama kodlarının kullanımı,
c) İnkâr edilemezlik: bir olay ya da eylem oluşumunun veya oluşmamasının kanıtını sağlamak üzere kriptografi tekniklerinin kullanımı,
d) Kimlik doğrulama: sistem kullanıcıları, varlıklar ve kaynaklar ile kullanıcılara ya da diğer sistem varlıklarına erişim ya da işlem talebini doğrulamak için kriptografik tekniklerin kullanımı.

Diğer bilgiler
Bir kriptografi çözümünün uygun olup olmadığı konusunda karar verme, kontrollerin seçiminin ve risk değerlendirmesinin daha geniş prosesin bir parçası olarak görülmelidir. Bu değerlendirme daha sonra hangi kontrollerin uygulandığının ve hangi amaç ve iş prosesleri için kriptografik kontrolün uygun olup olmadığını belirlemek için kullanılabilir.

Kriptografik kontrollerin kullanım politikası, kriptografik tekniklerin kullanımındaki riskleri asgariye indirmek ve faydaları azamiye çıkarmak ile uygunsuz ve hatalı kullanımı önlemek için gereklidir.

Bilgi güvenliği politika amaçlarını karşılamak için uygun kriptografik kontrollerin seçiminde uzman tavsiyesi aranmalıdır.

10.1.2 Anahtar yönetimi

Kontrol
Kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair bir politika geliştirilmeli ve tüm yaşam çevirimleri süresince uygulanmalıdır.

Uygulama kılavuzu
Politika, anahtarların üretilmesi, depolanması, arşivlenmesi, alınması, dağıtımı, çekilmesi ve imha edilmesini de içeren yaşam çevrimleri boyunca kriptografik anahtarların yönetimi için gerekleri içermelidir.
Kriptografik algoritmalar, anahtar uzunlukları ve kullanım uygulamaları en iyi uygulamalara göre seçilmelidir.
Uygun anahtar yönetimi; kriptografik anahtarların üretilmesi, depolanması, arşivlenmesi, alınması, dağıtımı, çekilmesi ve imha edilmesi için güvenli prosesi gerektirir.

Tüm kriptografik anahtarlar değişikliğe ve kayba karşı korunmalıdır. Ek olarak, gizli ve özel anahtarlar, ifşa edilme gibi yetkisiz kullanıma karşı korunmalıdır.

Anahtarların üretilmesi, depolanması ve arşivlenmesi için kullanılan ekipmanlar fiziksel olarak korunmalıdır.

Anahtar yönetim sistemi, aşağıdaki hususlar için üzerinde anlaşılmaya varılmış standartlar, prosedürler ve güvenli yöntemler setini temel almalıdır:

a) Farklı şifreleme sistemleri ve farklı uygulamalar için anahtarların üretimi,
b) Açık anahtar sertifikası yayınımı ve edinimi,
c) Teslim alındığında anahtarların nasıl etkinleştirileceği de dâhil olmak üzere, anahtarların amaçlanan varlıklara dağıtılması,
d) Yetkili kullanıcıların anahtarlara nasıl erişebileceği de dâhil olmak üzere, anahtarların saklanması,
e) Anahtarların ne zaman değiştirilmesi gerektiği ve bunun nasıl yapılması gerektiği konusundaki kurallar da dâhil olmak üzere, anahtarların değiştirilmesi ya da güncellenmesi,
f) Zarar görmüş anahtarlara müdahale,
g) Anahtar zarara uğradığında ya da bir kullanıcı bir kuruluştan ayrıldığında (ki bu durumda da anahtar arşive kaldırılmalıdır) olduğu gibi, anahtarların nasıl geri çekilmesi ya de aktive edilmesi gerektiği de dâhil olmak üzere, anahtarların geri alınması,
h) Kaybolan ya da kötüye kullanılan anahtarların kurtarılması,
i) Anahtarların yedeklenmesi ya da arşivlenmesi,
j) Anahtarların ortadan kaldırılması,
k) Anahtar yönetimi ile ilişkili faaliyetlerin kayıt dosyalarının oluşturulması ve denetlenmesi.

Yanlış kullanım olasılığını azaltmak amacıyla anahtarlar için aktivasyon ve aktivasyon iptal tarihleri, anahtar kullanım politikasında tanımlanan belirli süre için anahtarların kullanılabilir olacağı şekilde tanımlamalıdır.

Gizli ve özel anahtarların güvenli bir şekilde yönetilmesi konusuna ek olarak, açık anahtarların geçerliliği de dikkate alınmalıdır. Bu kimlik doğrulama süreci normalde sertifika otoriteleri tarafından sağlanan açık anahtar sertifikaları kullanılarak gerçekleştirilebilir. Gereken güven derecesini sağlamak için prosedürler yerinde olmalıdır ve uygun kontroller kuruluş tarafından sağlanmalıdır.
Bir belgelendirme otoritesi gibi dış kriptografik hizmet tedarikçileriyle yapılan hizmet seviyesi anlaşmalarının ya da sözleşmelerinin içeriği, sorumluluk, hizmetlerin güvenilirliği ve hizmetlerin provizyonuna ilişkin yanıt süreleri konularını kapsamalıdır (bk. Madde 15.2).

Diğer bilgiler
Kriptografik anahtarların yönetiminde kriptografik tekniklerin etkin kullanımı esas alınmalıdır. Anahtar yönetimi hakkında daha fazla bilgi ISO/IEC 11770 [2] [3] [4] standardında sağlanmıştır.

Kriptografik teknikler, kriptografik anahtarların korunmasında kullanılabilir. Kriptografik anahtarlara erişimle ilgili yasal taleplerin karşılanması için prosedürlerin dikkate alınması gerekebilir. Örneğin, şifrelenmiş bir bilginin bir duruşma sırasında kanıt olarak deşifre edilmiş halde erişilebilir olması gerekebilir.

11 Fiziksel ve çevresel güvenlik

11.1 Güvenli alanlar

Amaç: Yetkisiz fiziksel erişimi, kuruluşun bilgi ve bilgi işleme tesislerine hasar verilmesini ve müdahale edilmesini engellemek.

11.1.1 Fiziksel güvenlik sınırı

Kontrol
Hassas veya kritik bilgi ve bilgi işleme tesislerini barındıran alanları korumak için güvenlik sınırları tanımlanmalı ve kullanılmalıdır.

Uygulama kılavuzu
Fiziksel güvenlik sınırları için uygun olan yerlerde aşağıdaki hususlar dikkate alınmalı ve uygulanmalıdır:

a) Güvenlik sınırları tanımlanmalıdır; her bir güvenlik sınırının konumlandırılması ve kuvvetlendirilmesi, risk değerlendirme sonuçları ve sınırların içerisindeki varlıkların güvenlik gereklerine bağlıdır,
b) Bilgi işleme tesislerinin bulunduğu bina veya alanın sınırları fiziksel olarak belirlenmelidir (örneğin; çevrede veya alan içinde zorla içeriye girmenin kolayca olabileceği herhangi bir boşluk

bulunmamalıdır); alanın dışını çevreleyen çatısı, duvarları ve zemin kaplaması dayanıklı olarak inşa edilmiş olmalı ve tüm dış duvarlar yetkisiz erişime karşı uygun bir şekilde korunmuş olmalıdır; örneğin, kapı ve pencereler gözetimsiz olduğu zamanlarda kilitlenmeli ve özellikle zemin seviyelerde pencere için dış koruma (parmaklıklar, uyarı sinyalleri ve kilitler vb.) dikkate alınmalı,

c) Bina veya alana fiziksel erişim kontrolü için insanlı danışma alanı ya da diğer araçlar olmalıdır, binalara ve alanlara erişim sadece yetkilendirilmiş personel ile sınırlı olmalıdır,
d) Fiziksel bariyerler uygun olan yerlerde çevre kirliliğini ve izinsiz fiziksel erişimi engellemek için inşa edilmelidir,
e) Bölgesel, ulusal ve uluslararası standartlarla uyumlu olarak direnci gerekli seviyede kurmak için duvarlar ile birlikte güvenlik sınırlarındaki tüm yangın kapılarına uyarı sinyalleri takılmalı, izlenmeli ve test edilmelidir; bu önlemler güvenli bir şekilde yerel yangın koduna uygun olarak çalışmalıdır,
f) Uygun saldırı algılama sistemleri, ulusal, bölgesel ve uluslararası standartlara göre kurulmalı ve düzenli olarak tüm dış kapılar ve erişilebilir pencereler kontrol edilmeli; boş alanlar her zaman uyarı sinyalleri ile donatılmalıdır, diğer alanlar için koruma kapsamı ayrıca sağlanmalıdır, örneğin; bilgisayar odası ve iletişim odaları,
g) Kuruluş tarafından yönetilen bilgi işleme tesisleri dış taraflarca yönetilen yerlerden fiziksel olarak ayrılmalıdır.

Diğer bilgiler
Fiziksel koruma, kuruluşun tesislerinde ve bilgi işleme tesislerinde bir ya da daha fazla fiziksel engeller oluşturularak gerçekleştirilebilir. Birden fazla engel kullanımı, ilave bir koruma sağlayarak tek bir engelin başarısızlığı durumunda güvenliğin derhal tehlikeye girmesini önler.

Güvenli alan, sürekli iç fiziksel güvenlik engelleri ile çevrili, kilitlenebilir bir ofis ya da birkaç oda olabilir. Fiziksel erişim kontrolü için ek engeller ve sınırlar, güvenlik sınırı içinde farklı güvenlik gerekleri olan alanlar arasında gerekebilir. Birden fazla kuruluşun aynı bina içerisinde olduğu durumlarda fiziksel erişim güvenliğine özel dikkat edilmelidir.

Risk değerlendirmesinde belirtildiği gibi özellikle güvenli alanlar için fiziksel kontrollerin uygulanması, kuruluşun teknik ve ekonomik koşullarına adapte edilmelidir.

11.1.2 Fiziksel giriş kontrolleri

Kontrol
Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunmalıdır.

Uygulama kılavuzu
Aşağıdaki hususlar dikkate alınmalıdır:

a) Ziyaretçilerin giriş ve çıkışlarının tarih ve saatleri kayıt altına alınmalıdır ve daha önce erişimi onaylanmadığı sürece tüm ziyaretçiler denetlenmelidir; ziyaretçilere sadece belirli, yetkilendirildikleri amaçlar için erişim verilmelidir ve alanının güvenlik gereklerinde ve acil durum prosedürlerinde ilgili talimatlar belirtilmelidir. Ziyaretçilerin kimliği uygun bir yöntem ile doğrulanmalıdır,
b) Hassas bilgilerin işlendiği veya saklandığı alanlara erişim sadece uygun erişim kontrolleri uygulanarak yetkili kişiler ile sınırlandırılmalıdır; örneğin, erişim kartı ve şifresi gibi iki faktörlü kimlik doğrulama mekanizması uygulanarak,
c) Tüm erişimlerin fiziksel kayıt defteri ya da elektronik denetim izleri güvenli şekilde sürdürülmeli ve izlenmelidir,
d) Tüm çalışanların, yüklenicilerin ve harici taraf çalışanların görünür bir kimlik takma zorunluluğu olmalıdır ve refakat edilmeyen bir ziyaretçi ile karşılaştıklarında veya kimlik takmayan bir kişi gördüklerinde hemen güvenlik personeline bilgi vermelidir,
e) Dış taraf destek personeline sadece gerektiğinde güvenli alanlara veya gizli bilgi işleme tesislerine kısıtlı erişim verilmelidir, bu erişim yetkilendirilmeli ve izlenmelidir,
f) Güvenli bölgeye erişim hakları düzenli olarak gözden geçirilmeli, güncellenmeli ve gerektiğinde iptal edilmelidir (bk. Madde 9.2.5 ve Madde 9.2.6).

11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması

Kontrol
Ofisler, odalar ve tesisler için fiziksel güvenlik tasarlanmalı ve uygulanmalıdır.

Uygulama kılavuzu
Aşağıdaki hususlar ofislerin, odaların ve tesislerin güvenliğini sağlamak için dikkate alınmalıdır:

a) Anahtar konumundaki tesislere herkesin erişimini engellemek için söz konusu tesisler uygun şekilde konumlandırılmalıdır,
b) Binalar göze çarpmayan bir şekilde olmalıdır ve bilgi işleme faaliyetlerinin, bina içinde veya dışında, varlığını tanımlayan belirgin bir işaret olmaksızın amaçlarıyla ilgili en az ipucunu vermelidir,
c) Gizli bilgilerin ve faaliyetlerin dışarından korunması için dışarıdan görülebilir ve duyulabilir olmasını engellemek üzere tesislerin yapılandırılmalıdır. Elektromanyetik kalkan kullanımı uygun olan yerlerde göz önünde bulundurulmalıdır,
d) Gizli bilgi işleme tesislerinin yerlerini belirten dizinler ve dâhili telefon rehberleri yetkilendirilmemiş herkes tarafından kolayca erişilebilir yerlerde olmamalıdır.

11.1.4 Dış ve çevresel tehditlere karşı koruma

Kontrol
Doğal felaketler, kötü niyetli saldırılar veya kazalara karşı fiziksel koruma tasarlanmalı ve uygulanmalıdır.

Uygulama kılavuzu
Yangın, sel, deprem, patlama, sivil kargaşa ve doğal ya da insan yapımı felaketlerin diğer formlarından zarar görmesinin nasıl önleneceği hakkında uzman tavsiyesi alınmalıdır.

11.1.5 Güvenli alanlarda çalışma

Kontrol
Güvenli alanlarda çalışma için prosedürler tasarlanmalı ve uygulanmalıdır.

Uygulama kılavuzu
Aşağıdaki hususlar dikkate alınmalıdır:

a) Personel, güvenli alanın varlığını ve içeride yürütülen faaliyetleri, bilmesi gerektiği kadar bilmelidir.
b) Güvenlik sebeplerinden dolayı ve kötü niyetli faaliyetlere fırsat vermemek için güvenli alanlarda denetlenmemiş çalışmalardan kaçınılmalıdır.
c) Sahipsiz güvenli alanlar fiziksel olarak kilitlenmeli ve periyodik olarak gözden geçirilmelidir,
d) Yetki verilmediği sürece, fotoğraf, video, ses ve diğer kayıt cihazları ve mobil cihazlardaki kameralara izin verilmemelidir.

Güvenli alanlarda çalışmak için anlaşmalar güvenli bir alanda çalışan çalışanlar ve dış taraf kullanıcılar için kontrolleri içerir ve güvenli bir alanda yer alan tüm faaliyetleri kapsar.

11.1.6 Teslimat ve yükleme alanları

Kontrol
Yetkisiz kişilerin tesise giriş yapabildiği, teslimat ve yükleme alanları gibi erişim noktaları ve diğer noktalar kontrol edilmeli ve mümkünse yetkisiz erişimi engellemek için bilgi işleme tesislerinden ayrılmalıdır.

Uygulama kılavuzu
Aşağıdaki hususlar dikkate alınmalıdır:

a) Dağıtım ve yükleme alanlarına binanın dışından erişim, tanımlanmış ve yetkilendirilmiş personel ile sınırlandırılmalıdır,
b) Dağıtım ve yükleme alanları, dağıtım personelinin binanın diğer bölümlerine erişim sağlamasını engelleyebilecek şekilde tasarlanmalıdır,
c) Dağıtım ve yükleme alanlarının dış kapısı, iç kapıları açıldığında emniyete alınmalıdır,
d) Bir teslimat ve yükleme alanında gelen malzemeler taşınmadan önce patlayıcılar, kimyasallar ya da diğer tehlikeli maddeler içerip içermedikleri bakımından kontrol ve muayene edilmelidir,
e) Gelen malzeme tesise girişte varlık yönetimi prosedürlerine (bk. Madde 8) uygun olarak kayıt edilmelidir,
f) Mümkünse gelen ve giden sevkiyatlar fiziksel olarak ayrılmalıdır,

g) Gelen malzemeler yolda karıştırılıp karıştırılmadığının tespiti için kontrol edilmelidir. Bu tür karıştırma müdahaleleri tespit edilirse derhal güvenlik personeline rapor edilmelidir.

11.2 Teçhizat

Amaç: Varlıkların kaybedilmesi, hasar görmesi, çalınması veya ele geçirilmesini ve kuruluşun faaliyetlerinin kesintiye uğramasını engellemek.

11.2.1 Teçhizat yerleştirme ve koruma

Kontrol
Teçhizat, çevresel tehditlerden ve tehlikelerden ve yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmeli ve korunmalıdır.

Uygulama kılavuzu
Teçhizat korumada aşağıdaki hususlar dikkate alınmalıdır:

a) Teçhizatalar, çalışma alanları içine gereksiz erişimi en aza indirgemek üzere konumlandırılmalıdır,
b) Hassas veri işlenen bilgi işleme tesisleri, kullanımları sırasında yetkilendirilmemiş kişiler tarafından bilgilerin görünmesi riskini azaltmak için dikkatli bir şekilde konumlandırılmalıdır,
c) Depolama tesisleri, yetkisiz erişimi önlemek için güvence altına alınmalıdır,
d) Özel koruma gerektiren öğeler, genel koruma düzeyini azaltmak için himaye edilmelidir,
e) Kontroller, potansiyel fiziksel ve çevresel tehditlerin risklerini azaltmak için uyarlanmalıdır. Örneğin, hırsızlık, yangın, patlayıcı maddeler, duman, su (veya su kesintisi), toz, titreşim, kimyasal etkiler, elektrik kaynağı girişimi, iletişim girişimi, elektromanyetik radyasyon ve vandalizm.
f) Kuruluşun, yeme, içme ve sigara içme politikaları bilgi işleme tesislerine yakınlığına göre oluşturulmalıdır,
g) Sıcaklık ve nem gibi çevresel koşullar, bilgi işleme tesislerini olumsuz etkileyebilecek koşullar için izlenmelidir,
h) Yıldırımdan korunma tüm binalar için uygulanmalı ve yıldırımdan korunma filtreleri tüm gelen güç ve iletişim hatlarına takılmalıdır,
i) Klavye örtüleri gibi özel koruma yöntemlerinin kullanılması endüstriyel ortamlarda kullanılan ekipmanlarda dikkate alınmalıdır,
j) Gizli bilgileri işleyen teçhizatlar, elektromanyetik yayılım nedeniyle bilgi sızma riskini en aza indirmek için korunmalıdır.

11.2.2 Destekleyici altyapı hizmetleri

Kontrol
Teçhizat destekleyici altyapı hizmetlerindeki hatalardan kaynaklanan enerji kesintileri ve diğer kesintilerden korunmalıdır.

Uygulama kılavuzu
Destekleyici altyapı hizmetleri (örneğin; elektrik, telekomünikasyon, su tesisatı, gaz, kanalizasyon, havalandırma ve klima) aşağıdaki hususları desteklemelidir:

a) Ekipman üreticisinin özelliklerine ve yerel yasal gereksinimlere uyum,
b) Diğer destekleyici altyapı hizmetlerinin kapasite büyümesi ve etkileşimlerini karşılamak için kapasitenin düzenli olarak değerlendirilmesi,
c) Düzgün işleyişi sağlamak için denetlenmeli ve test edilmelidir,
d) Gerekirse, arızaları tespit etmek için alarm sistemine sahip olmalıdır,
e) Gerekirse, çeşitli fiziksel yönlendirme ile çoklu beslemeye sahip olmalıdır.

Acil aydınlatma ve iletişim sağlanmalıdır. Elektrik, su, gaz ve diğer destekleyici altyapı hizmetlerini kesmek için kullanılan acil durum anahtarları ve vanalar; acil çıkışların veya ekipman odalarının yakınında konumlandırılmalıdır.

Diğer bilgiler

Ağ bağlantısı için ilave yedekleme, birden fazla destekleyici altyapı hizmetleri sağlayıcından birden fazla yol ile elde edilebilir.

11.2.3 Kablo güvenliği

Kontrol
Veri veya destekleyici bilgi hizmetlerini taşıyan enerji ve iletişim kabloları, dinleme, girişim oluşturma veya hasara karşı korunmalıdır.

Uygulama kılavuzu
Kablolama güvenliğinde aşağıdaki hususlar dikkate alınmalıdır:

a) Bilgi işleme tesislerindeki güç ve telekomünikasyon hatları mümkünse yer altında olmalıdır ya da yeterli alternatif korumaya sahip olmalıdır,
b) Güç kabloları, iletişim kablolarında girişimi engellemek için ayrılmalıdır,
c) Hassas ve kritik sistemler için daha fazla düşünülmesi gereken kontroller aşağıdadır:
    1) Zırhlı kanal kurulumu ve kilitli odalar veya muayene kutuları ve sonlandırma noktaları,
    2) Kabloları elektromanyetikten korumak için kalkan kullanılması,
    3) İzinsiz cihazların kablolara takılı olması durumunu engellemek için teknik tarama ve fiziksel kontrollerin başlatılması,
    4) Patch panel ve kablo odalarına kontrollü erişim.

11.2.4 Teçhizat bakımı

Kontrol
Teçhizatın bakımı, sürekli erişilebilirliğini ve bütünlüğünü temin etmek için doğru şekilde yapılmalıdır.

Uygulama kılavuzu
Teçhizat bakımında aşağıdaki hususlar dikkate alınmalıdır:

a) Teçhizatın tedarikçinin önerilen servis aralıklarına ve özelliklerine uygun olarak bakımı yapılmalıdır,
b) Sadece yetkili bakım personeli teçhizatların onarım ve bakımını yapmalıdır,
c) Tüm arıza şüphelerinin, gerçek arızaların ve tüm önleyici ve düzeltici bakımların kaydı tutulmalıdır,
d) Ekipman bakımı için planlanan zamanda uygun kontroller uygulanmalıdır, bu bakımın alan veya kuruluş dışındaki ilgili personel tarafından yapılıp yapılmayacağı dikkate alınarak; gerekli durumlarda, gizli bilgiler teçhizatlardan temizlenmelidir veya bakım personeli yeterli düzeyde güvenlik taramasından geçirilmelidir,
e) Sigorta poliçelerinin getirdiği tüm gereksinimlere uyulmalıdır,
f) Bakımdan sonra çalışmaya alınacak teçhizatı devreye almadan önce, teçhizatın kurcalanmadığını ve arıza olmamasını temin etmek için muayene edilmelidir.

11.2.5 Varlıkların taşınması

Kontrol
Teçhizat, bilgi veya yazılım ön yetkilendirme olmaksızın kuruluş dışına çıkarılmamalıdır.

Uygulama kılavuzu
Aşağıdaki hususlar dikkate alınmalıdır:

a) Varlıkları kuruluş çevresi dışına çıkarma yetkisinin hangi çalışanın ve yüklenicinin sahip olduğu açıkça tanımlanmalıdır,
b) Varlıkların kaldırılması için zaman sınırlamaları ayarlanmalıdır ve uygunluk için varlığın geri dönüşü doğrulanmalıdır,
c) Gerektiğinde ve uygun olduğunda varlıklar kuruluş çevresi dışına çıkarıldığında ve geri getirildiğinde kayıt edilmelidir,
d) Varlıkları işleyen ya da kullanan herhangi bir kişinin kimliği, rolü ve aboneliği yazılı hale getirilmelidir ve bu belgeler teçhizat, bilgi ya da yazılım ile iade edilmelidir.

Diğer bilgiler
Varlığın izinsiz kaldırılmasını algılamak için üstlenilen rastgele kontroller, ayrıca yetkisiz kayıt cihazlarının, silahların vb. tespitini yapabilir ve siteye girmelerini ve çıkmalarını engeller. Bu tür yerinde kontroller, ilgili

yasalara ve düzenlemelere uygun olarak yapılmalıdır. Bireyeler, kontrollerin yerinde yapılmakta olduğunun farkında olmalıdır. Doğrulama sadece yasa ve düzenleme gereksinimlerine uygun yetkilendirme ile yapılmalıdır.

11.2.6 Teçhizat ve kuruluş dışındaki varlıkların güvenliği

Kontrol
Kuruluş dışındaki varlıklara, kuruluş yerleşkesi dışında çalışmanın farklı riskleri de göz önünde bulundurularak güvenlik uygulanmalıdır.

Uygulama kılavuzu
Kuruluşun dışındaki herhangi bir bilgi depolama ve işleme teçhizatlarının kullanımı, yönetim tarafından yetkilendirilmiş olmalıdır. Bu uygulama kuruluşa ait teçhizatlar da, kişiye ait teçhizatlar da ve kuruluş adına kullanılan teçhizatlar da geçerlidir.

Kuruluş dışında çalışan teçhizatların korunması için aşağıdaki hususlar dikkate alınmalıdır:

a) Kuruluş dışındaki teçhizat ve medyalar kamuya açık yerlerde gözetimsiz bırakılmamalıdır,
b) Teçhizatı korumak için üreticinin talimatlarına her zaman dikkat edilmelidir; örneğin, güçlü elektromanyetik alanlara maruz kalmaya karşı koruma,
c) Lokasyon dışı (evde çalışma, uzaktan çalışma ve geçici alanlar gibi) için kontroller, risk değerlendirmesi ile tespit edilmelidir ve uygun kontroller uygulanmalıdır, örneğin kilitlenebilir dosya dolapları, temiz masa politikası, bilgisayarlar için erişim kontrolü ve ofis ile güvenli iletişim (Ayrıca bk. ISO/IEC 27033 [15] [16] [17] [18] [19]),
d) Kuruluş dışında kullanılan teçhizatlar, farklı bireyler ya da dış taraflar arasında transfer olduğunda, teçhizattan sorumlu olanların en azından isimleri ve kuruluşlarını da içeren kayıt tutulmalıdır.

Hasar, hırsızlık veya dinlemeler gibi riskler bölgeler arasında önemli ölçüde değişebilir ve en uygun kontrollerin belirlenmesinde bu riskler dikkate alınmalıdır.

Diğer bilgiler
Bilgi depolama ve işleme teçhizatlarının ev çalışması için tutulması veya normal çalışma bölgesinden uzağa taşınması bütün formları (kişisel bilgisayarlar, ajandalar, mobil telefonlar, akıllı kartlar, kâğıt ve diğer formlar) içerir.

Mobil teçhizatları korumanın diğer yönleri hakkında daha fazla bilgi Madde 6.2'de bulunabilir.

Alan dışı çalışma ya da mobil BT ekipmanlarının kullanımının kısıtlanması ile çalışanların caydırmak için uygun olabilir.

11.2.7 Teçhizatın güvenli olarak yok edilmesi veya tekrar kullanımı

Kontrol
Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımdan önce tüm hassas verilerin ve lisanslı yazılımların kaldırılmasını veya güvenli bir şekilde üzerine yazılmasını temin etmek amacıyla doğrulanmalıdır.

Uygulama kılavuzu
Teçhizatlar, depolama ortamı içeriği yok edilmeden veya tekrar kullanılmadan önce doğrulanmalıdır.

Gizli ya da telif hakkı bilgileri saklanan ortamlar fiziksel olarak yok edilmelidir veya bilgi yok edilmelidir. Bilgi yok edilmesi, standart silme veya format işlevi kullanmak yerine bilginin tekrar elde edilememesi için silme veya yazma teknikleri kullanılarak yapılmalıdır.
Diğer bilgiler
Hassas verileri içeren hasarlı ortamlar onarım için gönderilmeden veya atılmadan önce fiziksel olarak imha edilmelidir, hasarlı cihazların hassas veriler içerip içermediğini belirlemek için bir risk değerlendirmesi gerekebilir. Bilgi, teçhizatın yeniden kullanımı veya dikkatsiz imhası nedeniyle tehlikeye girebilir.

Güvenli disk silmeye ek olarak, tüm diski şifreleme gizli bilgilerin açıklanması riskini azaltır, ekipman imha edildiğinde ya da yeniden düzenlendiğinde aşağıdaki hususları sağlamalıdır:

a) Şifreleme sürecinin yeterince güçlü olması ve tüm diski kapsaması (bellek boşluğu, getir götür kütüğü gibiler dâhil),
b) Şifreleme anahtarları kaba kuvvet saldırısına direnecek kadar uzun olması,
c) Şifreleme anahtarlarının kendilerini gizli tutması (örneğin; aynı disk üzerinde depolanmamış olması)

Şifreleme ile ilgili öneriler için Madde 10'a bakılmalıdır.

Depolama ortamı üzerine güvenli yazma için teknikler depolama ortamı teknolojilerine göre farklılık gösterir. Üzerine yazma araçları, depolama ortam teknolojisi için uygulanabilir olduğundan emin olmak amacıyla gözden geçirilmelidir.

11.2.8 Gözetimsiz kullanıcı teçhizatı

Kontrol
Kullanıcılar, gözetimsiz teçhizatın uygun şekilde korunmasını temin etmelidir.

Uygulama kılavuzu
Gözetimsiz teçhizatın korunması amacıyla, tüm kullanıcılar güvenlik gereksinimlerinin ve prosedürlerinin farkında olmalıdır, buna ek olarak kullanıcılar sorumluluklarının farkında olmalıdır.

Kullanıcılara aşağıdaki tavsiyelere uymaları önerilir:

a) Uygun kilitleme mekanizması (parola korumalı ekran koruyucu gibi) ile korunmadığı sürece etkin oturumlar bittiğinde oturumu kapatma,
b) Görev tamamlandıktan sonra uygulamalarda ya da ağ hizmetlerinde oturumu kapatma,
c) Bir tuş kilidi veya benzeri kontrol ile bilgisayar ve mobil cihazları yetkisiz kullanımdan koruma; örneğin, kullanım dışında erişim parolası.

11.2.9 Temiz masa ve temiz ekran politikası

Kontrol
Kâğıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme tesisleri için bir temiz ekran politikası benimsenmelidir.

Uygulama kılavuzu
Temiz masa ve temiz ekran politikasında, bilgi sınıflandırmaları (bk. Madde 8.2), yasal ve sözleşme gereksinimleri (bk. Madde 18.1) ve ilgili riskleri, kuruluşun kültürel konuları dikkate alınmalıdır. Aşağıdaki hususlar dikkate alınmalıdır:

a) Hassas veya kritik iş bilgileri; örneğin, kâğıt üzerinde veya elektronik depolama ortamlarında bulunan bilgi, özellikle ofisin boşalması halinde, gerekmediği zaman kilit altında (kasada, kabinette veya güvenlik mobilyalarının diğer formlarında) olmalıdır,
b) Bilgisayarlar ve terminaller, gözetimsiz bırakıldığında kapatılmalı ya da parolalar, token ve benzeri kullanıcı kimlik doğrulama mekanizmalarınca kontrol edilen ekran ve tuş kilidi mekanizmaları ile korunmalıdır, bilgisayarlar ve terminaller kullanımda olmadıkları durumlarda tuş kilitleri, parolalar veya diğer kontroller ile korunmalıdır,
c) Fotokopi ve diğer çoğaltma teknolojilerinin (örneğin; tarayıcı, sayısal kameralar) yetkisiz kullanımı önlenmelidir,
d) Hassas ve sınıflandırılmış bilgi içeren ortamlardaki bilgiler yazıcıdan çıktı alındıktan hemen sonra silinmelidir.

Diğer bilgiler
Temiz masa/temiz ekran politikası, normal çalışma saatlerinde ve dışında yetkisiz erişimi, bilginin hasar görmesi ve kaybı riskini azaltır. Kasalar ve bilgi saklama tesislerinin diğer formları içlerinde sakladıkları bilgiyi yangın, deprem, sel ve patlama gibi afetlerden koruyabilir.

Yazıcılarda pin kodu fonksiyonunun kullanımına dikkat edilmelidir, böylece sadece yazıcının yanında duran ve çıktı sahibi olan, yazıcı çıktısını alabilir.

12 İşletim güvenliği

12.1 İşletim prosedürleri ve sorumlulukları

Amaç: Bilgi işleme tesislerinin doğru ve güvenli işletimlerini temin etmek.

12.1.1 Yazılı işletim prosedürleri

Kontrol
İşletim prosedürleri yazılı hale getirilmeli ve ihtiyacı olan tüm kullanıcılara sağlanmalıdır.

Uygulama kılavuzu
Bilgisayar açma ve kapama, yedekleme, teçhizat bakımı, ortam işleme, bilgisayar odası ve elektronik posta işleme yönetimi ve güvenlik prosedürleri gibi bilgi işleme ve iletişim araçları ile ilişkili işletim faaliyetleri için yazılı prosedürler hazırlanmalıdır.

İşletim prosedürleri aşağıdakileri içeren belirli talimatları içermelidir:

a) Sistemin kurulumu ve yapılandırılması,
b) Hem otomatik hem de elle bilgi işleme ve işletimi,
c) Yedekleme (bk. Madde 12.3),
d) Diğer sistemler ile karşılıklı bağımlılıklar da dâhil en erken işe başlama ve en geç işi bitirme zamanlarını içeren zamanlama gereksinimleri,
e) Sistem destek programlarının kullanımı ile ilgili kısıtlamalar dâhil olmak üzere iş yürütme esnasında ortaya çıkabilecek işleme hataları ve diğer istisnai durumlar için talimatlar (bk. Madde 9.4.4),
f) Beklenmeyen işletimsel ya da teknik zorluk olaylarında dış destek iletişimini de içeren destek ve yükseltme (escalation) kişilerinin iletişim bilgileri,
g) Özel yazı malzemesi kullanımı veya başarısız işlerin çıktılarının güvenli imhası için prosedürlerde dâhil olmak üzere gizli çıktı yönetimi gibi özel çıktı ve ortam işleme talimatı (bk. Madde 8.3 ve Madde 11.2.7),
h) Sistemde arıza meydana geldiğinde kullanmak üzere sistemi yeniden başlatma ve kurtarma prosedürleri,
i) Sistem kayıt bilgileri ve denetim takibi yönetimi (Madde 12.4).
j) Prosedürlerin izlenmesi.

İşletim prosedürleri ve sistem faaliyetleri için prosedürlerin yazılı hali resmi olarak kabul edilmeli ve yetkili yönetim tarafından değişiklikler yapılabilmelidir. Teknik olarak mümkün olan durumlarda bilgi sistemleri aynı prosedürler, araçlar ve yardımcı programlar kullanılarak sürekli olarak yönetilmelidir.

12.1.2 Değişiklik yönetimi

Kontrol
Bilgi güvenliğini etkileyen, kuruluş iş prosesleri, bilgi işleme tesisleri ve sistemlerdeki değişiklikler kontrol edilmelidir.

Uygulama kılavuzu
Aşağıdaki hususlar dikkate alınmalıdır:

a) Önemli değişikliklerin tanımlanması ve kaydedilmesi,
b) Değişikliklerin planlanması ve test edilmesi,
c) Değişikliklerin bilgi güvenliği etkileri de dâhil potansiyel etkilerinin değerlendirilmesi,
d) Önerilen değişiklikler için resmi onay prosedürleri,
e) Bilgi güvenliği gereksinimlerinin karşılandığının doğrulanması,
f) İlgili tüm personele değişiklik detaylarının bildirilmesi,
g) Başarısız değişikliklerin ve öngörülmeyen olayların onarılması ya da sona erdirilmesi için prosedürler ve sorumluluklar da dâhil geri dönüş prosedürleri,
h) Bir olayı çözmek için gerekli değişikliklerin hızlı ve kontrollü uygulanmasını sağlamak için bir acil değişim sürecinin sağlanması (bk. Madde 16.1).

Resmi yönetim sorumlulukları ve prosedürleri tüm değişikliklerin tatmin edici bir şekilde kontrolünü sağlayan bir şekilde olmalıdır. Değişiklikler yapıldığında ilgili tüm bilgileri içeren denetim kayıtları tutulmalıdır.

Diğer bilgiler
Bilgi işleme tesislerindeki ve sistemlerindeki değişikliklerin yetersiz kontrolü, sistem veya güvenlik hatalarına neden olabilir. İşletim ortamındaki değişiklikler, özellikle de bir sistemin geliştirme ortamından işletme ortamına aktarımında değişiklikler uygulamaların güvenilirliğine etki edebilir (bk. Madde 14.2.2).

12.1.3 Kapasite yönetimi

Kontrol
Kaynakların kullanımı izlenmeli, ayarlanmalı ve gerekli sistem performansını temin etmek için gelecekteki kapasite gereksinimleri ile ilgili kestirimler yapılmalıdır.

Uygulama kılavuzu
Kapasite gereksinimleri söz konusu sistemin iş kritikliği dikkate alınarak belirlenmelidir. Sistemi ayarlama ve izleme, gerekli hallerde, sistemlerin kullanılabilirliğini ve verimliliğini artırmak için uygulanmalıdır. Tarama kontrolleri zamanında sorunları tespit etmek için yerinde yapılmalıdır. Gelecekteki kapasite gereksinimlerinin kestirimleri, yeni iş ve sistem gereksinimlerini ve kuruluşun bilgi işleme yeteneklerinde mevcut ve öngörülen eğilimlerini dikkate almalıdır.

Uzun tedarik sürelerine ve yüksek maliyetlere sahip kaynaklar için özel ilgi gerekir. Bu nedenle yöneticiler anahtar sistem kaynaklarının kullanımını izlemelidir. Yöneticiler, özellikle iş uygulamaları ve yönetim bilgi sistemi araçları ile ilgili olarak kullanım eğilimlerini belirlemeledir.

Yöneticiler, sistem güvenliği veya hizmetleri için bir tehdit sunan kilit personelin üzerindeki darboğazları ve bağımlılığı belirlemek ve önlemek için bu bilgileri kullanmalı ve uygun eylem planlarını yapmalıdır.

Yeterli kapasitenin sağlanması, kapasite arttırılarak ya da talep azaltılarak elde edilebilir. Kapasite talep yönetim örnekleri aşağıdaki hususları içerir:

a) Kullanılmayan verinin silinmesi (disk alanı),
b) Uygulamaların, sistemlerin, veri tabanlarının ya da ortamların hizmetten çıkarılması,
c) Toplu proseslerin ve zamanlamaların optimizesi,
d) Uygulama mantığının ya da veri tabanı sorgularının optimize edilmesi,
e) Eğer iş kritik değilse kaynak tüketen hizmetler için reddetme ya da bant genişliği sınırlaması (örneğin; video akışları)

Yazılı hale getirilmiş kapasite yönetim planı kritik sistemler için düşünülmelidir.

Diğer bilgiler
Bu kontrol insan kaynakları kapasitesinin yanı sıra ofis ve tesisleri de ele alır.

12.1.4 Geliştirme, test ve işletim ortamlarının birbirinden ayrılması

Kontrol
Geliştirme, test ve işletim ortamları, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmalıdır.

Uygulama kılavuzu
İşletimsel sorunları önlemek için gerekli olan işletim, test ve geliştirme ortamları arasında bir ayrım seviyesi tanımlanmalı ve uygulanmalıdır.

Aşağıdaki hususlar dikkate alınmalıdır:

a) Geliştirmeden işletim durumuna yazılımın transferi için kurallar tanımlanmalı ve yazılı hale getirilmelidir,

b) Geliştirme ve işletim yazılımı, farklı etki alanlarında veya dizinlerde, farklı sistem ve bilgisayar işlemcilerinde çalışmalıdır,
c) İşletimdeki sistemlerin ve uygulamalarının değişiklikleri işletimdeki sistemlere uygulanmadan önce test ya da hazırlama ortamında test edilmelidir,
d) İstisnai durumlar dışında, testler işletimdeki sistemler üzerinde yapılmamalıdır,
e) Derleyiciler, editörler ve diğer geliştirme araçları veya sistem programları istenilmediği zaman işletimdeki sistemden erişilebilir olmamalıdır,
f) Kullanıcılar, işletim ve test sistemi için farklı kullanıcı profilleri kullanmalıdır ve menüler hata riskini azaltmak için uygun kimlik doğrulama mesajlarını göstermelidir,
g) Hassas veriler, test sistemi için eşdeğer kontroller sağlanmadan test sistemi ortamlarına kopyalanmamalıdır (bk. Madde 14.3).

Diğer bilgiler
Geliştirme ve test faaliyetleri, sistem hatası ya da dosya veya sistem ortamlarında istenmeyen değişiklikler gibi ciddi sorunlara neden olabilir. Bilinen ve istikrarlı bir ortam sağlamak için testleri anlamlı geliştirmeye ve çalışma ortamına uygunsuz geliştirici erişimini engellemeye ihtiyaç vardır.

Geliştirme ve test personelinin işletim sistemi ve bilgilerine erişiminin olduğu yerde, bu personel yetkilendirilmemiş ve test edilmemiş kodu siteme ekleyebilir veya işletim verilerini değiştirebilir. Bazı sistemlerde bu özellik, ciddi işletimsel sorunlara neden olabilecek sahtekârlık yapma ya da test edilmemiş veya kötü amaçlı kodun sisteme eklenmesi şeklinde hatalı kullanıma neden olabilir.

Geliştirme ve test personelleri, aynı zamanda işlemsel bilgilerin gizliliği için bir tehdit oluşturmaktadır. Geliştirme ve test faaliyetleri, aynı işlem ortamını paylaşıyorsa yazılım ve bilgide istenmeyen değişikliklere neden olabilir. Geliştirme, test ve işletim çevrelerinin ayrımı, iş verileri ve işletim yazılımlarına yetkisiz erişimi engellemek veya kazara değiştirme riskini azaltmak için istenilir (Test verilerinin korunması için bk. Madde 14.3).

12.2 Kötücül yazılımlardan koruma

Amaç: Bilgi ve bilgi işleme tesislerinin kötücül yazılımlardan korunmasını temin etmek.

12.2.1 Kötücül yazılımlara karşı kontroller

Kontrol
Kötücül yazılımlardan korunmak için tespit etme, engelleme ve kurtarma kontrolleri uygun kullanıcı farkındalığı ile birlikte uygulanmalıdır.

Uygulama kılavuzu
Kötücül yazılıma karşı koruma; kötücül yazılım kod tespitine ve yazılım onarımına, güvenlik bilincine ve uygun sistem erişim ve değişim yönetimi kontrollerine dayanmalıdır. Aşağıdaki hususlar dikkate alınmalıdır:

a) Yetkisiz yazılım kullanımını yasaklayan resmi bir politika kurulması (bk. Madde 12.6.2 ve Madde 14.2),
b) Yetkisiz yazılım kullanımını tespit etmek ya da önlemek için kontrollerin uygulanması (örneğin; beyaz liste uygulaması),
c) Bilinen ya da şüphelenilen kötücül web sitelerini tespit etmek ve önlemek için kontrollerin uygulanması (örneğin; kara liste uygulaması).
d) Özel koruma gerektiren kısımlar, gerekli korumanın genel seviyesini azaltmak için ayrıca korunaklı olmalıdır,
e) Kontroller, çevresel tehditleri ve potansiyel fiziksel riskleri en aza indirgemek için kabul edilmelidir, örneğin; hırsızlık, yangın, patlayıcı madde, duman, su (ya da su kesintisi), toz, titreşim, kimyasal etkiler, elektrik kaynağı girişimi, haberleşme girişimi, elektromanyetik radyasyon ve vandalizm,
f) Kritik iş proseslerini destekleyen sistemlerin yazılım ve veri içeriğinin düzenli olarak gözden geçirilmesi; onaylanmamış dosyaların ve yetkisiz değişikliklerin olması durumunda resmi olarak araştırılması;
g) Önceden alınan bir tedbir olarak ya da rutin bir esasa bağlanarak, bilgisayarların taranması için kötücül yazılım tespitinin kurulumu, düzenli güncellenmesi ve yazılımın onarılması, buradaki bahsedilen tarama aşağıdaki hususları içermelidir;

h) Sistemin kötücül yazılıma karşı korunması ile ilgili yönetim prosedürleri ve sorumlulukların tanımlanması, bu prosedür ve sorumlulukların kullanımı konusunda eğitim verilmesi, kötücül yazılım saldırılara karşı kurtarma ve raporlama faaliyetlerinin tanımlanması,
i) Kötücül yazılım saldırılarından korunmak için gerekli tüm veri ve yazılım yedekleme ve kurtarma düzenlemeleri dâhil olmak üzere uygun iş sürekliliği planlarını hazırlanması (bk. Madde 12.3),
j) Yeni kötücül yazılımlar ile ilgili bilgi veren doğrulama web siteleri ve/veya e-posta listeleri gibi yerlerden düzenli bilgi toplamak için prosedürlerin uygulanması,

Diğer bilgiler
Farklı tedarikçilerden ve teknolojilerden bilgi işleme çevrelerini zararlı kodlara karşı koruyan iki veya daha fazla yazılım ürünlerinin kullanımı kötücül yazılım koruması etkinliğini arttırabilir.

Bakım ve acil durum prosedürleri sırasında normal kötücül yazılım koruması kontrolleri devre dışı olabileceğinden kötücül yazılım girişine karşı korunmak için dikkat edilmelidir.

Belirli koşular altında, kötücül yazılıma karşı koruma işletimde bozulmalara neden olabilir.

Kötü amaçlı yazılım kontrolü için kullanılan yazılım, kötücül yazılım tespitinde ve onarımında genellikle yeterli değildir ve kötücül yazılım girişini önlemek için işletim prosedürleri ile birlikte kullanılmalıdır.

12.3 Yedekleme

Amaç: Veri kaybına karşı koruma sağlamak.

12.3.1 Bilgi yedekleme

Kontrol
Bilgi, yazılım ve sistem imajlarının yedekleme kopyaları alınmalı ve üzerinde anlaşılmış bir yedekleme politikası doğrultusunda düzenli olarak test edilmelidir.

Uygulama kılavuzu
Yedekleme politikası, bilgi, yazılım ve sistemlerin yedeklenmesi için kuruluş gereksinimlerini tanımlamak amacıyla oluşturulmalıdır.

Yedekleme politikası, saklama ve koruma gereklerini tanımlamalıdır.

Yeterli yedekleme tesisleri, bir felaket veya ortam hatasından sonra gerekli tüm bilgi ve yazılımın telafi edilebilir olmasından emin olmak için sağlanmalıdır.

Yedekleme planı tasarlanırken aşağıdaki öğeler dikkate alınmalıdır:

a) Yedekleme kopyaları ve restorasyon prosedürlerinin dokümantasyonunun tam ve doğru kaydı üretilmelidir,
b) Yedeklerin türü (örneğin; tam veya diferansiyel yedekleme) ve sıklığının kuruluşun iş gereksinimlerini, ilgili bilgilerin güvenlik gereksinimlerini ve kuruluşun sürekli çalışması için bilginin kritikliğini yansıtması gerekir,
c) Yedeklemeler, merkezde bir felaketten dolayı görülecek hasardan kaçınmak için yeterli bir mesafede olan uzak bir yerde muhafaza edilmelidir,
d) Yedekleme bilgileri, merkezinde uygulanan standartlara uygun fiziksel ve çevresel koruma (bk. Madde 11) düzeyine uygun olarak korunmalıdır;
e) Yedekleme ortamı, acil durumlarda kullanmak gerektiğinde güvenerek kullanmak için düzenli aralıklar ile test edilmelidir; bu ortam geri yükleme prosedürlerinin testi ve geri yükleme zamanı gerekliliğine karşı kontrol ile kombine edilmelidir. Yedeklenen verilerin geri yüklenme yeteneği testi özel test ortamında yapılmalıdır, orijinal ortamlarda yedekleme ya da geri yükleme sürecinin başarısız olması durumunda onarılamaz veri kaybına ya da hasarına neden olacağından orijinal ortamında yapılmamalıdır,
f) Gizliliğin önemli olduğu durumlarda, yedeklemenin şifreleme yoluyla korunması gerekir.

İşletimsel prosedürler, yedekleme politikasına göre yedeklemenin tamamlanmasını sağlamak için yedeklemenin yürütülmesini izlemeli ve zamanlanmış yedekleme başarısızlıkları ele alınmalıdır.

Bireysel sistemler ve hizmetler için yedekleme düzenlemeleri, iş sürekliliği planlarının gereksinimlerini sağladığından emin olmak için düzenli olarak test edilmelidir. Kritik sistemler ve hizmetlerde yedekleme düzenlemeleri bir felaket durumunda komple sistemi kurtarmak için tüm bilgi sistemlerini, uygulamaları ve gerekli verileri içermelidir.

Gerekli iş bilgileri için saklama süresi, arşiv kopyalarının kalıcı muhafaza edilmesi için gereksinimler dikkate alınarak tespit edilmelidir.

12.4 Kaydetme ve izleme

Amaç: Olayları kaydetmek ve kanıt üretmek.

12.4.1 Olay kaydetme

Kontrol
Kullanıcı faaliyetleri, istisnai durumlar, hatalar ve bilgi güvenliği olaylarını kaydeden olay kayıtları üretilmeli, saklanmalı ve düzenli olarak gözden geçirilmelidir.

Uygulama kılavuzu
Olay kayıtları ilgili olduğunda aşağıdaki hususları içermelidir:

a) Kullanıcı kimlikleri,
b) Sistem faaliyetleri,
c) Oturum açma ve oturum kapatma gibi anahtar olayların tarihleri, saatleri ve detayları,
d) Mümkünse aygıt kimliği ya da yeri ve sistem tanımlayıcısı,
e) Başarılı ve reddedilmiş, sistem erişim girişimlerinin kayıtları,
f) Başarılı ve reddedilmiş, veri ve diğer kaynaklara erişim girişimlerinin kayıtları,
g) Sistem yapılandırma değişiklikleri,
h) Ayrıcalıkların kullanımı,
i) Sistem araçları ve uygulamalarının kullanımı,
j) Erişilen dosyalar ve erişim türü,
k) Ağ adresi ve protokolleri,
l) Erişim kontrol sistemi tarafından üretilen alarmlar,
m) Anti-virüs sistemleri ve saldırı tespit sistemleri gibi koruma sistemlerinin etkinleştirilmesi ve devre dışı bırakılması,
n) Uygulamalarda kullanıcılar tarafından yürütülen işlemlerin kayıtları.

Olay kayıtları, sistem güvenliği hakkında konsolide raporlar ve alarmlar üretme yeteneğine sahip otomatik izleme sistemleri için temel oluşturur.

Diğer bilgiler
Olay kayıtları, hassas veri ve kişisel kimlik bilgilerini içerebilir. Uygun gizlilik koruma önlemleri alınmalıdır (bk. Madde 18.1.4).

Mümkünse, sistem yöneticilerinin kendi faaliyetlerinin kayıtlarını kapatmaları veya silmeleri engellenmelidir (bk. Madde 12.4.3).

12.4.2 Kayıt bilgisinin korunması

Kontrol
Kaydetme tesisleri ve kayıt bilgileri kurcalama ve yetkisiz erişime karşı korunmalıdır.

Uygulama kılavuzu
Aşağıdakiler dâhil olmak üzere, kayıt tesisleri ile kayıt bilgilerinin ve işletimsel problemlerin yetkisiz değiştirmeye karşı korunması için kontroller amaçlanmalıdır:

a) Kaydedilen mesaj türlerinde değişimler,
b) Kayıt dosyalarının düzenlenmesi ya da silinmesi,
c) Kayıt dosyası depolama kapasitesinin aşılması. Bu durumda olayların kaydedilmesi gerçekleştirilemez ya da daha önceden kaydedilen olayların üzerine yazma işleminin gerçekleşmesi.

Bazı denetim kayıtlarının, kayıt tutma politikasının bir parçası olarak ya da kanıt toplama ve koruma gereksinimleri nedeniyle arşivlenmesi gerekli olabilir (bk. Madde 16.1.7).

Diğer bilgiler
Sistem kayıtları genellikle güvenlik izlemesi için gereksiz olan büyük hacimli bilgi içerir. Bilgi güvenliğini izleme amacıyla önemli olayların tanımlanmasına yardımcı olmak için, bir ikinci kayıt bölümüne uygun mesaj türleri otomatik olarak kopyalanır ve/veya uygun sistem bileşenleri kullanılır ya da dosya sorgulama ve akıcılığını gerçekleştirmek için denetim araçları dikkate alınır.

Sistem kayıtlarının korunması gerekir, çünkü veri değiştirilebilir ya da veri silinebilir, bu olayların olması yanlış bir güvenlik duygusu oluşturabilir. Bir sistem yöneticisi ya da operatörünün kontrolü dışında bir sisteme kayıtların gerçek zamanlı kopyalanması kayıtları korumak için kullanılabilir.

12.4.3 Yönetici ve operatör kayıt kayıtları

Kontrol
Sistem yöneticileri ve sistem operatörlerinin faaliyetleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.

Uygulama kılavuzu
Ayrıcalıklı kullanıcı hesabı sahiplerinin, kendilerinin doğrudan kontrolü altında bulunan bilgi işleme tesislerinin kayıtlarını işlemeleri mümkün olabilir, bu nedenle ayrıcalıklı kullanıcılar için hesap verilebilirliği sağlamak amacıyla kayıtların korunması ve gözden geçirilmesi gerekmektedir.

Diğer bilgiler
Sistem ve ağ yöneticisinin kontrolü dışında yönetilen saldırı tespit sistemi, uyum için sistem ve ağ yönetim faaliyetlerinin izlenmesinde kullanabilir.

12.4.4 Saat senkronizasyonu

Kontrol
Bir kuruluş veya güvenlik alanında yer alan tüm ilgili bilgi işleme sistemlerinin saatleri tek bir referans zaman kaynağına göre senkronize edilmelidir.

Uygulama kılavuzu
Zaman gösterimi, senkronizasyon ve doğruluk için dış ve iç gereksinimler yazılı hale getirilmelidir. Bu gereksinimler, yasal, düzenleyici, sözleşeme gereksinimleri, standartlara uygunluk ya da iç izleme için gereksinimler olabilir. Kuruluş içinde kullanılmak üzere bir standart zaman belirlenmelidir.

Kuruluş dış kaynak(lar)dan bir referans zamanı elde etmek için yaklaşımı ve dâhili saatlerin güvenilir bir şekilde nasıl senkronize olacağını yazılı hale getirmeli ve uygulanmalıdır.
Diğer bilgiler
Bilgisayar saatlerinin doğru ayarı, denetim kayıtlarının doğruluğunu sağlamak için önemlidir. Bu kayıtlar incelemeler ya da yasal ya da disiplin durumlarında kanıt olarak istenebilir. Yanlış denetim kayıtları bu tür incelemelerin yapılmasına engel olur ve böyle kanıtların güvenilirliğine zarar verir. Milli atomik saat tarafından yayınlanan radyo zamanı ile bağlantılı bir saat, kayıt sistemleri için ana saat olarak kullanılabilir. Bir ağ zaman protokolü tüm sunucuları ana saat ile senkronize tutmak için kullanılabilir.

12.5 İşletimsel yazılımın kontrolü

Amaç: İşletimdeki sistemlerin bütünlüğünü temin etmek.

12.5.1 İşletimdeki sistemler üzerine yazılım kurulumu

Kontrol
İşletimdeki sistemler üzerine yazılım kurulumunun kontrolü için prosedürler uygulanmalıdır.

Uygulama kılavuzu
İşletimdeki sistemlerde yazılım değişimi kontrolünde aşağıdaki hususlara dikkat edilmelidir:

a) İşletimsel sistem yazılımının, uygulamaların ve program kütüphanelerinin güncellenmesi yalnız uygun yönetim yetkilendirmesi ile tayin edilen yönetici tarafından gerçekleştirilmelidir (bk. Madde 9.4.5),
b) İşletimdeki sistemlerde sadece çalıştırılabilir onaylı kod bulunmalıdır, geliştirme kodu ya da derleyiciler olmamalıdır,
c) Uygulama ve işletimsel sistem yazılımları sadece kapsamlı ve başarılı bir şekilde test edildikten sonra uygulanmalıdır; testler, kullanılabilirliği, güvenliği, diğer sistemlere etkiyi ve kullanıcı dostluğunu kapsamalıdır ve ayrı sistemler üzerinde yapılmalıdır (bk. Madde 12.1.4); bu testler ile ilgili program kaynak kütüphanelerinin güncellenmesi sağlanmalıdır,
d) Bir yapılandırma kontrol sistemi, sistem dokümantasyonu da dâhil olmak üzere tüm uygulanan yazılımları kontrol altında tutmak için kullanılmalıdır,
e) Değişiklikleri uygulamadan önce bir geri alma stratejisi olmalıdır,
f) İşletimsel program kütüphanelerinin tüm güncellemelerinin bir denetim kaydı tutulmalıdır,
g) Uygulama yazılımının önceki sürümleri bir acil durum önlemi olarak saklanmalıdır,
h) Yazılımının eski sürümleri tüm gerekli bilgi, parametreler, prosedürler, yapılandırma detayları ve destekleyen yazılım ile birlikte veriler arşivde tutulabildiği sürece saklanmalıdır.

İşletimdeki sistemlerde tedarikçi tarafından sağlanan yazılım kullanımı, tedarikçi tarafından desteklenen bir seviyede sürdürülmelidir. Zamanla, yazılım tedarikçileri tarafından sağlanan destek yazılımın eski sürümleri için sona erecektir. Kuruluş, desteklenmeyen yazılımlara dayanan risklere dikkat etmelidir.

Yeni bir sürüme yükseltme kararı alındığında değişim için iş gereksinimleri ve sürüm güvenliği dikkate alınmalıdır. Örneğin; yeni bilgi güvenliği işlevleri tanıtımı ya da bu sürümü etkileyen bilgi güvenliği problemlerinin sayısı ve şiddeti. Bilgi güvenliği açıklıklarının azaltmasına ya da kaldırılmasına yardımcı olmak için yazılım yamaları uygulanmalıdır (ayrıca, bk. Madde 12.6).
Tedarikçilere fiziksel ya da mantıksal erişim, gerektiğinde yalnızca destek amacıyla ve yönetimin onayı ile verilmelidir. Tedarikçinin faaliyetleri izlenmelidir (bk. Madde 15.2.1).

Bilgisayar yazılımı, dış sağlanan yazılım ve modüllere temel alıyor olabilir. Ancak, yetkisiz değişiklikleri önlemek için bu yazılım ve modüller güvenlik açıklıkları oluşturabileceğinden izlenmeli ve kontrol edilmelidir.

12.6 Tekniklik açıklıkların yönetilmesi

Amaç: Teknik açıklıklardan yararlanılmasını engellemek.

12.6.1 Teknik açıklıkların yönetimi

Kontrol
Kullanılmakta olan bilgi sistemlerinin teknik açıklıklarına dair bilgi, zamanında elde edilmelidir. Kuruluşun bu tür açıklıklara karşı zafiyeti değerlendirilmeli ve ilgili riskin ele alınması için uygun tedbirler alınmalıdır.

Uygulama kılavuzu
Varlıkların güncel ve eksiksiz envanteri (bk. Madde 8) etkili teknik açıklıkların yönetilmesi için bir önkoşuldur. Teknik açıklıkların yönetilmesini desteklemek için gerekli özel bilgiler; yazılım tedarikçisini, sürüm numarasını, dağıtımın mevcut durumunu (örneğin; yazılımın hangi sistemlere hangi yazılımların kurulduğu gibi) ve yazılım için kuruluş içindeki sorumlu kişiyi/kişileri içerir.

Olası teknik güvenlik açıklılarının belirlenmesinden sonra uygun ve zamanında aksiyon alınmalıdır. Aşağıdaki kılavuzluk teknik güvenlik açıklıkları için etkili bir yönetim süreci kurmak amacıyla takip edilmelidir:

a) Kuruluş; izleme, açıklık, risk değerlendirmesi, yama, varlık izleme ve her türlü koordinasyon görevleri de dâhil olmak üzere teknik açıklıkların yönetilmesi ile ilişkili rolleri ve sorumlulukları tanımlamalı ve kurmalıdır,
b) İlgili teknik güvenlik açıklıklarını belirlemek ve onlar hakkında farkındalığı korumak için kullanılacak bilgi kaynakları, yazılım ve diğer teknolojiler için tanımlanmalıdır (varlık envanteri listesi taban alınarak, bk. Madde 8.1.1); bu bilgi kaynakları, envanter değişiklikleri ya da diğer yeni veya faydalı kaynaklar temel alınarak güncellenmelidir,
c) Olası ilgili teknik açıklıklar hakkında uyarılara tepki göstermek için bir zaman çizelgesi tanımlanmalıdır,
d) Olası teknik açıklıkların belirlenmesinden sonra kuruluş ilişkili riskleri ve alınması gereken eylemleri tanımlamalıdır; eylem, açığı olan sistemlere yama geçilmesi ve/veya diğer kontrollerin uygulanması olabilir,
e) Bir teknik güvenlik açığının ne kadar acil ele alınması gerekliliğine bağlı olarak, alınan eylem değişim yönetiminin ilgili kontrollerine uygun olarak yerine getirilmeli (bk. Madde 12.1.2) veya bilgi güvenliği olaylarına müdahale prosedürleri takip edilmelidir (bk. Madde 16.1.5),
f) Meşru kaynaklarda yayınlana bir yama varsa, yama yükleme ile ilgili riskler değerlendirilmelidir (yamanın yüklenmesi riski ile açıklığın oluşturduğu riskler karşılaştırılmalıdır),
g) Yamaların, etkinliğinden emin olmak ve geri dönülemez etkilerle sonuçlanmasından kaçınmak için kurulum öncesinde test edilip değerlendirilmesi gerekir, eğer yama yoksa aşağıdaki gibi diğer kontroller dikkate alınmalıdır;
    1) Açıklıkla ilgili hizmetlerin ya da özelliklerin kapatılması,
    2) Erişim kontrollerinin uyumlaştırılması ya da eklenmesi, örneğin; güvenlik duvarları, ağ sınır cihazları (bk. Madde 13.1),
    3) Gerçek saldırıların tespiti için izlemenin arttırılması,
    4) Güvenlik açığı hakkında farkındalığın arttırılması,
h) Gerçekleştirilen tüm prosedürler için bir denetim kaydı tutulmalıdır,
i) Teknik açıklık yönetim prosesinin etkinliğinden ve verimliliğinden emin olmak için proses düzenli olarak izlenmeli ve değerlendirilmelidir,
j) Yüksek riskli sistemler ilk önce ele alınmalıdır,
k) Açıklıklar hakkındaki verileri ihlal olayı tepki fonksiyonuna iletmek ve bir ihlal olayı meydana geldiğinde gerçekleştirilmesi gereken teknik prosedürleri sağlamak üzere; etkili bir teknik açıklık yönetim süreci, ihlal olayı yönetim faaliyetleri ile aynı doğrultuda olmalıdır,
l) Bir güvenlik açığı tespit edildiğinde ama uygun önlem olmadığında durumu çözmek için bir prosedür tanımlanmalıdır. Bu durumda, kuruluş bilinen güvenlik açıklıkları ile ilgili riskleri değerlendirmeli ve uygun tespit ve düzeltici eylemleri tanımlamalıdır.

Diğer bilgiler
Teknik açıklıkların yönetilmesi, değişim yönetiminin bir alt fonksiyonu olarak görülebilir ve bu gibi durumlarda değişim yönetimi proseslerinden ve prosedürlerinden yararlanılabilir (bk. Madde 12.1.2 ve Madde 14.2.2).

Tedarikçiler genellikle yamaları olabildiğince kısa sürede yayınlamaları konusunda baskı altındadırlar. Bu nedenle, bir yama sorunu çözemeyebilir ve olumsuz etkileri olabilir. Aynı zamanda, bazı durumlarda yama uygulandıktan sonra yamanın kaldırılması kolay olmayabilir.

Maliyet ya da kaynak eksikliği gibi nedenlerle yamaların yeterli testi mümkün değilse, diğer kullanıcılar tarafından bildirilen deneyime dayalı olarak ilgili risklerin değerlendirilmesi de dikkate alınarak yama belirli bir gecikme süresi ile uygulanabilir. ISO/IEC 27031 [14] kullanılması yararlı olabilir.

12.6.2 Yazılım kurulumu kısıtlamaları

Kontrol
Kullanıcılar tarafından yazılım kurulumuna dair kurallar oluşturulmalı ve uygulanmalıdır.

Uygulama kılavuzu
Kuruluş, kullanıcıların hangi yazılım türünü kurabileceğini katı bir politika ile tanımlamalı ve mecburi uygulamalıdır.

En az ayrıcalık ilkesi uygulanmalıdır. Bazı ayrıcalıklar verilirse kullanıcılar yazılım yüklemek için yetkili olabilir.

Kuruluş, izin verilen yazılım yüklemelerinin türünü (örneğin; mevcut yazılımların güvenlik yamaları ve güncellemeleri) ve hangi tür yüklemelerin yasak olduğunu (örneğin; potansiyel olarak kötü niyetli olma ile ilgili

kaynağı bilinmeyen ya da şüpheli olan yazılım ya da kişisel kullanım için olan yazılım) belirlemelidir. Bu ayrıcalıklar söz konusu kullanıcıların rolleri dikkate alınarak verilmelidir.

Diğer bilgiler
İşlem aygıtları üzerine yazılımların kontrolsüz kurulumu, açıkların gelmesine ve sonrasında bilgi sızıntısına, bütünlük kaybına ya da diğer bilgi güvenliği ihlal olaylarına ya da fikri mülkiyet haklarının ihlaline neden olabilir.

12.7 Bilgi sistemleri tetkik hususları

Amaç: Tetkik faaliyetlerinin işletimdeki sistemler üzerindeki etkilerini asgariye indirmek.

12.7.1 Bilgi sistemleri tetkik kontrolleri

Kontrol
İşletimdeki sistemlerin doğrulanmasını kapsayan tetkik gereksinimleri ve faaliyetleri, iş proseslerindeki kesintileri asgariye indirmek için dikkatlice planlanmalı ve üzerinde anlaşmaya varılmalıdır.

Uygulama kılavuzu
Aşağıdaki hususlara dikkat edilmelidir:

a) Sistemler ve veriye erişim için tetkik gereksinimleri konusunda ilgili yönetim ile mutabık olunmalıdır,
b) Teknik tetkik testlerinin kapsamına karar verilmeli ve kontrol edilmelidir,
c) Tetkik testleri, yazılım ve veriye sadece okunabilir erişim ile sınırlandırılmalıdır,
d) Sadece okunabilir erişim dışında kalan erişim, sistem dosyalarının yalıtılmış kopyalarına izin verilmelidir, bu kopyalar tetkik tamamlandığında silinmelidir ya da tetkik dokümantasyon şartları altında bu tür dosyaları tutmak için bir zorunluluk varsa uygun koruma sağlanmalıdır,
e) Özel ve ek bir işleme için gerekler tanımlanmalı ve kararlaştırılmalıdır,
f) Sistem erişilebilirliğini etkileyebilecek tetkik testleri mesai saatleri dışında çalıştırılmalıdır,
g) Tüm erişimler izlenmeli ve referans kaydı oluşturmak için kaydedilmelidir.

13 Haberleşme güvenliği

13.1 Ağ güvenliği yönetimi

Amaç: Ağdaki bilgi ve destekleyici bilgi işleme tesislerinin korunmasını sağlamak.

13.1.1 Ağ kontrolleri

Kontrol
Sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağlar yönetilmeli ve kontrol edilmelidir.

Uygulama kılavuzu
Ağlardaki bilginin güvenliğini ve yetkisiz erişimlerden ağa bağlı hizmetlerin korunmasını sağlamak için kontroller uygulanmalıdır. Özellikle, aşağıdaki hususlar dikkate alınmalıdır:

a) Ağ ekipmanlarının yönetimi için sorumluluklar ve prosedürler oluşturulmalıdır,
b) Ağlar için operasyonel sorumluluklar, uygun olduğu durumlarda bilgisayar işlemleri ayrılmalıdır (bk. Madde 6.1.2),
c) Halka açık ağlar veya kablosuz ağlar üzerinden geçen verilerin ve bağlı sistemler ile uygulamaların gizliliğini ve bütünlüğünü korumak için özel kontroller kurulmalıdır (bk. Madde 10 ve Madde 13.2), ağ hizmetlerinin ve bağlı bilgisayarların erişilebilirliğini sağlamak için özel kontroller gerekli olabilir,
d) Bilgi güvenliği ile ilgili olabilecek veya bilgi güvenliğini etkileyebilecek faaliyetlerin tespiti ya da kaydı için uygun günlük kaydetme ve izleme mekanizmaları oluşturulmalıdır,
e) Hem kuruluşa verilen hizmetlerin optimizasyonunu dağlamak hem de bilgi işleme altyapılarına uygulanan kontrollerin tutarlılığını sağlamak amacıyla yönetim faaliyetleri koordine edilmelidir,

f) Ağlardaki sistemlerde kimlik doğrulaması olmalıdır,
g) Sistemlerin ağa bağlantısı sınırlandırılmalıdır.

Diğer bilgiler
Ağ güvenliği hakkında ek bilgi ISO/IEC 27033 standardında bulunabilir. [15][16][17][18][19]

13.1.2 Ağ hizmetlerinin güvenliği

Kontrol
Tüm ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve yönetim gereksinimleri tespit edilmeli ve hizmetler kuruluş içinden veya dış kaynak yoluyla sağlanmış olsun olmasın, ağ hizmetleri anlaşmalarında yer almalıdır.

Uygulama kılavuzu
Ağ hizmet sağlayıcısının üzerinde anlaşmaya varılan hizmetleri güvenli bir şekilde yönetebilme yeteneği belirlenmeli ve düzenli olarak izlenmelidir. Ayrıca, denetim yetkisi üzerinde anlaşmaya varılmalıdır.

Güvenlik özellikleri, hizmet seviyesi ve yönetim gereksinimleri gibi özel hizmetler için gerekli güvenlik düzenlemeleri tanımlanmalıdır. Kuruluş, ağ hizmet sağlayıcısının bu önlemleri uyguladığından emin olmalıdır.

Diğer bilgiler
Ağ hizmetleri, bağlantıların sağlanmasını ve özel ağ hizmetlerini, katma değerli ağları ve saldırı tespit sistemleri ve güvenlik duvarı gibi ağ güvenlik çözümlerini içerir.

Bu hizmetler basit olarak bant genişliğinden karmaşık katma değerli önerilere kadar bir alana yayılabilir. Aşağıdakiler ağ hizmetleri güvenlik özellikleri olabilir:

a) Ağ hizmetlerinin güvenliği için kimlik doğrulama, şifreleme ve ağ bağlantısı kontrolleri gibi uygulanan teknolojiler,
b) Güvenlik ve ağ bağlantı kuralları ile uyumlu ağ hizmetleri ile güvenli bağlantı için gerekli teknik parametreler,
c) Gerektiğinde ağ hizmetlerine veya uygulamalarına erişimi kısıtlamak için ağ hizmetlerinin kullanım prosedürü.

13.1.3 Ağlarda ayrım

Kontrol
Ağlarda, bilgi hizmetleri, kullanıcılar ve bilgi sistemleri grupları ayrılmalıdır.

Uygulama kılavuzu
Geniş ağların güvenliğini yönetmenin bir yöntemi, söz konusu ağları ayrı ağ etki alanlarına bölmektir. Etki alanları; güven seviyelerine (örneğin; halka açık erişim etki alanı, masaüstü etki alanı, sunucu etki alanı), kuruluş birimlerine (örneğin; insan kaynakları, finans, pazarlama) veya bu ikisinin bazı kombinasyonlarına (örneğin; birden fazla kuruluş birimlerine bağlanan sunucu etki alanı) göre seçilebilir. Ayrım; farklı fiziksel ağlar kullanılarak veya farklı mantıksal ağlar (örneğin; sanal özel ağ) kullanılarak yapılabilir.

Her bir etki alanının sınırı iyi tanımlanmalıdır. Ağ etki alanları arasında erişime izin verilmelidir; Ancak, erişim etki alanları arasındaki sınırlarda bir ağ geçidi (örneğin; güvenlik duvarı, filtreleme yönlendiricisi) kullanılarak kontrol edilmelidir. Etki alanları içinde ağların ayrımı ve ağ geçitleri aracılığıyla izin verilen erişimin kriterleri, her bir etki alanının güvenlik gereksinimlerinin değerlendirmesine dayalı olmalıdır. Değerlendirme; erişim kontrol politikasına (bk. Madde 9.1.1), erişim gereksinimlerine, işlenin bilginin değer ve sınıflandırmasına uygun olmalı ve aynı zamanda uygun ağ geçidi teknolojisini içeren göreceli bir maliyet ve performans etkisini dikkate almalıdır.

Hassas ortamlar için tüm kablosuz erişimler harici bir bağlantı olarak ele alınmalı ve bu erişim ağ kontrol politikalarına (bk. Madde 13.1.1) göre ağ geçidinden geçene kadar ve dâhili sistemlere erişim hakkı verilmeden önce bu erişim iç ağlardan ayrılmalıdır.

Modern, standartlara dayalı kablosuz ağların kimlik doğrulama, şifreleme ve kullanıcı seviyesinde ağ erişim kontrolü teknolojileri, düzgün bir şekilde uygulandığı zaman kuruluşun iç ağına doğrudan bağlantı için yeterli olabilir.

Diğer bilgiler
Gerekebileceğinden, ağlar genellikle kurumsal sınırların ötesine genişletilmiştir. İş ortaklarının bilgi işleme ve ağ tesislerini paylaşımı ya da bunlara ara bağlantı kurması gibi genişlemeler, ağ kullanımında kurumsal bilgi sistemlerinin yetkisiz erişim riskini artırabilir. Çünkü söz konusu sistemlerin hassasiyeti ve kritikliği olduğu için diğer ağ kullanıcılarına karşı koruma gerektirebilir.

13.2 Bilgi transferi

Amaç: Bir kuruluş içerisinde ve herhangi bir dış varlık arasında transfer edilen bilginin güvenliğini sağlamak.

13.2.1 Bilgi transfer politikaları ve prosedürleri

Kontrol
Tüm iletişim olanağı türlerinin kullanımıyla bilgi transferini korumak için resmi transfer politikaları, prosedürleri ve kontrolleri mevcut olmalıdır.

Uygulama kılavuzu
Bilgi transferi için haberleşme tesisleri kullanılırken takip edilmesi gereken prosedürler ve kontroller için aşağıdaki maddeler dikkate alınmalıdır:

a) Dinleme, kopyalama, değiştirme, yanlış yönlendirme ve yok edilme sebebiyle transfer bilgileri korumak için tasarlanmış prosedürler;
b) Elektronik haberleşme kullanımı yoluyla bulaşabilen kötücül yazılımları algılama ve karşı koruma için prosedürler (bk. Madde 12.2.1);
c) Bir ek formunda iletilen, hassas elektronik bilgileri korumak için prosedürler;
d) Haberleşme olanaklarının kabul edilebilir kullanımını özetleyen kılavuzlar ve politika (bk. Madde 8.1.3)
e) Personel, dış taraf ve herhangi bir diğer kullanıcının sorumlulukları için kuruluşun taviz vermemesi, örneğin; iftira, taciz, taklit, zincir mektupları yönlendirme, yetkisiz/izinsiz satın alma vb yollarla;
f) Bilginin doğruluğunu, bütünlüğünü ve gizliliğini korumak için kriptografik tekniklerin kullanılması (bk. Madde 10)
g) İlgili ulusal ve yerel yasalar ve düzenlemelere uygun mesajları içeren tüm iş yazışmaları için saklama ve imha kılavuzları,
h) Kullanılan haberleşme olanakları ile ilişkili kontroller ve kısıtlamalar, örneğin; dış posta adreslerine elektronik postaların otomatik yönlendirmesi,
i) Gizli bilgilerin ortaya çıkmasına karşı uygun önlemleri almak için personele tavsiyeler,
j) Yanlış arama sonucu hatayla saklanmış mesajlar ya da ortak sistemlerde saklanmış mesajlar yetkisiz kişiler tarafından tekrar dinlenebileceğinden telesekretere gizli bilgi içeren mesajların bırakılmaması,
k) Faks makineleri veya hizmetlerini kullanma sorunları hakkında personele aşağıdaki gibi tavsiyeler verilmesi:
    1) Dâhili mesaj depolama sistemlerine mesajları almak için yetkisiz erişim,
    2) Özel numaralara mesaj göndermek için makinelerin kasti veya tesadüfi programlanması,
    3) Yanlışlıkla aranmış ya da yanlış kaydedilmiş numarayı kullanarak yanlış numaraya belgeleri ve mesajları gönderme.

Ek olarak, personele kamuya açık alanlarda ya da güvensiz haberleşme kanalları üzerinde, açık ofislerde ve toplantı salonlarında gizli konuşmalar yapılmaması gerektiği hatırlatılmalıdır.

Bilgi transferi hizmetleri ilgili yasal gereksinimlere uymalıdır. (bk. Madde 18.1)

Diğer bilgiler
Bilgi transferi; elektronik posta, ses, faks ve video dâhil olmak üzere bir dizi farklı tipte haberleşme olanakları aracılığıyla oluşabilir.

Yazılım transferi, satışa hazır ürünleri satıcılardan tedarik etme ve internetten indirme dâhil olmak üzere bir dizi farklı ortamlar aracılığıyla olabilir.

Elektronik veri değişiminde; elektronik ticaret ve elektronik haberleşme ile ilgili iş süreçleri, yasal ve güvenlik etkileri ile kontrol gereksinimleri dikkate alınmalıdır.

13.2.2 Bilgi transferindeki anlaşmalar

Kontrol
Anlaşmalar, kuruluş ve dış taraflar arasındaki iş bilgilerinin güvenli transferini ele almalıdır.

Uygulama kılavuzu
Bilgi transferi anlaşmaları aşağıdakileri içermelidir:

a) İletim, sevk ve alındı kontrolü ve bildirimi için yönetim sorumlulukları,
b) İzlenebilirlik ve inkâr edememeyi sağlamak için prosedürler,
c) Paketleme ve iletim için asgari teknik standartlar,
d) Emanet anlaşmaları,
e) Kurye kimlik tanımlama standartları,
f) Verinin kaybı gibi bilgi güvenliği ihlal olaylarındaki sorumluluklar ve yükümlülükler,
g) Bilgilerin uygun şekilde korunmasını ve etiketlerin hemen anlaşılır olmasını sağlayarak, kritik ve hassas bilgi için kabul edilmiş bir etiketleme sisteminin kullanımı (bk. Madde 8.2)
h) Bilgi ve yazılımı, okuma ve kaydetme için teknik standartlar,
i) Kriptografi gibi hassas öğeleri korumak için gerekli tüm özel kontroller (bk. Madde 10),
j) Transfer sırasında bilgi için bir dizi gözetim sağlanması,
k) Erişim kontrolünün kabul edilebilir seviyeleri.

Transferdeki fiziksel ortamı (bk. Madde 8.3.3) ve bilgiyi korumak için politikalar, prosedürler ve standartlar kurulmalı ve sürdürülmelidir. Ayrıca, bu hususlara transfer anlaşmalarında atıf yapılmalıdır.

Herhangi bir anlaşmanın bilgi güvenliği içeriği, iş bilgileri ile ilgili hassasiyeti yansıtmalıdır.
Diğer bilgiler
Anlaşmalar, elektronik ya da kâğıt ortamında olabilir ve resmi anlaşmalar şeklini alabilir. Gizli bilgilerin transferi için kullanılan özel mekanizmalar, tüm kuruluşlar ve anlaşma türleri ile tutarlı olmalıdır.

13.2.3 Elektronik mesajlaşma

Kontrol
Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.

Uygulama kılavuzu
Elektronik mesajlaşma için bilgi güvenliği hususları aşağıdakileri içermelidir:

a) Mesajın; yetkisiz erişime, değiştirilmeye ya da servis dışı bırakılmaya karşı kuruluş tarafından kabul edilen uygun sınıflandırma düzeni ile korunması,
b) Mesajın doğru adreslenmesinin ve taşınmasının sağlanması,
c) Hizmetlerin güvenilirlik ve erişilebilirliği,
d) Yasal konular, örneğin; elektronik imzalar için gereksinimler,
e) Anında mesajlaşma, sosyal ağlar ya da dosya paylaşımı gibi dış hizmetlerin kullanım öncesinde onaylanması,
f) Halka açık ağlara erişilebilirliği kontrol etmek için güçlü seviyede kimlik doğrulama yapılması.

Diğer bilgiler
İş iletişiminde rol oynayan elektronik mesajlaşmanın e-posta, elektronik veri değişimi ve sosyal ağlar gibi birçok türü vardır.

13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları

Kontrol

Bilginin korunması için kuruluşun ihtiyaçlarını yansıtan gizlilik ya da ifşa etmeme anlaşmalarının gereksinimleri tanımlanmalı, düzenli olarak gözden geçirilmeli ve yazılı hale getirilmelidir.

Uygulama kılavuzu
Gizlilik veya ifşa etmeme anlaşmaları yasal olarak uygulanabilir terimleri kullanarak gizli bilgileri korumanın gereksinimlerini ele almalıdır. Gizlilik ve ifşa etmeme anlaşmaları kuruluşun çalışanlarına ya da dış taraflara uygulanır. Diğer tarafların türleri dikkate alınarak ve söz konusu tarafların gizli bilgilere izin verilen erişimleri ve işleme yetkileri dikkate alınarak gerekli öğeler seçilmeli ve ilave edilmelidir. Gizlilik veya ifşa etmeme anlaşmaları için gereksinimleri belirlemek amacıyla aşağıdaki unsurlar dikkate alınmalıdır:

a) Korunacak bilginin bir tanımı (örneğin; gizli bilgiler),
b) Gizliliğin süresiz muhafaza edilmesi gereken durumlar da dâhil olmak üzere anlaşma süresi,
c) Anlaşma sona erdirdiğinde yapılması gereken eylemler,
d) Bilginin yetkisiz olarak ifşa edilmesini önlemek için yetkililerin sorumlulukları ve yerine getirmesi gereken hususlar,
e) Bilginin sahipliği, ticari sırlar ve fikri mülkiyet hakları ve bu gizli bilgilerin nasıl korunması gerektiği,
f) Gizli bilgilerin kullanım izni ve bilgileri kullanmak için imza hakları,
g) Gizli bilgileri içeren faaliyetleri izleme ve denetleme hakkı,
h) Yetkisiz açıklamanın ya da gizli bilgilerin sızdırılmasının bildirimi ve raporlama prosesi,
i) İade veya yok etme anlaşmasına bırakılacak bilgi için terimler,
j) Anlaşmanın ihlali durumunda yapılması beklenen eylemler.

Bir kuruluşun bilgi güvenliği gereksinimlerine dayalı olarak, gizlilik veya ifşa etmeme anlaşmalarında başka unsurlara gerek duyulabilir.

Gizlilik ve ifşa etmeme anlaşmaları, uygulandığı yerin geçerli tüm yasa ve düzenlemelerine uygun olmalıdır (bk. Madde 18.1).

Gizlilik ve ifşa etmeme anlaşmaları için gereksinimler periyodik olarak veya gereksinimleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.

Diğer bilgiler
Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korur ve imzalayan yetkilinin, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtir.

Farklı koşullarda, kuruluşun gizlilik ve ifşa etmeme anlaşmalarının farklı biçimlerini kullanması gerekebilir.

14 Sistem edinimi, geliştirme ve bakımı

14.1 Bilgi sistemlerinin güvenlik gereksinimleri

Amaç: Bilgi güvenliğinin, bilgi sistemlerinin tüm yaşam döngüsü boyunca dâhili bir parçası olmasını sağlamak. Bu aynı zamanda halka açık ağlar üzerinden hizmet sağlayan bilgi sistemleri için gereksinimleri de içerir.

14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi

Kontrol
Bilgi güvenliği ile ilgili gereksinimler, yeni bilgi sistemleri gereksinimlerine veya var olan bilgi sistemlerinin iyileştirmelerine dâhil edilmelidir.

Uygulama kılavuzu
Bilgi güvenliği gereksinimleri; politikalar ve düzenlemelerin, tehdit modellemesinin, olay incelemelerinin veya zayıflık eşik değerlerinin kullanımının uygunluk gereksinimlerini sağlaması gibi çeşitli yöntemler kullanılarak tanımlanmalıdır. Tanımlama sonuçları tüm paydaşlar tarafından gözden geçirilmeli ve yazılı hale getirilmelidir.

Bilgi güvenliği gereksinimleri ve kontrolleri; güvenliğin yeterli olmamasının işe olası olumsuz etkisini ve ilgili bilgilerin iş değerini (bk. Madde 8.2) yansıtmalıdır.

Bilgi güvenliği gereksinimleri ve ilgili proseslerin tanımlanması ve yönetimi, bilgi sistemleri projelerinin erken aşamalarında birleştirilmelidir. Bilgi güvenliği gereksinimlerine tasarım aşaması gibi erken bir aşamada dikkat edilmesi, daha etkili ve düşük maliyetli çözümlere yol açabilir.

Ayrıca bilgi güvenliği gereksinimlerinde aşağıdaki hususlara dikkat etmek gerekir:

a) Kullanıcı kimlik doğrulaması gereksinimlerini elde etmek amacıyla, kullanıcıların iddia ettikleri kimlik bilgilerine karşı gereken güven seviyesi,
b) Hem iş kullanıcıları için hem de ayrıcalıklı veya teknik kullanıcılar için yetkilendirme ve erişim sağlama prosesleri,
c) Kullanıcılar ve operatörlerin görevleri ve sorumlulukları hakkında bilgilendirme,
d) Varlıkların koruma ihtiyacının gerektiği yerlerde özellikle kullanılabilirlik, gizlilik, bütünlük değerlerini içermesi,
e) Kayıt, izleme ve inkâr edememe gereksinimleri gibi iş proseslerinden sağlanan gereksinimler,
f) Diğer güvenlik kontrolleri tarafından zorunlu kılınan gereksinimler, örneğin; veri sızıntısı algılama sistemleri veya kaydetme ve izleme ara yüzleri.

Halka açık ağlar üzerinden hizmet veren uygulamalar veya uygulanan işlemler ile ilgili olarak özel kontrol maddeleri olan Madde 14.1.2 ve Madde 14.1.3 göz önünde bulundurulmalıdır.

Ürünlerin satın alınması durumunda resmi bir test etme ve satın alma süreci takip edilmelidir. Tedarikçiler ile olan sözleşmelerde, belirlenen güvenlik gereksinimleri ele alınmalıdır. Önerilen üründe güvenlik işlevleri belirtilen gereksinimleri karşılamıyorsa, belirlenen riskler ve ilişkili kontroller ürün satın almadan önce yeniden gözden geçirilmelidir.

Son yazılım/hizmet yığını ile uyumlu ürünün güvenlik yapılandırması için uygun kılavuzluk sistemi değerlendirilmeli ve uygulanmalıdır.

Ürünlerin kabulü için; ürünlerin işlevselliği açısından, belirlenen güvenlik gereksinimlerinin karşılanmasına güvence verilmesi gibi kriterler tanımlanmalıdır. Ürünler satın alınmadan önce bu kriterlere göre değerlendirilmelidir. Ek işlevsellikler, kabul edilemez ek riskleri getirmediğini temin etmek için gözden geçirilmelidir.

Diğer bilgiler
ISO/IEC 27005[11] ve ISO 31000[27] bilgi güvenliği gereksinimleri karşılayan kontrolleri tanımlamak için risk yönetim süreçlerinin kullanımı hakkında kılavuzluk sağlar.

14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması

Kontrol
Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilgi, hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan ve değiştirmeden korunmalıdır.

Uygulama kılavuzu
Halka açık ağlar üzerinden geçen uygulama hizmetleri için bilgi güvenliği konuları aşağıdakileri kapsamalıdır:

a) Kullanıcı kimlik doğrulma gereksinimlerini elde etmek amacıyla, kullanıcıların talep edilen kimliklerini kanıtlayacak gerekli güven seviyesi,
b) Bir konu ya da anahtar işlem belgelerini imzalayan, içeriğini onaylayabilen kişi ile ilişkili yetkilendirme prosesleri,
c) İşletişim ortaklarının, hizmetin temini veya kullanımı için kendi yetkilerinden tam haberdar olmalarını sağlama,
d) İhale ve sözleşme prosesleri ile ilgili hususlar gibi anahtar belgeler ve sözleşmeleri inkâr edememe amacıyla gizliliği, bütünlüğü, gönderilme kanıtı ve alınması için gereksinimlerin belirlenmesi ve karşılanması,
e) Anahtar belgelerin bütünlüğünde gerekli güven seviyesi,

f) Herhangi bir gizli bilgiyi koruma gereksinimleri,
g) Makbuzların onayının, dağıtım adresi ayrıntılarının, ödeme bilgisi ve herhangi sipariş işleminin gizliliği ve bütünlüğü,
h) Bir müşteri tarafından tedarik edilen ödeme bilgilerini doğrulamak için uygun doğrulama derecesi,
i) Dolandırıcılığa karşı korumak için ödemenin en uygun anlaşma formu seçilerek yapılması,
j) Sipariş bilgilerinin gizliliğini ve bütünlüğünü korumak için gerekli olan koruma seviyesi,
k) İşlem bilgisi kaybı ya da tekrarlanmasından kaçınılması,
l) Hileli işlemler ile ilişkili sorumluluk,
m) Sigorta gereksinimleri.

Yukarıdaki hususların çoğu yasal gereksinimlerle (bk. Madde 18, özellikle kriptografi yasaları için bk. Madde 18.1.5) uyumluluk da dikkate alınarak kriptografik kontrollerin uygulaması (bk. Madde 10) ile sağlanabilir.

Ortaklar arasında uygulama hizmet anlaşmaları; yetkilendirme detaylarını kapsayan, hizmetlerin kabul şartlarını her iki tarafın taahhüt ettiği, belgelenmiş bir anlaşma ile desteklenmelidir.

Saldırılara karşı direnç gereksinimlerinin, hizmet sunmak için gerekli olan ağ bağlantıların kullanılabilirliğini sağlama ya da ilgili uygulama sunucularını koruma için gerekli gereksinimleri içerebildiği dikkate alınmalıdır.

Diğer bilgiler
Halka açık ağlar üzerinden erişilebilen uygulamalar; hileli faaliyetler, sözleşme anlaşmazlıkları veya kamuya bilgilerin ifşa edilmesi gibi ağ ile ilgili bir dizi tehdide tabidir. Bu nedenle, ayrıntılı risk değerlendirmesi ve kontrollerin uygun seçimi vazgeçilmezdir. Kimlik doğrulama ve güvenli veri aktarımı için genelde kriptografi yöntemi içeren kontroller gereklidir.

Uygulama hizmetleri, riskleri azaltmak için ortak anahtar kriptografisi ve sayısal imza kullanımı (bk. Madde 10) gibi güvenli kimlik doğrulama yöntemlerinden yararlanabilir. Bu hizmetlere ihtiyaç duyulduğunda, güvenilir üçüncü taraflar kullanabilir.

14.1.3 Uygulama hizmet işlemlerinin korunması

Kontrol
Uygulama hizmet işlemlerindeki bilgi; eksik iletimi, yanlış yönlendirmeyi, yetkisiz mesaj değiştirmeyi, yetkisiz ifşayı, yetkisiz mesaj çoğaltmayı ya da mesajı yeniden oluşturmayı önlemek için korunmalıdır.

Uygulama kılavuzu
Uygulama hizmet işlemleri için bilgi güvenliği konuları aşağıdaki hususları içermelidir:

a) İşleme katılan taraflarca işlemde her bir taraf tarafından elektronik imza kullanımı,
b) İşlemin aşağıdaki hususları temin eden tüm yönleri, örneğin;
   1) Tüm taraflardaki kullanıcının gizli kimlik doğrulama bilgilerinin geçerli olması ve doğrulanması,
   2) İşlemin gizli kalması,
   3) Tüm tarafları kapsayan gizlilik ilişkisinin korunması,
c) Tüm taraflar arasındaki haberleşme yolunun şifrelenmesi,
d) Tüm ilgili taraflar arasında, iletişim kurmak için kullanılan protokollerin güvence altına alınması,
e) İşlem ayrıntılarının depolanması için kurumsal intranet üzerinde var olan bir depolama platformu gibi halka açık ortam dışında yer sağlanması ve doğrudan internetten erişilebilir bir depolama ortamında tutulmaması,
f) Güvenli bir otorite kullanılması durumunda (örneğin; sayısal imzaların veya sayısal sertifikaların verilmesi ve korunması amacıyla) güvenlik, sıra ile tüm sertifika/imza yönetimi süreci boyunca yerleştirilir ve gömülü hale getirilir.

Diğer bilgiler
Kabul edilen kontrollerin kapsamının, uygulama hizmet işleminin her bir formu ile ilişkili olan risk seviyesi ile orantılı olması gerekir.

Tamamlanması veya depolanması yoluyla işlenip oluşturulan işlemlerin, yargı çevresindeki yasal ve düzenleyici şartlara uyması gerekebilir.

14.2 Geliştirme ve destek proseslerinde güvenlik

Amaç: Bilgi güvenliğinin bilgi sistemleri geliştirme yaşam döngüsü içerisinde tasarlanıyor ve uygulanıyor olmasını sağlamak.

14.2.1 Güvenli geliştirme politikası

Kontrol
Yazılım ve sistemlerin geliştirme kuralları belirlenmeli ve kuruluş içerisindeki geliştirmelere uygulanmalıdır.

Uygulama kılavuzu
Güvenli geliştirme, güvenli bir hizmeti, mimariyi, yazılımı ve sistemi kurmak için bir gereksinimdir.

Güvenli bir geliştirme politikası içinde, aşağıdaki hususlara dikkat edilmelidir:

a) Geliştirme ortamının güvenliği,
b) Yazılım geliştirme yaşam döngüsü içinde güvenlik konusunda kılavuzluk,
   1) Yazılım geliştirme metodolojisinde güvenlik,
   2) Kullanılan her programlama dili için güvenli kodlama kılavuzları,
c) Tasarım aşamasında güvenlik gereksinimleri,
d) Proje aşamaları içinde güvenlik kontrol noktaları,
e) Güvenli veri depoları,
f) Versiyon kontrolünde güvenlik,
g) Gerekli uygulama güvenlik bilgisi,
h) Geliştiricilerin güvenlik açıklıklarını kaçınma, bulma ve onarma yeteneği.

Güvenli programlama teknikleri, hem yeni geliştirmeler hem de kod içinde geçerli en iyi uygulamalar ile tutarlı olmayan veya geliştirilmesinde standart uygulanmasının bilinmediği yerde senaryolarda yeniden kullanım için kullanılmalıdır. Güvenli kodlama standartları dikkate alınmalı ve uygun olduğu yerlerde kullanımı zorunlu olmalıdır. Geliştiriciler bunların kullanımı konusunda eğitilmeli ve test ve kod incelenmesi ile bunların kullanıldığını doğrulanmalıdır.

Geliştirme dış kaynaklı ise, kuruluş güvenli geliştirme için bu kuralların dış tarafça takip edildiği konusunda güvence sahibi olmalıdır. (bk. Madde 14.2.7)

Diğer bilgiler
Geliştirme aynı zamanda ofis uygulamaları, komut dizisi oluşturma, tarayıcılar ve veritabanları gibi uygulamalar içinde yer alabilir.

14.2.2 Sistem değişiklik kontrolü prosedürleri

Kontrol
Geliştirme yaşam döngüsü içerisindeki sistem değişiklikleri resmi değişiklik kontrol prosedürlerinin kullanımı ile kontrol edilmelidir.

Uygulama kılavuzu
Resmi değişim kontrol prosedürleri, ilk tasarım aşamalarından tüm bakım çalışmalarına kadar sistem, uygulamalar ve ürünlerin bütünlüğünü sağlamak için yazılı hale getirilmeli ve zorunlu olmalıdır.

Yeni sistemlerin dâhil edilmesinde ve mevcut sistemlerde yapılacak önemli değişikliklerde; dokümantasyon, şartname, test etme, kalite kontrol ve uygulamanın yönetimi konularında resmi proses takip edilmelidir.

Bu prosesler, risk değerlendirmesi, değişikliklerin etkisinin analizi ve güvenlik kontrolleri için gerekli özellikleri içermelidir. Bu proses aynı zamanda, mevcut güvenlik ve kontrol prosedürlerinden ödün verilmediğini temin etmelidir, destek programcılarına çalışmaları için sadece sistemin gerekli yerlerine izin verilmelidir ve herhangi bir değişiklik için resmi bir anlaşma ve onay olmalıdır.

Mümkün olduğunca, uygulama ve işletim değişiklik kontrol prosedürleri bütünleştirilmelidir (ayrıca, bk. Madde 12.1.2). Bu değişim kontrol prosedürleri aşağıdakileri içermelidir ama aşağıdakilerle sınırlandırılmamalıdır:

a) Uzlaşıya varılmış yetki seviyelerinin bir kaydının tutulması,
b) Değişikliklerin yetkili kullanıcılar tarafından yapıldığının temin edilmesi,
c) Değişikliklerden zarar görmemelerini temin etmek için kontrollerin ve bütünlük prosedürlerinin gözden geçirilmesi,
d) Tadilat gerektiren tüm yazılımın, bilginin, veri tabanı varlıklarının ve donanımın belirlemesi,
e) Bilinen güvenlik açıkları olasılığının belirlenmesi ve en aza indirmesi için güvenli kritik kod kontrolü;
f) Ayrıntılı teklifler için iş başlangıcından önce onay alınması,
g) Yetkili kullanıcıların uygulamadan önceki değişiklikleri kabul etmesinin sağlanması;
h) Her bir değişiklik tamamlandığında sistem dokümantasyon kümesinin güncellendiğinden ve eski dokümantasyonun arşive kaldırıldığından ya da imha edildiğinden emin olunması,
i) Tüm yazılım güncellemeleri için bir versiyon kontrolü yürütülmesi,
j) Tüm değişiklik istekleri için bir denetim zinciri sürdürülmesi,
k) Uygun hale gelmesi için işletim dokümantasyonunun (bk. Madde 12.1.1) ve kullanıcı prosedürlerinin gerektiği şekilde değiştirilmesinin temin edilmesi,
l) Değişikliklerin yerleştirilmesinin doğru zamanda gerçekleştirilmesini ve söz konusu iş proseslerinin olumsuz yönde etkilenmemesinin temin edilmesi.

Diğer bilgiler
Yazılım değişikliği, işletim ortamını etkileyebilir veya tam tersi de olabilir.

Yeni yazılımın, üretim ve geliştirme ortamlarının her ikisinden de ayrılmış olan bir ortamda test edilmesi iyi uygulama örneğidir (ayrıca, bk. Madde 12.1.4). Bu, yeni yazılım üzerinde kontrol sahibi olmaya yönelik bir yol sağlar ve test amaçlı kullanılan işletimsel bilginin ilave korunmasına izin verir. Bunun, yamaları, hizmet paketlerini ve diğer güncellemeleri içerir.

Otomatik güncelleme yapılan yerlerde, güncellemelerin hızlı dağıtım faydasına karşı sistemin bütünlük ve erişilebilirliğine yönelik riski değerlendirilmelidir. Bazı güncellemeler kritik uygulamaların çökmesine olmasına neden olabildiği için otomatik güncellemeler kritik sistemlerde kullanılmamalıdır.

14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirilmesi

Kontrol
İşletim platformları değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş kritik uygulamalar gözden geçirilmeli ve test edilmelidir.

Uygulama kılavuzu
Bu proses aşağıdakileri kapsamalıdır:

a) İşletim platformu değişikliklerinden zarar görmediğinden emin olmak için uygulama kontrol ve bütünlük prosedürlerinin gözden geçirilmesi,
b) İşletim platformu değişikliklerine ilişkin uygulama öncesinde, uygun test ve gözden geçirmelere imkân tanımak için değişiklik bildirimlerinin zamanda yapılmasının temin edilmesi,
c) İş sürekliği planlarına ilişkin uygun değişikliklerin yapılmasının temin edilmesi (bk. Madde 17).

Diğer bilgiler
İşletim platformları; işletim sistemleri, veri tabanları ve ara katman platformları içerir. Kontroller, uygulamalardaki değişiklikler için uygulanmalıdır.

14.2.4 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar

Kontrol
Yazılım paketlerine yapılacak değişiklikler, gerek duyulanlar hariç önlenmeli ve tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.

Uygulama kılavuzu

Mümkün ve uygulanabilir oldukça, tedarikçi tarafından sağlanan yazılım paketleri değiştirilmeden kullanılmalıdır. Bir yazılım paketinin değiştirilmesi gerekli görüldüğünde, aşağıdaki noktalar göz önünde bulundurulmalıdır:

a) Yerleşik kontrollerin ve bütünlük proseslerinin ele geçirilme riski,
b) Üreticinin onayının alınmasının gerekip gerekmediği,
c) Üreticiden gerekli değişikliklerin standart program güncellemeleri olarak temin edilebilme olasılığı,
d) Değişikliklerin sonucu olarak, kuruluşun yazılımın gelecekteki bakımı konusunda yükümlülük altında kalması halinde oluşacak etki.
e) Kullanılmakta olan diğer yazılımlar ile uyumluluk.

Eğer orijinal yazılımda değişiklikler gerekli ise yazılımın orijinali saklanmalı ve değişiklikler belirlenen bir kopyaya uygulanmalıdır. Bir yazılım güncelleme yönetim süreci, tüm yetkilendirilmiş yazılımlar için en güncel onaylı yamaları ve uygulama güncellemeleri ile uygulanmalıdır (bk. Madde 12.6.1). Tüm değişiklikler, gerektiğinde gelecekteki yazılım güncellemeleri için tekrar uygulanabilmeleri amacıyla tam olarak test edilmeli ve yazılı hale getirilmelidir. Gerekirse, değişiklikler bağımsız bir değerlendirme kuruluşu tarafından test edilmeli ve doğrulanmalıdır.

14.2.5 Güvenli sistem mühendisliği esasları

Kontrol
Güvenli sistem mühendisliği esasları belirlenmeli, yazılı hale getirilmeli, sürdürülmeli ve tüm bilgi sistemi uygulama çalışmalarına uygulanmalıdır.

Uygulama kılavuzu
Güvenli mühendislik ilkelerine dayalı olan güvenli bilgi sistemi mühendisliği prosedürleri; oluşturulmalı, yazılı hale getirilmeli ve kurum içindeki bilgi sistemi mühendislik faaliyetlerine uygulanmalıdır. Güvenlik, erişilebilirlik ihtiyacı ile bilgi güvenliği ihtiyacını dengeleyerek tüm mimari katmanlarda (iş, veri, uygulama ve teknoloji) tasarlanmalıdır. Yeni teknoloji, güvenlik risklerine karşı analiz edilmeli ve tasarımı bilinen saldırı yollarına karşı gözden geçirilmelidir.

Bu ilkeler ve oluşturulan mühendislik prosedürleri düzenli olarak mühendislik süreci içinde güvenliğin gelişmiş standartlarına etkili bir şekilde katkı sağlaması için gözden geçirilmelidir. Ayrıca, düzenli olarak yeni potansiyel tehditlere karşı koyma açısından güncel kalmasını sağlamak ve uygulanan çözümleri ve teknolojideki gelişmelerin uygulanabilir kalması için gözden geçirilmelidir.

Kurulan güvenlik mühendisliği esasları, kuruluş ve kuruluşun dış kaynaklı tedarikçisi arasında sözleşme ve diğer bağlayıcı anlaşmalar yoluyla uygulanması gereken dış kaynaklı bilgi sistemlerine uygulanmalıdır. Kuruluş, tedarikçilerin güvenlik mühendislik ilkelerinin kendine ait olanların katılığı ile karşılaştırılabilir olabileceğini onaylamalıdır.

Diğer bilgiler
Uygulama geliştirme prosedürleri, giriş ve çıkış ara yüzlerine sahip olan uygulamaların geliştirilmesinde güvenli mühendislik tekniklerini uygulamalıdır. Güvenli mühendislik teknikleri; kullanıcı kimlik doğrulama teknikleri, güvenli oturum kontrolü ve veri doğrulama, temizleme ve hata ayıklama kodlarının giderilmesi konusunda kılavuzluk sağlar.

14.2.6 Güvenli geliştirme ortamı

Kontrol
Kuruluşlar tüm sistem geliştirme yaşam döngüsünü kapsayan sistem geliştirme ve bütünleştirme girişimleri için güvenli geliştirme ortamları kurmalı ve uygun bir şekilde korumalıdır.

Uygulama kılavuzu
Güvenli bir geliştirme ortamı; sistem geliştirme ve uyumu ile ilişkili insanları, prosesleri ve teknolojiyi kapsar.

Kuruluşlar, aşağıdaki hususları dikkate alarak bağımsız sistem geliştirme çalışmaları ile ilişkili riskleri değerlendirmeli ve özel sistem geliştirme çalışmaları için güvenli geliştirme ortamları oluşturmalıdır:

a) Sistem tarafından işlenen, depolanan ve iletilen verinin hassaslığı,
b) Uygulanabilir dış ve iç gereksinimler, örneğin; düzenlemeler veya politikalardan,

c) Kuruluş tarafından sistem gelişimini destekleyen önceden uygulanmış güvenlik kontrolleri,
d) Ortamda çalışan personelin güvenilirliği (bk. Madde 7.1.1),
e) Sistem geliştirme ile ilişkili dış kaynak kullanım derecesi,
f) Farklı geliştirme ortamları arasındaki ayrım ihtiyacı,
g) Geliştirme ortamına erişim kontrolü,
h) Ortamdaki ve ortamda depolanmış koddaki değişikliklerin izlenmesi,
i) Yedeklerin kurum dışında güvenli yerlerde saklanması,
j) Verinin ortama ve ortam dışına olan hareketlerinin kontrolü.

Kuruluşlar, belirli bir geliştirme ortamı için koruma düzeyi belirlendikten sonra güvenli geliştirme prosedürlerinde ilgili prosesleri yazılı hale getirmeli ve ihtiyaç duyan tüm bireylere bunları sağlamalıdır.

14.2.7 Dışardan sağlanan geliştirme

Kontrol
Kuruluş dışarıdan sağlanan sistem geliştirme faaliyetini denetlemeli ve izlemelidir.

Uygulama kılavuzu
Sistem geliştirme dış kaynaklı olduğunda, aşağıdaki hususlar kuruluşun tüm dış tedarik zinciri için dikkate alınmalıdır:

a) Dış kaynaklı tedarik içeriği ile ilişkili lisans anlaşmaları, kod mülkiyeti ve fikri mülkiyet hakları (bk. Madde 18.1.2),
b) Güvenli tasarım, kodlama ve test uygulamaları için sözleşme gereksinimleri (bk. Madde 14.2.1),
c) Dış geliştiriciye onaylanmış tehdit modelinin temini,
d) Çıktıların kalitesi ve doğruluğu için kabul testleri,
e) Güvenlik ve gizlilik kalitesinin en düşük kabul edilebilir seviyelerini belirlemek için kullanılan güvenlik eşik değerleri olan kanıtın temini,
f) Dağıtım üzerinde hem kasıtlı hem de kasıtsız zararlı içerikten korunmak için uygulanan yeterli test etme kanıtının temini,
g) Bilinen güvenlik açıklarının varlığına karşı korunmak için yeterli derecede test yapıldığına dair kanıtların temini,
h) Emanet anlaşmaları; örneğin, kaynak kod artık mevcut değilse,
i) Geliştirme prosesleri ve kontrolleri ile ilgili sözleşmeden doğan denetim hakkı,
j) Dağıtımları oluşturmak için kullanılan ortam yapısının etkili dokümantasyonu,
k) Kuruluş, uygulanabilir yasalar ve verimlilik doğrulama kontrolünün uyumundan sorumludur.

Diğer bilgiler
Tedarikçi ilişkileri hakkında daha fazla bilgi ISO/IEC 27036 standardında bulunabilir. [21][22][23]

14.2.8 Sistem güvenlik testi

Kontrol
Güvenlik işlevselliğinin test edilmesi, geliştirme süresince gerçekleştirilmelidir.

Uygulama kılavuzu
Yeni ve güncelleştirilmiş sistemler, bir dizi koşul altında test girdileri ve beklenen çıktıların ve faaliyetlerin detaylı bir programının hazırlanmasını kapsayan geliştirme prosesleri süresince kapsamlı doğrulama ve test gerektirir. Kurum içi geliştirmeler için bu tür testler başlangıçta geliştirme ekibi tarafından yapılmalıdır. Bağımsız kabul testleri (hem dış kaynaklı hem de kuruluş içinde) yalnızca sistemin sadece beklendiği gibi çalışmasını sağladıktan sonra yapılmalıdır (bk. Madde14.1.1 ve 14.1.9). Testin kapsamı, sistemin önemi ve doğası ile orantılı olmalıdır.

14.2.9 Sistem kabul testi

Kontrol
Kabul test programları ve ilgili kriterler, yeni bilgi sistemleri, yükseltmeler ve yeni versiyonlar için belirlenmelidir.

Uygulama kılavuzu
Sistem kabul testi, bilgi güvenliği gereksinimleri testini (bk. Madde 14.1.1 ve 14.1.2) ve güvenli sistem geliştirme uygulamaları ile uyumluluğu içermelidir (bk. Madde 14.2.1). Test ayrıca, temin edilen bileşenler ve

bütünleşik sistemler üzerinde yapılmalıdır. Kuruluşlar, kod analiz araçları veya açıklık tarayıcıları gibi otomatikleştirilmiş araçları kullanabilir. Kuruluş güvenlikle ilgili hataların giderildiğini doğrulamalıdır.

Sistemin, kuruluşun ortamında açıklara sebep olmayacağına ve testlerin güvenilir olduğunu temin etmek için testler gerçekçi bir test ortamında yapılmalıdır.

14.3 Test verisi

Amaç: Test için kullanılan verinin korunmasını sağlamak.

14.3.1 Test verisinin korunması

Kontrol
Test verisi dikkatli bir şekilde seçilmeli, korunmalı ve kontrol edilmelidir.

Uygulama kılavuzu
Test amacıyla kişiyi tanımlamak için kullanılan bilgileri içeren işlemsel verinin ya da diğer tüm gizli bilgilerin kullanımından kaçınılmalıdır. Test amacıyla, kişiyi tanımlamak için kullanılan bilgileri ve diğer gizli bilgiler kullanıldığında tüm hassas ayrıntılar ve içerik silinme ya da değiştirilme işleminden korunmalıdır (bk. ISO/IEC 29101[26]).

Test amacıyla kullanıldığında, işlemsel verilerin korunması için aşağıdaki kılavuzlara dikkat edilmelidir:

a) İşletimsel uygulama sistemlerine uygulanan erişim kontrol prosedürleri, test uygulama sistemleri içinde geçerli olmalıdır,
b) İşletimsel bilgiler test ortamına her kopyalandığında ayrı yetkilendirme yapılmalıdır;
c) Test işlemi tamamlanmasının hemen ardından işletimsel bilgiler test ortamında silinmelidir,
d) Bir denetim kaydı oluşturmak amacıyla işletimsel bilginin kopyalanması ve kullanımı kaydedilmelidir.

Diğer bilgiler
Sistem ve kabul testleri genellikle, işletimsel verilere mümkün olan en yakın yüksek hacimli test verisi gerektirebilir.

15 Tedarikçi ilişkileri

15.1 Tedarikçi ilişkilerinde bilgi güvenliği

Amaç: Kuruluşa ait tedarikçiler tarafından erişilebilen varlıkların korunmasını sağlamak.

15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası

Kontrol
Tedarikçinin kuruluşun varlıklarına erişimi ile ilgili riskleri azaltmak için bilgi güvenliği gereksinimleri tedarikçi ile kararlaştırılmalı ve yazılı hale getirilmelidir.

Uygulama kılavuzu
Kuruluş, politika da özellikle kuruluşun bilgilerine erişen tedarikçileri ele alarak bilgi güvenliği kontrollerini tanımlamalı ve zorlamalıdır. Bu kontroller, kuruluş tarafından uygulanan prosesleri ve prosedürleri ele almalıdır, bununla birlikte kuruluşun bu prosesleri ve prosedürleri tedarikçilere aşağıdaki hususları da içerecek şekilde uygulaması gerekir:

a) Tedarikçi türlerinin belirlenmesi ve yazılı hale getirilmesi, örneğin; kuruluşça bilgilere erişim izni verilen BT hizmetleri, lojistik araçları, finansal hizmetler, BT altyapı bileşenleri,

b) Tedarikçi ilişkilerini yönetmek için bir standart proses ve yaşam döngüsü,
c) Tedarikçilerin farklı türleri için tanımlanan bilgi erişim türlerine izin verilmesi ve erişimler izlenmesi ve kontrol edilmesi,
d) Kuruluşun iş ihtiyaçları ve gereksinimleri ve risk profili temel alınarak bireysel tedarikçi anlaşmaları için her bilgi türü ve erişim türü için asgari bilgi güvenliği gereksinimleri,
e) Üçüncü taraf gözden geçirme ve ürün doğrulama dâhil her tedarikçi türü ve erişim türü için kurulan bilgi güvenliği gereksinimleri uyumluluğunun izlenmesi için prosesler ve prosedürler,
f) Taraflarca sağlanan bilgi ya da bilgi işlemenin bütünlüğünü sağlamak amacıyla doğruluk ve bütünlük kontrolleri,
g) Kuruluşun bilgilerini korumak için tedarikçilere uygulanan yükümlülük türleri,
h) Hem kuruluş hem de tedarikçilerin sorumlulukları dâhil olmak üzere tedarikçi erişimi ile ilişkili acil durumların ve ihlal olaylarının işlenmesi,
i) Esneklik ve gerekirse, taraflarca sağlanan bilgi ve bilgi işleme kullanılabilirliğini sağlamak için kurtarma ve acil durum düzenlemeleri,
j) Kuruluşun satın almalar ile ilgili personeli için uygulanabilir politikalar, prosesler ve prosedürler ile ilgili farkındalık eğitimi,
k) Kuruluşun sistemleri ve bilgilerine tedarikçi erişim düzeyleri ve tedarikçi türlerine göre uygun katılım ve davranış kuralları konusunda tedarikçi personeli ile etkileşimde olan kuruluş personeli için farkındalık eğitimi,
l) Bilgi güvenliği şartları ve kontrollerinin yazılı hale getirileceği her iki taraf tarafından bir anlaşmanın hangi şartlar altında imzalanacağı,
m) Bilgi, bilgi işleme tesisleri ve taşınması gereken herhangi bir şeyin gerekli geçiş işlemini yönetme, ve geçiş işlemi süresince bilgi güvenliğinin sürdürülmesi.

Diğer bilgiler
Bilgi, yetersiz bilgi güvenliği yönetimi ile tedarikçi tarafından riske atılabilir. Bilgi işleme tesislerine tedarikçi erişimini yönetmek için kontroller tespit edilmeli ve uygulanmalıdır. Örneğin, bilgilerin gizliliği için özel bir ihtiyaç varsa, ifşa etmeme anlaşmaları kullanılabilir. Başka bir örnek, aktarımı, ya da erişimi, sınırlar ötesi bilgi aktarımını içeren tedarikçi anlaşmalarında veri koruma riskleridir. Kuruluş dâhilinde yer alan bilgilerin korunması için kuruluş, yasal ya da sözleşmeden doğan sorumluluklarının farkında olmalıdır.

15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme

Kontrol
Kuruluşun bilgisine erişebilen, bunu işletebilen, depolayabilen, iletebilen veya kuruluşun bilgisi için bilgi teknolojileri altyapı bileşenlerini temin edebilen tedarikçilerin her biri ile anlaşılmalı ve ilgili tüm bilgi güvenliği gereksinimleri oluşturulmalıdır.

Uygulama kılavuzu
Kuruluş ile tedarikçi arasında yanlış anlaşılma olasılığını kaldırmak ve ilgili bilgi güvenliği gereksinimlerini karşılamak için her iki tarafın yükümlülüklerinden emin olmak amacıyla tedarikçi anlaşmaları yapılmalı ve yazılı hale getirilmelidir.

Tespit edilen bilgi güvenliği gereksinimlerini karşılamak amacıyla anlaşmalara dâhil edilmesi için aşağıdaki şartlar dikkate alınmalıdır:

a) Sağlanacak ya da erişilecek bilginin tanımı ve bilgi sağlama ve erişim yöntemleri,
b) Kuruluşun bilgi sınıflandırma düzenine uygun bilgi sınıflandırması (bk. Madde 8.2), gerekirse kuruluşun kendi sınıflandırma düzeni ve tedarikçi sınıflandırma düzeni arasındaki eşleştirme,
c) Veri koruma, fikri mülkiyet hakları ve telif hakları dâhil yasal ve düzenleyici gereksinimler ve bunların nasıl karşılandığının açıklaması,
d) Erişim kontrolü, performans gözden geçirme, izleme, raporlama ve denetimi içeren üzerinde anlaşılmış bir kontrol kümesini uygulamak için her bir sözleşme tarafının yükümlülükleri,
e) Bilginin kabul edilebilir kullanıma dair kurallar, gerekirse, kabul edilemez kullanımı da dâhil olmak üzere,
f) Kuruluşun bilgisine erişmek veya almak için yetkili tedarikçi personelinin açık listesi ya da tedarikçi personeli tarafından kuruluşun bilgisine erişmek ve almak amacıyla yetkilendirme ve yetkilendirilmenin kaldırılması için prosedürler ya da şartlar,
g) Belirli bir sözleşmeye yönelik bilgi güvenliği politikaları,
h) İhlal olayı yönetimi gereksinimleri ve prosedürleri (özellikle ihlal olayına müdahale esasında bildirim ve ortak çalışma),

i) Belirli prosedürler ve bilgi güvenliği gereksinimleri için eğitim ve farkındalık gereksinimleri, örneğin; ihlal olayına müdahale, yetkilendirme prosedürleri,
j) Uygulanması gereken kontroller dâhil olmak üzere, taşere etme için ilgili düzenlemeler,
k) Bilgi güvenliği konularında irtibat personeli de dâhil olmak üzere ilgili anlaşma tarafları,
l) Taramanın tamamlanmadığı veya sonuçların şüphe veya çekinceye neden olduğu durumda taramanın gerçekleştirme ve bildirim prosedürleri için sorumluluklar da dâhil olmak üzere tedarikçi personeli için varsa tarama gereksinimleri,
m) Anlaşma ile ilgili tedarikçi prosesleri ve kontrollerini denetim hakkı,
n) Arıza çözümü ve anlaşmazlık çözümü prosesleri,
o) Periyodik kontrollerin etkinliği hakkında bağımsız bir rapor sunmak için tedarikçinin yükümlülüğü ve raporda gündeme getirilen ilgili hususların zamanında düzeltilmesi konusunda anlaşma,
p) Kuruluşun güvenlik gereksinimleri ile uyumluluk için tedarikçi yükümlülükleri.

Diğer bilgiler
Anlaşmalar, farklı kuruluşlar ve tedarikçilerin farklı türleri arasında önemli ölçüde değişebilir. Bu nedenle, tüm ilgili bilgi güvenliği riskleri ve gereksinimleri de dâhil edilmesine dikkate alınmalıdır. Tedarikçi anlaşmaları diğer tarafları da içerebilir (örneğin; alt-tedarikçiler).

Yedek ürün ve hizmetlerin temininde gecikmeyi engellemek için, tedarikçinin ürün ve hizmetlerini sağlayamaması durumunda faaliyetin devam etmesi için prosedürler anlaşmada ele alınmalıdır.

15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri

Kontrol
Tedarikçiler ile yapılan anlaşmalar, bilgi ve iletişim teknolojileri hizmetleri ve ürün tedarik zinciri ile ilgili bilgi güvenliği risklerini ifade eden şartları içermelidir.

Uygulama kılavuzu
Aşağıdaki hususlar tedarik zinciri güvenliği ile ilgili tedarikçi anlaşmalarına dâhil edilmek üzere dikkate alınmalıdır:

a) Tedarikçi ilişkileri için genel bilgi güvenliği şartlarına ek olarak bilgi ve iletişim teknolojileri ürün veya hizmet temininde uygulanmak üzere bilgi güvenliği şartlarının tanımlanması,
b) Bilgi ve iletişim teknolojisi hizmetleri için, tedarikçiler kuruluşa sağlanan bilgi ve iletişim teknolojisi hizmetinin bir bölümünde alt yüklenici kullanıyorsa; tedarikçilerin, tedarik zinciri boyunca kuruluşun güvenlik gereksinimlerini yaygınlaştırması gerekir,
c) Bilgi ve iletişim teknolojisi ürünleri için, bu ürünler diğer tedarikçilerden satın alınan bileşenleri içeriyorsa; tedarikçilerin, tedarik zinciri boyunca kuruluşun doğru güvenlik uygulamalarını yaygınlaştırması gerekir,
d) Belirtilen güvenlik gereksinimlerine bağlı kalarak bilgi ve iletişim teknolojisi ürünleri ve hizmetlerinin dağıtımını doğrulamak için bir izleme prosesinin ve kabul edilebilir yöntemlerin gerçekleştirilmesi,
e) İşlevselliğin sürdürülmesi için kritik olan ve bundan dolayı daha fazla dikkat inceleme gerektiren ürün veya hizmet bileşenleri, kurum dışında yapılıyorsa, (özellikle en üst tedarikçinin ürün veya hizmet bileşenlerini diğer tedarikçilerden temin etmesi durumunda) bu ürün veya hizmet bileşenlerinin tespiti için bir proses uygulanması,
f) Kritik bileşenler ve bunların kaynaklarının tedarik zinciri boyunca takip edilebilir olması için güvence sağlanması,
g) Bilgi ve iletişim teknolojisi ürünlerinin herhangi bir beklenmeyen veya istenmeyen özellikler olmadan, beklendiği gibi çalışması için güvence sağlanması,
h) Kuruluş ile tedarikçiler arasında tedarik zinciri, diğer olası konularda ve uzlaşılarda bilgi paylaşımı için kuralların tanımlanması,
i) Bilgi ve iletişim teknolojisi bileşenlerinin yaşam süresi, erişilebilirliği ve ilişkili güvenlik risklerini yönetmek için belirli proseslerin uygulanması. Yukarıdaki ifade, artık mevcut olmayan bileşenlere dair güvenlik risklerinin yönetimini de içerir (bu bileşenler, tedarikçilerin faaliyetine son vermiş olmasından veya teknolojinin gelişmesinden dolayı tedarikçilerin artık bunları sağlayamaması nedeniyle mevcut olmayabilir).

Diğer bilgiler
Özel bilgi ve iletişim teknolojileri tedarik zinciri risk yönetimi uygulamaları; genel bilgi güvenliği, kalite, proje yönetimi ve sistem mühendisliği uygulamaları üzerine inşa edilir, ancak; bunların yerine geçmez.

Kuruluşlara, bilgi ve iletişim teknolojisi tedarik zincirini ve sağlanan ürünler ve hizmetler hakkında önemli bir etkiye sahip tüm konulara vakıf olan tedarikçiler ile çalışması tavsiye edilir. Kuruluş, tedarikçiler ile anlaşmalarını açık ve anlaşılır yaparak bilgi ve iletişim teknolojisi tedarik zinciri bilgi güvenliği uygulamalarını etkileyebilir. Bu durum, bilgi ve iletişim teknolojisi tedarik zincirindeki diğer tedarikçiler tarafından ele alınmalıdır.

Burada ele alınan bilgi ve iletişim teknolojisi tedarik zinciri bulut bilişim hizmetlerini içerir.

15.2 Tedarikçi hizmetleri sağlama yönetimi

Amaç: Tedarikçi anlaşmalarıyla uyumlu olarak kararlaştırılan seviyede bir bilgi güvenliğini ve hizmet sunumunu sürdürmek.

15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme

Kontrol
Kuruluşlar, düzenli aralıklarla tedarikçi hizmet sunumunu izlemeli, gözden geçirmeli ve tetkik etmelidir.

Uygulama kılavuzu
Tedarikçi hizmetlerinin izlenmesi ve gözden geçirilmesi, anlaşmaların bilgi güvenliği şart ve koşullarına riayet edildiğini ve bilgi güvenliği ihlal olayları ve sorunlarının doğru şekilde yönetilmesini temin etmelidir.

Bir kuruluş ve tedarikçi arasındaki hizmet yönetimi ilişkisi ve prosesleri aşağıdaki hususları içeriyor olmalıdır:

a) Anlaşmalara riayet edildiğinin kontrolü için hizmet performansı düzeylerinin izlemesi,
b) Anlaşmalar gereği; tedarikçilerce üretilen hizmet raporlarının gözden geçirilmesi ve düzenli ilerleme toplantılarının düzenlenmesi,
c) Bağımsız denetçi raporları varsa bunların gözden geçirilmesi ile birlikte tedarikçilerin denetlenmesi ve tespit edilen hususların takip edilmesi,
d) Bilgi güvenliği ihlal olayları hakkında bilgi sağlanması ve anlaşmalar, tüm destekleyici kılavuzlar ve prosedürler gereği bu bilgilerin gözden geçirilmesi,
e) Hizmetlerin sunumu ile ilgili kesintilerin ve hataların izlenmesi, işletim sorunları, hataların ve bilgi güvenliği olayları kayıtlarının ve tedarikçi denetim kayıtlarının gözden geçirilmesi,
f) Herhangi bir tespit edilen problemin çözülmesi ve yönetilmesi.
g) Kendi tedarikçileri ile tedarikçinin ilişkilerinin bilgi güvenliği yönünden gözden geçirilmesi,
h) Çalışabilir planları ile birlikte tedarikçinin yeterli hizmet yeteneğinin devamlılığının sağladığından emin olunması,

Tedarikçi yönetimi için sorumluluğu, belirlenmiş bir hizmet yönetim ekibine ya da bir bireye atanmalıdır. Buna ek olarak, kuruluş anlaşma gereksinimlerine uyulması ve uygulanmasını gözden geçirmek için tedarikçilerin sorumlulukları atadığından emin olmalıdır. Yeterli teknik beceri ve kaynaklar, anlaşma gereklerini (bk. Madde 6.2.3) ve özellikle bilgi güvenliği gereklerini izlemek için sağlanmalıdır. Hizmet sağlamada eksiklikler tespit edildiğinde, uygun eylemler alınmalıdır.

Kuruluş, tedarikçi tarafından erişilen, işlenen ve yönetilen hassas ve kritik bilgilerin ve bilgi işleme tesislerinin tüm güvenlik hususlarının yeterli derecede genel kontrolünü ve görünürlüğünün sürdürülmesini sağlamalıdır. Kuruluş, değişim yönetimi, güvenlik açıklıklarının tespiti ve tanımlanmış raporlama süreci ile bilgi güvenliği ihlal olaylarının biçimi ve yapısı gibi güvenlik faaliyetlerinin görünürlüğünün sürdürüldüğünü sağlamalıdır.

15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme

Kontrol
Mevcut bilgi güvenliği politikalarını, prosedürlerini ve kontrollerini sürdürme ve iyileştirmeyi içeren tedarikçilerin hizmet tedariki değişiklikleri, ilgili iş bilgi, sistem ve dâhil edilen süreçlerin kritikliğini ve risklerin yeniden değerlendirmesini hesaba katarak yönetilmelidir.

Uygulama kılavuzu
Aşağıdaki hususlar dikkate alınmalıdır:

a) Tedarikçi anlaşmaları değişiklikleri,
b) Aşağıdakileri gerçekleştirmek için kuruluş tarafından yapılan değişiklikler,
    1) Sunulan mevcut hizmetleri zenginleştirmek,
    2) Tüm yeni uygulamaların ve sistemlerin geliştirilmesi,
    3) Kuruluşun politika ve prosedürlerinin değişiklikleri ve güncellemeleri,
    4) Yeni bilgi güvenliği olaylarını çözmek ve güvenliği artırmak için yeni kontroller,
c) Aşağıdakileri gerçekleştirmek için tedarikçi hizmetlerinde yapılan değişiklikler:
    1) Ağların değişimi ve genişletilmesi,
    2) Yeni teknolojilerin kullanımı,
    3) Yeni ürün veya yeni versiyonların/sürümlerin adapte edilmesi,
    4) Yeni geliştirme araçları ve ortamları,
    5) Hizmet tesislerinin fiziksel yerleşiminin değişimi,
    6) Tedarikçilerin değişimi,
    7) Başka bir tedarikçiye taşere etme.

16 Bilgi güvenliği ihlal olayı yönetimi

16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirmelerin yönetimi

Amaç: Bilgi güvenliği ihlal olaylarının yönetimine, güvenlik olayları ve açıklıklar üzerindeki bağlantısını da içeren, tutarlı ve etkili yaklaşımın uygulanmasını sağlamak.

16.1.1 Sorumluluklar ve prosedürler

Kontrol
Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için yönetim sorumlulukları ve prosedürleri oluşturulmalıdır.

Uygulama kılavuzu
Bilgi güvenliği ihlal olayı ile ilişkili yönetim sorumlulukları ve prosedürleri için aşağıdaki hususlara dikkat edilmelidir:

a) Yönetim sorumlulukları aşağıdaki prosedürlerin geliştirilmesini ve kuruluş içinde yeterince duyurulmasını tesis etmelidir:
    1) İhlal olayına müdahalenin planlanması ve hazırlığı için prosedürler,
    2) Bilgi güvenliği olaylarının ve ihlal olaylarının izlenmesi, tespiti, analizi ve raporlanması için prosedürler,
    3) İhlal olayları yönetimi faaliyetleri için kayıt tutma prosedürleri,
    4) Adli delil işlenmesi için prosedürler,
    5) Bilgi güvenliği olaylarının değerlendirilmesi, bilgi güvenliği olaylarında karar verme ve bilgi güvenliği zafiyetlerinin değerlendirilmesi için prosedürler,
    6) Dâhili ve harici kişi ya da kuruluşlarla iletişim ve bir ihlal olayından kontrollü kurtarma, yükseltme dâhil olmak üzere müdahale için prosedürler,
b) Yürürlükteki prosedürler aşağıdaki hususlar sağlanmalıdır:
    1) Kuruluş içinde bilgi güvenliği ihlal olaylarını ele alacak yetkili personel,
    2) Bilgi güvenliği ihlal olaylarının tespiti ve raporlanması için iletişim noktasının belirlenmesi,
    3) Bilgi güvenliği ihlal olayları ile ilişkili işlemlerde otoriteler, dış ilgi grupları ya da forumlarla uygun iletişim,
c) Raporlama prosedürleri aşağıdaki hususları içermelidir:
    1) Raporlama faaliyetinin desteklenmesi amacıyla bilgi güvenliği olayları rapor formlarının hazırlanması ve bir bilgi güvenliği olayı oluştuğunda raporlayan kişiye tüm gerekli işlemleri hatırlamasına yardımcı olmak,
    2) Bir bilgi güvenliği olayında işletilecek prosedür, örneğin; uygunsuzluk ya da ihlal türü, meydana gelen arıza, ekranda görülen mesajlar ve hemen iletişim noktasına raporlama ve sadece koordine edilmiş işlemleri gerçekleştirme gibi tüm ayrıntıların anında belirtilmesi,
    3) Güvenlik ihlallerini işleyen çalışanlar ile ilgili işlemler için yürürlükteki resmi bir disiplin prosesine atıf yapılması,

4) Bilgi güvenliği olayını raporlayan kişilerin olay ele alındıktan ve kapatıldıktan sonra bildirilmesini temin etmek için uygun geribildirim prosesleri.

Bilgi güvenliği ihlal olayları yönetimi için amaçlar üzerinde yönetim ile uzlaşılmalıdır ve bilgi güvenliği ihlallerinin yönetimi sorumlusunun bilgi güvenliği ihlalleri ile ilgilenmek için kuruluşun önceliklerini anlaması sağlanmalıdır.

Diğer bilgiler
Bilgi güvenliği ihlalleri, kurumsal ve ulusal sınırları aşabilir. Bu tür ihlal olaylarına müdahale etmek için uygun dış kuruluşlara ihlal olayları hakkında bilgi paylaşımı ve yanıt için koordinasyona giderek artan bir ihtiyaç vardır.

Bilgi güvenliği ihlali olayı yönetimi hakkında detaylı kılavuzluk ISO/IEC 27035 tarafından sağlanmaktadır. [20]

16.1.2 Bilgi güvenliği olaylarının raporlanması

Kontrol
Bilgi güvenliği olayları uygun yönetim kanalları aracılığı ile olabildiğince hızlı bir şekilde raporlanmalıdır.

Uygulama kılavuzu
Tüm çalışanlar ve yükleniciler, herhangi bir güvenlik olayının olabildiğince hızlı bir şekilde raporlanması konusunda kendi sorumluluklarının farkında olmalıdır. Ayrıca; tüm çalışanlar ve yükleniciler bilgi güvenliği olaylarının raporlanmasına ait prosedürün ve bu olayların raporlanması gereken iletişim noktasının farkında olmalıdır.
Bilgi güvenliği olaylarının raporlanmasında aşağıdaki durumlara dikkat edilmelidir:

a) Etkisiz güvenlik kontrolü,
b) Bilginin bütünlük, gizlilik veya erişilebilirlik beklentilerinin ihlali,
c) İnsan hataları,
d) Politikalar ve kılavuzlarla uygunsuzluk,
e) Fiziksel güvenlik düzenlemelerinin ihlali,
f) Kontrolsüz sistem değişiklikleri,
g) Yazılım ya da donanım arızaları,
h) Erişim ihlalleri.

Diğer bilgiler
Arızalar veya diğer anormal sistem davranışları bir güvenlik saldırısı ya da bir güvenlik ihlalinin göstergesi olabilir ve bu nedenle her zaman bilgi güvenliği olayı olarak rapor edilmelidir.

16.1.3 Bilgi güvenliği açıklıklarının raporlanması

Kontrol
Kuruluşun bilgi sistemlerini ve hizmetlerini kullanan çalışanlardan ve yüklenicilerden, sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmeleri ve bunları raporlamaları istenmelidir.

Uygulama kılavuzu
Tüm çalışanlar ve yükleniciler bilgi güvenliği ihlal olaylarını önlemek için mümkün olduğu kadar çabuk iletişim noktasına bu konuları rapor etmelidir. Raporlama mekanizması mümkün olduğunca kolay, kullanılabilir ve erişilebilir olmalıdır.

Diğer bilgiler
Çalışanlara ve yüklenicilere şüpheli güvenlik açıklıklarını kanıtlamaya çalışmamaları tavsiye edilmelidir. Zayıflıkların testi, sistemin olası suiistimali şeklinde yorumlanmaya neden olabilir ve ayrıca bilgi sistemleri veya hizmetlerde hasara neden olarak testi yapan kişi için yasal müeyyide doğurabilir.

16.1.4 Bilgi güvenliği olaylarında değerlendirme ve karar verme

Kontrol
Bilgi güvenliği olayları değerlendirilmeli ve bilgi güvenliği ihlal olayı olarak sınıflandırılıp sınıflandırılmayacağına karar verilmelidir.

Uygulama kılavuzu
İletişim noktası bilgi güvenliği olayı ve ihlallerinin sınıflandırılması ölçeğini kullanarak her bilgi güvenliği olayını değerlendirmelidir ve olayın bilgi güvenliği ihlal olayı olarak sınıflandırılıp sınıflandırılmayacağına karar vermelidir. Olayların sınıflandırması ve önceliklendirilmesi, ihlal olaylarının boyutlarının belirlenmesi ve etkilerinin tanımlanmasına yardımcı olabilir.

Kuruluşun bilgi güvenliği ihlal olayı müdahale ekibine (SOME) sahip olduğu durumlarda, değerlendirme ve karar, onay ya da yeniden değerlendirme için SOME'ye iletilebilir.

Değerlendirme ve karar sonuçları, ileride tekrar faydalanma ve doğrulama amacıyla kayıt edilmelidir.

16.1.5 Bilgi güvenliği ihlal olaylarına müdahale

Kontrol
Bilgi güvenliği ihlal olaylarına, yazılı prosedürlere uygun olarak müdahale edilmelidir.

Uygulama kılavuzu
Bilgi güvenliği ihlal olaylarına, yetkili iletişim noktalarından ve kuruluştaki diğer ilgili personel ya da dış taraflardan müdahale edilmelidir. (bk. Madde 16.1.1)

Müdahale aşağıdaki hususları içermelidir:

a) Ortaya çıktıktan sonra olabildiğince kısa sürede delil toplanması,
b) Gerektiği durumda bilgi güvenliği adli bilişim analizi yapılması (bk. Madde 16.1.7),
c) Gerektiği durumda yükseltme,
d) Daha sonra analiz etmek için tüm ilgili müdahale faaliyetlerinin düzgün kayıtlarının tutulmasından emin olmak,
e) Bilmesi gereken prensibine göre kurum içi ve kurum dışı kişiler veya birimlere bilgi güvenliği ihlal olayının varlığı veya diğer ilgili detayların duyurulması,
f) İhlal olayını gerçekleştiren veya buna katkıda bulunan bilgi güvenliği zayıflığı/zayıflıkları ile ele alma,
g) İhlal olayının başarıyla ele alınmasından sonra resmi olarak kapatılması ve kayıt edilmesi.

İhlal olayı sonrası analiz, gerektiği durumda ihlal olayının kaynağını belirlemek için yapılmalıdır.

Diğer bilgiler
İhlal olayına müdahalenin ilk hedefi 'normal güvenlik seviyesi'ni sürdürmektir ve gereken kurtarma faaliyetini başlatmaktır.

16.1.6 Bilgi güvenliği ihlal olaylarından ders çıkarma

Kontrol
Bilgi güvenliği ihlal olaylarının analizi ve çözümlemesinden kazanılan bilgi birikimi gelecekteki ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için kullanılmalıdır.

Uygulama kılavuzu
Bilgi güvenliği ihlal olaylarının türlerinin, hacimlerinin ve maliyetlerinin ölçeklendirilmesini ve izlenmesini sağlayacak bir mekanizma olmalıdır. Bilgi güvenliği ihlallerinin değerlendirilmesinden edinilen bilgiler tekrarlayan ya da yüksek etkili ihlal olaylarını tespit etmek için kullanılmalıdır.

Diğer bilgiler
Bilgi güvenliği ihlal olaylarının değerlendirilmesi; meydana gelme sıklığını, hasarı ve gelecek olayların maliyetlerini sınırlandırmak için gelişmiş ya da ek kontrollere ihtiyaç olduğunu gösterebilir ya da güvenlik politikasının gözden geçirilmesi prosesinde de dikkate alınabilir (bk. Madde 5.1.2).

Gizlilik hususlarına hassasiyet gösterme kapsamında gerçek bilgi güvenliği ihlal olaylarından anekdotlar, kullanıcı farkındalık eğitiminde (bk. Madde 7.2.2) kullanılabilir. Bu farkındalık eğitiminde; ne olabileceği, bu tür ihlal olaylarına nasıl müdahale edileceği ve gelecekte bunların nasıl önleneceği örnek olarak verilebilir.

16.1.7 Kanıt toplama

Kontrol

Kuruluş kanıt olarak kullanılabilecek bilginin teşhisi, toplanması, edinimi ve korunması için prosedürler tanımlamalı ve uygulamalıdır.

Uygulama kılavuzu
Disiplin ve yasal işlem tatbiki amacıyla kanıt üzerinde çalışırken uygulanacak iç prosedürleri geliştirilmeli ve takip edilmelidir.

Genel olarak; kanıt ile ilgili prosedürler, ortam ve aygıtların farklı türleri ve cihazların durumu (örneğin; cihazın açık veya kapalı olması) ile uyumlu kanıt tespiti, toplama, edinim ve korunma proseslerini sağlar. Prosedürler aşağıdaki hususları dikkate almalıdır:

a) Delil zinciri,
b) Kanıt emniyeti,
c) Personel emniyeti,
d) İlgili personellerin rolleri ve sorumlulukları,
e) Personel yeterliliği,
f) Dokümantasyon,
g) Bilgilendirme.

Toplanan kanıtların değerinin güçlendirilmesine yönelik olarak, mümkünse sertifikasyon ya da diğer personel nitelikleri ile ilgili yöntemler ve araçların kullanımı beklenmelidir.

Adli kanıtlar, kurumsal ya da hukuk sistemi sınırlarını aşabilir. Böyle durumlarda, kuruluş adli delil olarak gerekli bilgileri toplama yetkisine sahip olduğundan emin olmalıdır. Delilerin, farklı hukuk sistemleri arasında kabul olasılığını azami ölçüde tutmak için farklı hukuk gereksinimlerine dikkat edilmelidir.

Diğer bilgiler
Tespit etme, muhtemel kanıtların kabulü ve dokümantasyonu için arama içeren prosestir. Toplama, olası kanıtları içerebilen fiziksel öğeleri bir araya getirme prosesidir. Edinim, tanımlanmış bir dizi içindeki verilerin kopyalarının oluşturulması prosesidir. Muhafaza, olası delillerin bütünlüğünün ve ilk durumunun, sağlanması ve güvence altına alınması prosesidir.

Bilgi güvenliği olayı ilk tespit edildiğinde, bu olayın dava nedeni olup olmayacağı açık olmayabilir. Bu nedenle, ihlal olayının ciddiyetinin fark edilmesinden önce gerekli kanıtların kasıtlı ya da kazayla imha edilmesi tehlikesi vardır. Tüm öngörülen yasal işlemlerde, bir avukat ya da polisi erkenden sürece dâhil etmek ve gereken kanıt ile ilgili tavsiye almak önerilir.

Sayısal kanıtların tanımlanması, belirlenmesi, toplanması, edinimi ve korunması için kılavuzluk ISO/IEC 27037 [24] standardında sağlanmıştır.

17 İş sürekliliği yönetiminin bilgi güvenliği hususları

17.1 Bilgi güvenliği sürekliliği

Amaç: Bilgi güvenliği sürekliliği, kuruluşun iş sürekliliği yönetim sistemlerinin içerisine dâhil edilmelidir.

17.1.1 Bilgi güvenliği sürekliliğinin planlanması

Kontrol
Kuruluş olumsuz durumlarda, örneğin bir kriz ve felaket durumunda, bilgi güvenliği ve bilgi güvenliği yönetimi sürekliliğinin gereksinimlerini belirlemelidir.

Uygulama kılavuzu
Bir kuruluş, bilgi güvenliği sürekliliğinin sağlanmasının, iş sürekliliği yönetim sürecinde mi ya da felaket kurtarma yönetim sürecinde mi ele alınacağını belirlemelidir. Bilgi güvenliği gereksinimleri, iş sürekliliği ve felaket kurtarma için planlama yaparken belirlenmelidir.

Resmi iş sürekliliği ve felaket kurtarma planlaması olmadığı durumda, bilgi güvenliği yönetimi olumsuz durumlarda normal işletme şartları ile karşılaştırıldığında bilgi güvenliği gereksinimlerinin aynı kalması gerektiğini varsayılmalıdır. Alternatif olarak, bir kuruluş olumsuz durumlarda uygulanabilir bilgi güvenliği gereksinimlerini belirlemek amacıyla bilgi güvenliği hususları için bir iş etki analizi gerçekleştirebilir.

Diğer bilgiler
Bilgi güvenliği için hazırlanacak 'ek' iş etki analizine yönelik zaman ve çabayı azaltmak amacıyla, normal iş sürekliliği yönetimi ya da felaket kurtarma yönetimi iş etki analizi kapsamında bilgi güvenliği hususlarının ele alınması tavsiye edilir. Bu durum; bilgi güvenliği süreklilik gereksinimlerinin, iş sürekliliği yönetimi ya da felaket kurtarma yönetimi prosesinde açıkça formüle edilmesini gerektirir.

İş sürekliliği yönetimi hakkında bilgi ISO/IEC 27031, [14] ISO 22313 [9] ve ISO 22301 [8]'de bulunabilir.

17.1.2 Bilgi güvenliği sürekliliğinin uygulanması

Kontrol
Kuruluş, olumsuz bir olay süresince bilgi güvenliği için istenen düzeyde sürekliliğin sağlanması amacıyla prosesleri, prosedürleri ve kontrolleri oluşturmalı, yazılı hale getirmeli, uygulamalı ve sürdürmelidir.

Uygulama kılavuzu
Kuruluş, aşağıdakileri temin etmelidir:

a) Yıkıcı olayların azaltılması ve müdahale edecek gerekli yetkiye, deneyime ve yetkinliğe sahip personel için yeterli bir yönetim yapısı mevcut olmalıdır,
b) İhlal olayına müdahale edecek gerekli sorumluluk, yetkiye ve yeterliliğe sahip personel bir ihlal olayını yönetmek ve bilgi güvenliğini sağlamak için aday gösterilir,
c) Kuruluş, yıkıcı bir olayı yönetmek ve önceden belirlenmiş bir seviyede bilgi güvenliğini koruyacak şekilde yönetim tarafından onaylanmış bilgi güvenliliği süreklilik hedeflerine dayalı olarak yazılı hale getirilmiş planlar, müdahale ve kurtarma prosedürleri geliştirilmeli ve onaylanmalıdır (bk. Madde 17.1.1),

Kuruluş, bilgi güvenliği süreklilik gereksinimleri ile uyumlu aşağıdaki hususları oluşturmalı, yazılı hale getirilmeli, uygulamalı ve sürdürmelidir:
a) İş sürekliliği ya da felaket kurtarma prosesleri, prosedürleri ve destekleyici sistemler ve araçlarda yer alan bilgi güvenliği kontrolleri,
b) Olumsuz bir durum sırasında mevcut bilgi güvenliği kontrollerini sürdürmek için prosesler, prosedürler ve uygulama değişiklikleri,
c) Olumsuz bir durum sırasında sürdürülemeyen bilgi güvenliği kontrolleri için telafi edici kontroller.

Diğer bilgiler
İş sürekliliği ya da felaket kurtarma kapsamında, belirli prosesler ve prosedürler tanımlanmış olabilir. Bu prosesler ve prosedürler tarafından işlenen ya da bunlara özgü bilgi sistemlerinin desteklediği bilgiler korunmalıdır. Bu nedenle, bir kuruluş iş sürekliliği ya da felaket kurtarma prosesleri ve prosedürlerini uygularken ve sürdürürken bilgi güvenliği uzmanlarından yararlanmalıdır.

Uygulanmakta olan bilgi güvenliği kontrolleri olumsuz bir durum sırasında çalışmaya devam etmelidir. Güvenlik kontrolleri, bilgi güvenliğini sağlamayı sürdüremiyorsa, bilgi güvenliğini kabul edilebilir bir seviyede tutmak için diğer kontroller oluşturulmalı, uygulanmalı ve sürdürülmelidir.

17.1.3 Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi

Kontrol
Kuruluş, oluşturulan ve uygulanan bilgi güvenliği sürekliliği kontrollerinin, olumsuz olaylar durumunda geçerli ve etkili olduğundan emin olmak için belirli aralıklarda doğruluğunu sağlamalıdır.

"Uygulama kılavuzu"
İşletimsel ya da süreklilik bağlamında kurumsal, teknik, prosedürel ve proses değişiklikleri bilgi güvenliği süreklilik gereksinimlerinde değişikliklere yol açabilir. Bu gibi durumlarda, bilgi güvenliği için prosesler, prosedürler ve kontrollerin sürekliliği bu değişen ihtiyaçlara karşı gözden geçirilmelidir.

Kuruluşlar kendi bilgi güvenliği yönetimi sürekliliğini aşağıdaki hususlarla doğrulamalıdır:

a) Bilgi güvenliği süreklilik hedefleri ile uyumluluğundan emin olmak için bilgi güvenliği süreklilik prosesleri, prosedürleri ve kontrollerinin işlevselliğini tecrübe ve test etme,
b) Çalışan bilgi güvenliği sürekliliği prosesleri, prosedürleri ve kontrolleri performanslarının bilgi güvenliği süreklilik hedefleri ile tutarlı olmasını temin etmek için bilgi birikimi ve rutinleri tecrübe ve test etme,
c) Bilgi sistemleri, bilgi güvenliği prosesleri, prosedürleri ve kontrolleri ya da iş sürekliliği yönetimi/felaket kurtarma yönetim prosesi ve çözümlerin değişiminde bilgi güvenliği sürekliliği tedbirlerinin geçerliliğini ve etkinliğini gözden geçirme.

Diğer bilgiler
Bilgi güvenliği süreklilik kontrollerinin doğrulanması, genel bilgi güvenliği test ve doğrulamasından farklıdır ve değişim testleri dışında yapılmalıdır. Mümkünse, kurumun iş sürekliliği ya da felaket kurtarma testleri ile bilgi güvenliği sürekliliği kontrollerinin doğrulamasını bütünleştirmek tercih edilir.

17.2 Yedek fazlalıklar

Amaç: Bilgi işleme tesislerinin erişilebilirliğini temin etmek.

17.2.1 Bilgi işleme tesislerinin erişilebilirliği

Kontrol
Bilgi işleme tesisleri, erişilebilirlik gereksinimlerini karşılamak için yeterli fazlalık ile gerçekleştirilmelidir.

Uygulama kılavuzu
Kuruluşlar bilgi sistemlerinin erişilebilirliği için iş gereksinimlerini belirlemelidir. Mevcut sistemlerin mimarisi kullanılarak erişilebilirliğinin garanti edilemediği yerlerde yedekli bileşenler ya da mimariler düşünülmelidir. Uygulanabildiğinde, yedekli bilgi sistemleri, bir bileşen çalışmaması durumunda diğer bir bileşenin onun yerine amaçlanan şekilde çalışmasını sağlamak için test edilmelidir.

Diğer bilgiler
Bilgi sistemleri tasarlanırken yedeklilik fazlalıkların uygulanması, bilgi ve bilgi sistemlerinin bütünlüğe ya da gizliliğe yönelik risklerin ortaya çıkarabilir.

18 Uyum

18.1 Yasal ve sözleşmeye tabi gereksinimlere uyum

Amaç: Yasal, meşru, düzenleyici veya sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek.

18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama

Kontrol
İlgili tüm yasal, meşru, düzenleyici, sözleşmeden doğan gereksinimleri ve kuruluşun bu gereksinimleri karşılama yaklaşımı her bilgi sistemi ve kuruluş için açıkça tanımlanmalı, yazılı hale getirilmeli ve güncel tutulmalıdır.

Uygulama kılavuzu
Özel kontroller ve bireysel sorumlulukları karşılayan gereksinimler tanımlanmalı ve yazılı hale getirilmelidir.

Yöneticiler, kendi iş kolu için gereksinimleri karşılamak üzere kuruluşları için geçerli olan tüm mevzuatı tespit etmelidir. Kuruluş diğer ülkelerde iş yapıyorsa, yöneticileri ilgili tüm ülkelerdeki uyumu dikkate almalıdır.

18.1.2 Fikri mülkiyet hakları

Kontrol
Fikri mülkiyet hakları ve tescilli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalardan doğan gereksinimlere uyum sağlamak için uygun prosedürler uygulanmalıdır.

Uygulama kılavuzu
Fikri mülkiyet hakları olarak kabul edilen herhangi bir materyali korumak için aşağıdaki kılavuzluğa dikkat edilmelidir:

a) Yazılım ve bilgi ürünlerinin yasal kullanımını belirleyen fikri mülkiyet hakları uyum politikasının yayınlanması,
b) Telif haklarının ihlal edilmemesini temin etmek için sadece bilinen ve saygın kaynaklardan yazılım satın alınması,
c) Fikri mülkiyet haklarını korumak için politikalara dair farkındalığın sürdürülmesi ve bunları ihlal eden personele karşı disiplin işlemi uygulanacağının bildirilmesi,
d) Uygun varlık envanterlerinin sürdürülmesi ve fikri mülkiyet hakkı korunması gereksinimi olan tüm varlıkların belirlenmesi,
e) Lisansların, ana disklerin, kılavuzların ve benzerlerinin sahipliğine dair ispat ve delillerin muhafaza edilmesi,
f) Lisans çerçevesinde izin verilen kullanıcı sayısının aşılmamasını sağlayan kontrollerin uygulanması,
g) Yalnızca yetkili yazılım ve lisanslı ürünlerin yüklenmiş olduğunun gözden geçirilmesi,
h) Uygun lisans şartlarının devamının sağlanması için bir politika belirlenmesi,
i) Yazılımların diğer taraflara transferi veya yok edilmesi için bir politika sağlanması,
j) Açık ağlardan elde edilen bilgi ve yazılım koşul ve şartlarına uyum sağlanması,
k) Telif hakkı yasası tarafından izin verilen dışında ticari çekimlerden (fil, ses) bir bölüm kopya alma şeklinde çoğaltma ya da başka bir biçime dönüştürme yapılmaması,
l) Telif hakkı yasası tarafından izin verilen dışında kitapların, makalelerin, raporların ve diğer belgelerin tam veya kısmen kopyalanmaması.

Diğer bilgiler
Fikri mülkiyet hakları; yazılım veya belge telif haklarını, tasarım haklarını, markaları, patentleri ve kaynak kod lisanslarını kapsar.

Fikri mülkiyet hakkına sahip yazılım ürünleri genellikle özel lisans şartlarının belirtildiği lisans anlaşmaları altında tedarik edilir. Örneğin; belirtilen makinalarda ürünün kullanımının sınırlandırılması ya da sadece yedekleme kopyası oluşturmak için kopyalama sınırlandırılması. Kuruluş tarafından geliştirilen yazılım için fikri mülkiyet haklarının önemi ve farkındalık personele duyurulmalıdır.

Yasal, düzenleyici ve sözleşme gereksinimleri fikri mülkiyet hakkına sahip materyallerin kopyalanmasına sınırlama getirebilir. Özellikle, bu sınırlama yalnızca kuruluş tarafından geliştirilen materyallerin ya da kuruluşa geliştirici tarafından sağlanan lisanslı ürünlerin kullanımını gerektirebilir. Telif hakkı ihlali konusu, parasal cezaya ve ceza kovuşturmasına yol açan yasal işleme neden olabilir.

18.1.3 Kayıtların korunması

Kontrol
Kayıtlar kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı yasal, düzenleyici, sözleşmeden doğan gereksinimlere ve iş şartlarına uygun olarak korunmalıdır.

Uygulama kılavuzu
Belirli kurumsal kayıtların korunmasına karar verilirken, kurumsal sınıflandırma düzenine karşılık gelen bir sınıflandırma düzeni dikkate alınmalıdır. Kayıtlar; örneğin muhasebe kayıtları, veri tabanı kayıtları, işlem kayıtları, denetim kayıtları ve çalışma prosedürleri gibi kayıt tipleri şeklinde sınıflandırılmalıdır. Her bir kayıt sınıfı; saklama süreleri, ayrıntıları ve kâğıt, mikrofilm, manyetik, optik gibi izin verilebilir saklama ortamı türü ile birlikte saklanmalıdır. Şifreli arşiveler ve sayısal imzalar (bk. Madde 10) ile ilişkili tüm kriptografik anahtarlar ve programlar, kayıtların saklanması süresince kayıtların şifresini çözmek için saklanmalıdır.

Kayıtların saklanması için medya kullanımında, medya biçiminin zarar görmesi ihtimali göz önüne alınmalıdır. Saklama ve kullanma prosedürleri üreticinin tavsiyelerine uygun olarak yapılmalıdır.

Elektronik saklama ortamı seçildiğinde; gelecekteki teknoloji değişiklikleri nedeniyle oluşabilecek kayıplardan korumak için saklama dönemi boyunca veriye erişmeyi (hem ortam hem de biçim okunabilirliği olarak) sağlamak amacıyla prosedürler oluşturulmalıdır.

Veri saklama sistemleri seçilirken, gerekli veriyi kabul edilebilir bir zaman diliminde ve biçiminde geri getirebilme gereksinimlerinin karşılanmasına bağlı olarak seçilmesi hususuna dikkat edilmelidir.

Saklama ve işleme sistemi, uygulanabildiği durumlarda ulusal ya da bölgesel yasalara tanımlamaya uygun olarak kayıtların ve kayıtların saklama sürelerinin tanımlanmasını temin etmelidir. Bu sistem, kuruluş tarafından belirli bir süre sonra ihtiyaç duyulmayan kayıtların uygun şekilde yok edilmesine izin vermelidir.

Bu kayıtların korunması amacını karşılamak için aşağıdaki adımlar kuruluşta takip edilmelidir:

a) Kayıtların ve bilgilerin tutulması, saklanması, işlenmesi ve yok edilmesi için kılavuz yayınlanmalıdır,
b) Kayıtların muhafaza edilmesi için kayıtların ve zaman periyotlarının tanımlandığı saklama çizelgesi hazırlanmalıdır,
c) Önemli bilgi kaynaklarının envanteri tutulmalıdır,

Diğer bilgiler
Bazı kayıtların; yasal, düzenleyici veya sözleşme gereklerini karşılamak hem de temel iş faaliyetlerini desteklemek için güvenli bir şekilde muhafaza edilmesi gerekebilir. Bir kuruluşun yasal ve düzenleyici kurallara uygun şekilde çalıştığına dair kanıt, olası yasal ve suç teşkil eden eylemlere karşı savunmanın temin edilmesi veya bir kuruluşun paydaşlar, dış taraflar ve denetçilere kuruluşun finansal durumunu teyit etmesi için gereken kayıtlar örnek olarak verilebilir. Ulusal yasa ve düzenlemeler, bilgi saklama için zaman periyodu ve veri içeriği belirleyebilir.

Kurumsal kayıtların yönetimi hakkında daha fazla bilgi ISO 15489-1[5] standardında bulunabilir.

18.1.4 Kişi tespit bilgisinin mahremiyeti ve korunması

Kontrol
Kişi tespit bilgisinin mahremiyeti ve korunması, uygulanabilen yerlerde ilgili yasa ve düzenlemeler ile sağlanmalıdır.

Uygulama kılavuzu
Kişi tespit bilgisinin mahremiyeti ve korunması için bir kuruluşa ait veri politikası geliştirilmeli ve uygulanmalıdır. Bu politika, kişi tespit bilgisinin işlenmesinde yer alan tüm personele bildirilmelidir. Kişisel mahremiyetin ve kişi tespit bilgilerinin korunmasına dair bu politikaya ve ilgili tüm mevzuata ve düzenlemelere uyum, uygun yönetim yapısı ve kontrol gerektirir. Genellikle, mahremiyet yöneticis gibi bu işten sorumlu olacak bir kişinin atanması ile iyi bir sonuç elde edilebilir. Bu kişi; yöneticilere, kullanıcılara ve hizmet sağlayıcılara kendi bireysel sorumlulukları ve takip etmeleri gereken prosedürleri hakkında rehberlik etmelidir. Kişi tespit bilgisini işlemek için sorumluluklar ve mahremiyet ilkelerinin sağlanması hususunda farkındalık, ilgili yasal ve düzenlemelere uygun olarak ele alınmalıdır. Kişi tespit bilgilerini korumak için uygun teknik ve kurumsal önlemler alınmalıdır.

Diğer bilgiler
ISO/IEC 29100[25] standardı, bilgi ve iletişim teknolojisi sistemlerinde kişi tespit bilgisinin korunmasına yönelik yüksek seviyeli bir çerçeve sağlar. Bazı ülkeler, kişi tespit bilgisinin toplanması, işlenmesi ve iletiminde kontrolleri yerleştirmek için düzenlemeler yapmıştır (Genellikle bu bilgilerden bilgilerin sahibi tespit edilebilir). İlgili ulusal düzenlemelere bağlı olarak, bu tür kontroller kişi tespit bilgisini toplayan, işleyen ve dağıtan kişiler sorumluluklar getirebilir ve aynı zamanda diğer ülkelere kişi tespit bilgisinin transferi aktarılmasını imkânını sınırlayabilir.

18.1.5 Kriptografik kontrollerin düzenlenmesi

Kontrol
Kriptografik kontroller tüm ilgili sözleşmelere, yasalara ve düzenlemelere uyumlu bir şekilde kullanılmalıdır.

Uygulama kılavuzu
Aşağıdaki hususlar ilgili anlaşmalar, yasalar ve düzenlemeler ile uyum için dikkate alınmalıdır:

a) Kriptografik fonksiyonların gerçekleştirilmesi amacıyla kullanılan bilgisayar donanım ve yazılımının ithalat ve ihracatı üzerindeki kısıtlamalar,
b) Kriptografik fonksiyonların üzerine eklenmesine imkân tanıyacak şekilde tasarlanmış bilgisayar donanım ve yazılımı ithalat ve ihracatı üzerindeki kısıtlamalar,
c) Şifreleme kullanımıyla ilgili kısıtlamalar,
d) İçeriğin gizliliğinin sağlanabilmesi için donanım ya da yazılım tarafından şifrenmiş olan bilgiye ülkelerin yetkili kurumları tarafından zorunlu veya isteğe bağlı erişim yöntemleri.

İlgili yasalara ve düzenlemelere uyulması açısından hukuki danışmanlık alınmalıdır. Şifrelenmiş bilgi ya da şifreleme kontrollerinin farklı hukuki sistemler arasında geçişinden önce bu hukuki danışmanlık alınmalıdır.

18.2 Bilgi güvenliği gözden geçirmeleri

Amaç: Bilgi güvenliğinin kurumsal politika ve prosedürler uyarınca gerçekleştirilmesini ve yürütülmesini sağlamak.

18.2.1 Bilgi güvenliğinin bağımsız gözden geçirilmesi

Kontrol
Kuruluşun bilgi güvenliğine ve uygulamasının (örneğin; bilgi güvenliği için kontrol amaçları, kontroller, politikalar, prosesler ve prosedürler) yönetimine olan yaklaşımı belirli aralıklarla veya önemli değişiklikler meydana geldiğinde bağımsız bir şekilde gözden geçirilmelidir.

Uygulama kılavuzu
Bağımsız gözden geçirme yönetim tarafından başlatılmalıdır. Bu tür bağımsız bir gözden geçirme kuruluşun bilgi güvenliği yaklaşımının uygunluğu, yeterliliği ve etkinliği sürekli sağladığından emin olmak için gereklidir. Gözden geçirme, politika ve kontrol hedefleri de dâhil olmak üzere güvenlik yaklaşımında ihtiyaç duyulan değişiklikleri yapmak ve geliştirmeler için fırsatlar içermelidir.

Gözden geçirme, incelenen alandan bağımsız bireyler tarafından yapılmalıdır. Örneğin; iç denetim fonksiyonu, bağımsız bir yönetici ya da bu tip bir gözden geçirme konusunda uzmanlaşmış dış taraf olan bir kuruluş tarafından yapılmalıdır. Bu gözden geçirmeyi yapan kişiler uygun beceri ve deneyime sahip olmalıdır.

Bağımsız gözden geçirmenin sonuçları kayıt edilmeli ve gözden geçirmeyi başlatan yönetime rapor halinde sunulmalıdır. Bu kayıtlar saklanmalıdır.

Bağımsız gözden geçirme, bilgi güvenliğini yönetmek için kuruluşun yaklaşımının ve uygulamasının yetersiz olduğunu tespit ederse (örneğin bu yetersizlikler; yazılı hale getirilmiş amaçların ve gereklerin karşılanmaması veya bilgi güvenliği politikalarında ifade edilen bilgi güvenliği yönü ile uyumlu olmaması şeklinde olabilir (bk. Madde 5.1.1)), yönetim düzeltici faaliyetleri dikkate almalıdır.

Diğer bilgiler
Bağımsız bir gözden geçirme için ISO/IEC 27007 [12], “Bilgi güvenliği yönetim sistemi denetimi için kılavuz” ve ISO/IEC TR 27008 TR [13] “Bilgi güvenliği kontrolleri denetimi için kılavuz” kılavuzluk sağlar.

18.2.2 Güvenlik politikaları ve standartları ile uyum

Kontrol
Yöneticiler kendi sorumluluk alanlarında bulunan, bilgi işleme ve prosedürlerin, uygun güvenlik politikaları, standartları ve diğer güvenlik gereksinimleri ile uyumunu düzenli bir şekilde gözden geçirmelidir.

Uygulama kılavuzu
Yöneticiler; politikalar, standartlar ve diğer ilgili düzenlemelerde tanımlanan bilgi güvenliği gereklerinin karşılanmasının ne şekilde gözden geçirileceğini tespit etmelidir.

Gözden geçirme sonucunda herhangi bir uygunsuzluk bulunursa, yöneticiler:

a) Uyumsuzluk nedenini belirlemeli,
b) Uyumluluğun sağlanması için gereken eylemleri değerlendirmeli,
c) Uygun düzeltici faaliyetler uygulamalı,
d) Herhangi bir eksikliğin ya da zayıflığın tespitini ve düzeltici faaliyetin etkinliğini doğrulamak için gözden geçirmeli.

Yöneticiler tarafından gerçekleştirilen gözden geçirmeler ve düzeltici faaliyetlerin sonuçları kaydedilmeli ve bu kayıtlar muhafaza edilmelidir. Yöneticiler, bağımsız gözden geçirme kendi sorumluluk alanlarında gerçekleştiğinde gözden geçirme yapan kişilere sonuçları bildirmelidir (bk. Madde 18.2.1).

Diğer bilgiler
Sistem kullanımının işletiminin izlenmesi Madde 12.4'da ele alınmıştır.

18.2.3 Teknik uyum gözden geçirmesi

Kontrol
Kuruluşun bilgi güvenliği politika ve standartları ile uyumluluğu bilgi sistemleri düzenli bir şekilde gözden geçirilmelidir.

Uygulama kılavuzu
Teknik uyum bir teknik uzman tarafından sonraki gözden geçirmeler için teknik raporlar oluşturmak amacıyla tercihen kullanılan otomatik araçlar yardımı ile gözden geçirilmelidir. Alternatif olarak, deneyimli bir sistem mühendisi tarafından manuel gözden geçirilebilir (gerekirse uygun yazılım araçları ile desteklenen).

Sızma testleri veya açıklık değerlendirmeleri kullanılıyorsa, bu tür faaliyetlerin sistemin güvenliğini ihlal edebileceği konusuna dikkat edilmelidir. Bu tür testler planlanmalı, yazılı hale getirilmeli ve tekrarlanabilmelidir.

Herhangi bir teknik uyum gözden geçirilmesi sadece işi bilen, yetkili personel tarafından gerçekleştirilmeli ya da bu kişilerin gözetiminde olmalıdır.

Diğer bilgiler
Teknik uyum kontrolü, donanım ve yazılım kontrollerinin doğru biçimde uygulanmasını temin etmek için işletimdeki sistemlerin incelenmesini içerir. Bu tip uyum gözden geçirmesi, özel teknik uzman deneyimi gerektirir.

Uyumluluk gözden geçirmeleri; sızma testleri ve açıklık değerlendirmeleri gibi konuları kapsar. Bu amaç için sözleşmeli özel bağımsız uzmanlar tarafından uyumluluk testleri yürütülebilir. Bu, sistem yer alan açıklıkların tespiti ve bu güvenlik açıklıkları nedeniyle yetkisiz erişimi önlemede kontrollerin ne kadar etkili olduğunu denetlemek için yararlı olabilir.

Sızma testleri ve açıklık değerlendirmeleri belirli bir zaman ve durumdaki bir sistemin anlık görüntüsünü sağlar. Anlık görüntü aslında sızma girişimi/girişimleri süresince test edilen sistemin bazı bölümleri ile sınırlıdır. Sızma testi ve açıklık değerlendirmeleri risk değerlendirmesinin yerini tutmaz.

ISO/IEC 27008 [13] teknik uyum gözden geçirme konusunda özel bir kılavuzluk sağlar.

Kaynaklar

[1] ISO/IEC *Directives, Part 2*

[2] ISO/IEC 11770-1, *Information technology Security techniques — Key management — Part 1: Framework*

[3] ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[4] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

[5] ISO 15489-1, *Information and documentation — Records management — Part 1: General*

[6] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[7] ISO/IEC 20000-2,1)*Information technology — Service management — Part 2: Guidance on the application of service management systems*

[8] ISO 22301, *Societal security — Business continuity management systems — Requirements*

[9] ISO 22313, *Societal security — Business continuity management systems — Guidance*

[10] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[11] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[12] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[13] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[14] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[15] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[16] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[17] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threat (tehdit)s, design techniques and control issues*

[18] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*

[19] ISO/IEC 27033-5, *Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Network (VPNs)*

[20] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[21] ISO/IEC 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

[22] ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements*
[23] ISO/IEC 27036-3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security*

[24] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[25] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[26] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[27] ISO 31000, *Risk management — Principles and Guidelines*