TÜRK STANDARDLARI ENSTİTÜSÜ

TS EN ISO/IEC 27001:2017

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ TEMEL EĞİTİMİ

İÇERİK

Bölüm 1: Giriş

- TSE Hakkında, Eğitimin Amacı, Genel Yaklaşım, Yüksek Seviyeli Yapı, PUKÖ Modeli, Neden ÇYS?

Bölüm 2: Standard Maddeleri

- Madde 1.Kapsam, Madde 2.Atıf Yapılan Standardlar, Madde 3. Terimler ve Tarifler

Bölüm 3: Standard Maddeleri

- Madde 4.Kuruluş Bağlamı, Madde 5.Liderlik

Bölüm 4: Standard Maddeleri

- Madde 6.Planlama

Bölüm 5: Standard Maddeleri

- Madde 7.Destek, Madde 8.Operasyon

Bölüm 6: Standard Maddeleri

- Madde 9.Performans Değerlendirme, Madde 10.İyileştirme

TÜRK STANDARDLARI ENSTİTÜSÜ

Kısa adı TSE olan
TÜRK STANDARDLARI ENSTİTÜSÜ,
1954 yılında TOBB bünyesinde kurulmuş,1960 yılında 132 sayılı kanun ile bugünkü,*"özel hukuk hükümlerine göre yönetilen kamu kurumu*" niteliğini kazanmıştır.

TSE'nin merkezi **Ankara**'da olup,
Yurt içinde ; Bölge koordinatörlükleri, il müdürlükleri ve bölge laboratuvarları
Yurt dışında, temsilcilikleri ve çözüm ortakları mevcuttur.

Uluslararası Standartlar Teşkilatı

Uluslararası Elektroteknik Komisyonu

Avrupa Standartlar Komitesi

Avrupa Elektroteknik Standardizasyon Komitesi

Uluslararası Belgelendirme Ağı

Avrupa Kalite Teşkilatı

İslam Ülkeleri Standart ve Metroloji Enstitüsü

Bölgelerarası Standardizasyon Birliği

TSE, Belgelendirme faaliyetlerinin büyük bölümünü TÜRKAK tan akredite olarak yürütmektedir

EĞİTİMİN AMACI

TS EN ISO/IEC 27001:2017 “Bilgi güvenliği yönetim sistemleri – Şartlar ve kullanım kılavuzu” standardının,

- Bilgi güvenliği performansını arttırabilmek,
- Bilgi güvenliği sorumlulukları sürdürülebilmek,
- Bilgi güvenliğine katkı sağlayacak sistematik bir anlayışla yönetim sağlayabilmek,

amaçlarına yönelik olarak anlaşılabilirliğinin sağlanması,

Uygulamaya yönelik örneklerin paylaşılması ve pratik çalışmaların yapılması

ISO 27001 TARİHÇESİ

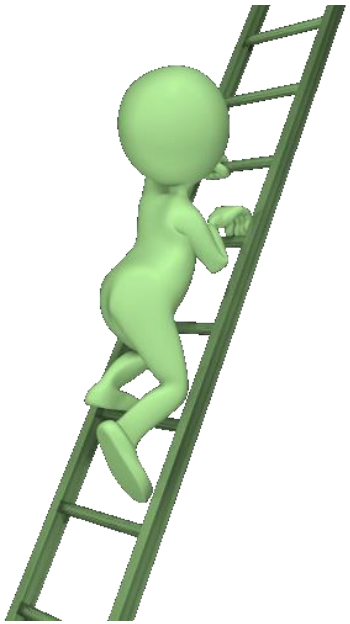
ISO/IEC 17799:2005 Bilgi teknolojisi - Bilgi güvenliği yönetimi için uygulama prensipleri

ISO/IEC 27001:2005 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler

ISO/IEC 27001:2013 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler

EN ISO/IEC 27001:2017 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinimler

YÜKSEK SEVİYELİ YAPI



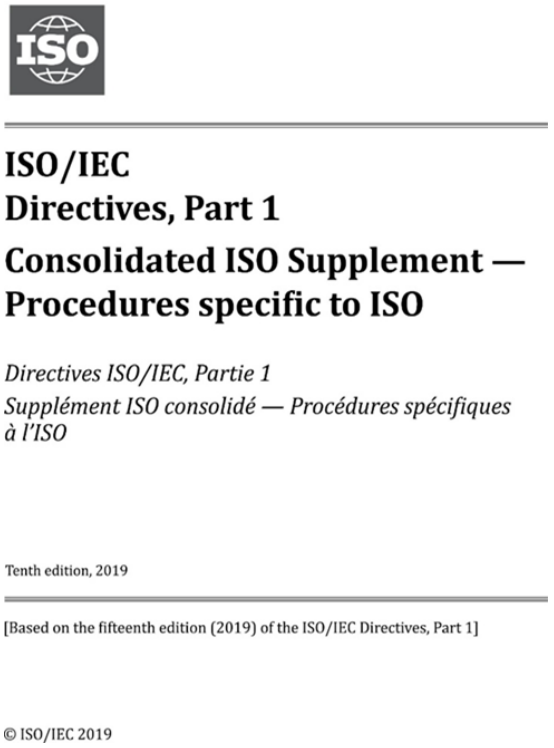
- Tüm yönetim sistemi standardları için ortak yapı (10 madde)
- Temel tanımlarda terminoloji birliği
- Ortak tanımlayıcı alt başlıklar
- Değişen şartlara uyum kabiliyeti
- Rekabetçi şartlara uyum
- Diğer yönetim sistemleriyle entegrasyonda kolaylık

AMAÇ: Uygulayıcılara kolaylık sağlanması

TÜRK STANDARDLARI ENSTİTÜSÜ

YÜKSEK SEVİYELİ YAPI STANDARD MADDELERİ

1. Kapsam
2. Atıf Yapılan Standardlar/Dokümanlar
3. Terimler ve Tarifler
4. Kuruluşun Bağlamı
5. Liderlik
6. Planlama
7. Destek
8. Operasyon
9. Performans Değerlendirme
10. İyileştirme



ISO

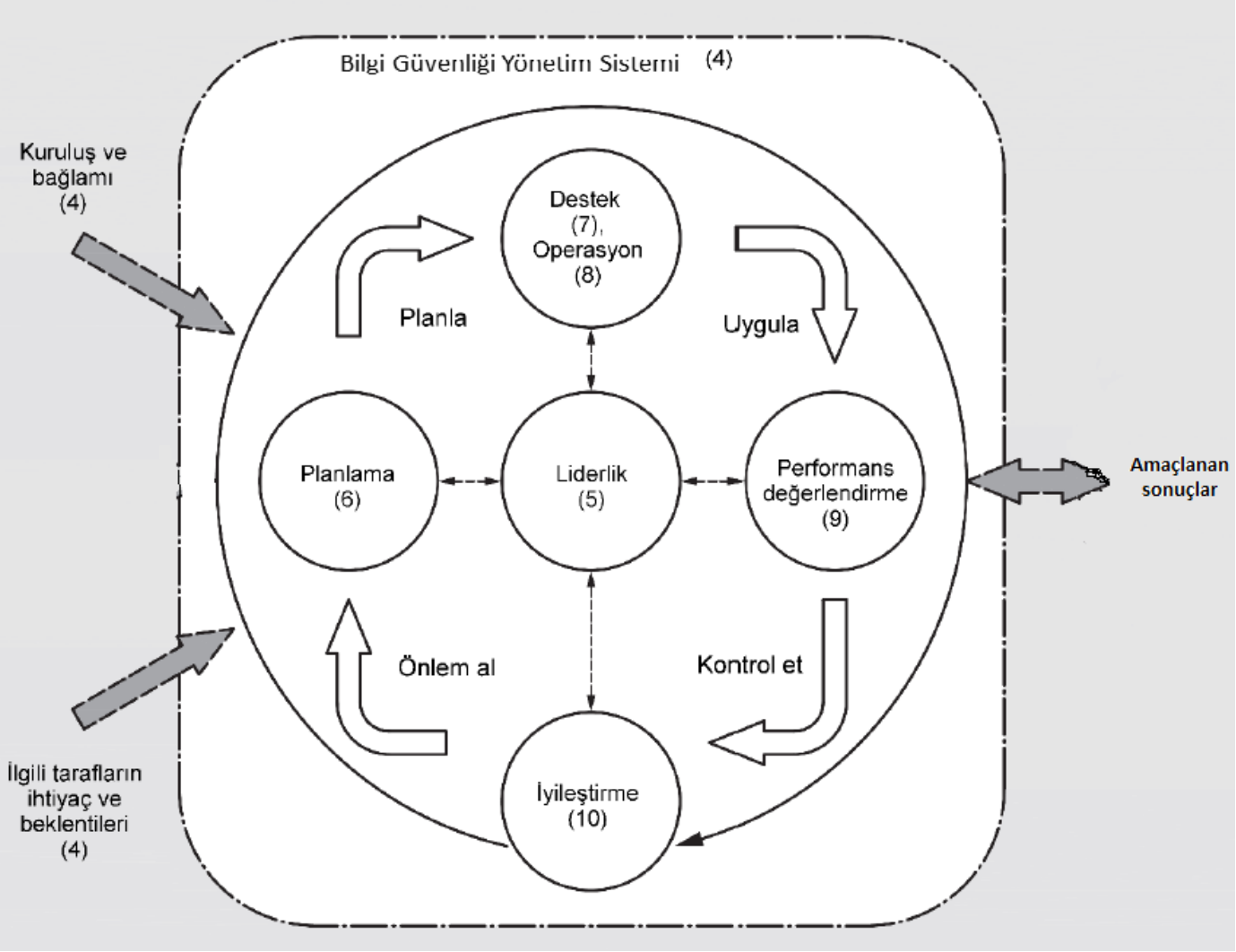
ISO/IEC
Directives, Part 1
Consolidated ISO Supplement — Procedures specific to ISO

Directives ISO/IEC, Partie 1
Supplément ISO consolidé — Procédures spécifiques à l'ISO

Tenth edition, 2019

[Based on the fifteenth edition (2019) of the ISO/IEC Directives, Part 1]

© ISO/IEC 2019



PUKÖ döngüsü içerisinde bu standardın yapısının gösterimi

PUKÖ döngüsü kısaca aşağıdaki şekilde açıklanabilir:

- **Planla:** Kuruluş politikalarına prosedürlerine göre sonuçlar elde etmek için sistemin amacı ve prosesleri ile ihtiyaç duyulan kaynakların oluşturulması, risk ve fırsatların tanımlanması ve belirlenmesi,

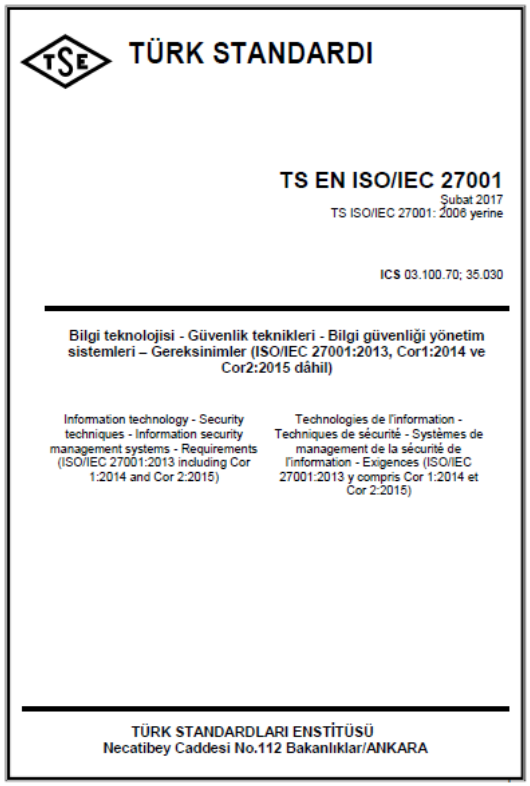
- **Uygula:** Planlananın uygulanması,

- **Kontrol et:** Politikalar, amaçlar, şartlar ve planlanan faaliyetlere karşı, prosesler ve sonuçlanan ürünlerin izlenmesi, (uygulanabildiğinde) ölçülmesi ve sonuçların rapor edilmesi,

- **Önlem al:** Gerektiğinde, performansı iyileştirmek için faaliyetlerin yapılması.

NEDEN BGYS ?

- ✓ Piyasada farklılaşma / itibar
- ✓ Üst yönetim ve müşteri gereksinimlerinin karşılanması
- ✓ Küresel kabul görmüş tek standart
- ✓ Bilgi güvenliği bilinci ile odaklanmış çalışanlar
- ✓ Yasal zorunlulukların karşılanması
- ✓ Zayıflıkların saptanıp giderilmesi/ Yeni ortaya çıkan tehdit ve açıklıklara hazırlıklı olmak
- ✓ Kurumsal yönetim (Uygulamaya konmuş politika ve prosedürler ile belirlenmiş sorumluluk ve yetkiler)
- ✓ Üst yönetimin Bilgi Güvenliğini sahiplenmesi
- ✓ Daha iyi güvenlik bilinci oluşması
- ✓ Diğer yönetim sistemleri ile kaynakların birleştirilmesi
- ✓ Sistemin başarısını ölçme mekanizması
- ✓ Bilgi güvenliği yönetim sistemi, bilginin gizliliği, bütünlüğü ve erişilebilirliğini risk yönetimi prosesini uygulayarak muhafaza eder ve ilgili taraflara risklerin doğru bir şekilde yönetildiğine dair güvence verir



TÜRK STANDARDI

TS EN ISO/IEC 27001

Şubat 2017

TS ISO/IEC 27001: 2006 yerine

ICS 03.100.70; 35.030

Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler (ISO/IEC 27001:2013, Cor1:2014 ve Cor2:2015 dâhil)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

TÜRK STANDARDLARI ENSTİTÜSÜ
Necatibey Caddesi No.112 Bakanlıklar/ANKARA

TSE
TS-ISO-IEC-27001
BGYS

TS EN ISO/IEC 27001:2017
Bilgi Güvenliği yönetim sistemleri – Gereksinimler

Bu standard uygunluğun değerlendirilmesi için kullanılan şartları içerir.

Bu standardda aşağıda belirtilen fiil şekilleri kullanılmaktadır:

- "-meli/ -malı" bir şartı belirtir,
- "esastır" kuvvetli bir tavsiyeyi belirtir,
- "izin verilir" bir müsaadeyi belirtir,
- "-abilir/ -ebilir" bir olabilirliği veya yapabilirlik/ yapabilirliği belirtir.

- "Not" olarak gösterilen bilgi, dokümanın anlaşılması veya kullanımı amaçlıdır.

TÜRK STANDARDLARI ENSTİTÜSÜ

TS EN ISO/IEC 27001:2017 STANDARD MADDELERİ

Madde 1 : Kapsam
Madde 2 : Atıf Yapılan Standard ve/veya Dokümanlar
Madde 3 : Terimler ve Tarifler
Madde 4 : Kuruluşun Bağlamı
Madde 5 : Liderlik
Madde 6 : Planlama
Madde 7 : Destek
Madde 8 : İşletim
Madde 9 : Performans Değerlendirme
Madde 10 : İyileştirme

0.2. Bilgi Güvenliği Yönetim Sisteminin Amacı

BGYS standartlar ailesinin kullanımı yoluyla, kuruluşlar finansal bilgiler, fikri mülkiyet ve çalışan ayrıntıları veya müşteriler veya üçüncü şahıslar tarafından kendilerine emanet edilen bilgiler dahil olmak üzere bilgi varlıklarının güvenliğini yönetmek için bir çerçeve geliştirebilir ve uygulayabilir. Bu standartlar, bilgilerin korunmasına uygulanan BGYS'lerinin bağımsız bir değerlendirmesine hazırlanmak için de kullanılabilir

1.Kapsam

Bu standard kuruluşun bağlamı dâhilinde bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları kapsar.

Bu standard aynı zamanda kuruluşun ihtiyaçlarına göre düzenlenmiş bilgi güvenliği risklerinin değerlendirilmesi ve işlenmesi için şartları da içerir.

Bu standardda ortaya konulan şartlar geneldir ve türleri, büyüklükleri ve doğalarından bağımsız olarak tüm kuruluşlara uygulanabilir olması hedeflenmiştir.

Bir kuruluşun bu standarda uyumluluk iddiasında bulunması durumda, Madde 4 ila Madde 10 arasında belirtilen şartların herhangi birinin hariç tutulması kabul edilebilir değildir.

2. Atıf yapılan standard ve/veya dokümanlar

- Tarihli atıflar için sadece atıf yapılan sürüm geçerlidir. Tarihsiz atıflar için, atıf yapılan dokümanın (tüm değişiklikler dâhil olmak üzere) son sürümü geçerlidir.
- ISO/IEC 27000, Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Genel Bakış ve Terimler sözlüğü

" Bilgi teknolojisi - güvenlik teknikleri" ile ilgili yayınlanan ISO27K standartları şunlardır:

1. ISO/IEC 27000 — Bilgi teknolojisi - Bilgi güvenliği yönetim sistemleri — Genel bakış ve Sözlük
2. ISO/IEC 27001 — Bilgi teknolojisi - Güvenlik Teknikleri - Bilgi güvenliği yönetim sistemleri — Gereksinimler
3. ISO/IEC 27002 — Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği kontrolleri için uygulama prensipleri
4. ISO/IEC 27003 — Bilgi güvenliği yönetim sistemi uygulama kılavuzu
5. ISO/IEC 27004 — Bilgi güvenliği yönetimi — İzleme, ölçüm, analiz ve değerlendirme

6. ISO/IEC 27005 — Bilgi güvenliği risk yönetimi
7. ISO/IEC 27006 — Bilgi güvenliği yönetim sistemlerinin denetim ve belgelendirmesini sağlayan kuruluşlar için gereksinimler
8. IISO/IEC 27011 — Telekomünikasyon kuruluşları için ISO/IEC 27002 tabanlı bilgi güvenliği yönetimi yönergeleri
9. ISO/IEC 27017 — Bulut hizmetleri için ISO/IEC 27002 tabanlı bilgi güvenliği denetimleri için uygulama kuralları
10. ISO/IEC 27019 — Enerji sektöründe proses kontrolü için bilgi güvenliği
11. ISO/IEC 27031 — İş sürekliliği için bilgi ve iletişim teknolojisine hazırlık rehberi
12. ISO/IEC 27032 — Siber güvenlik kılavuzu
13. ISO/IEC 27033 — BT ağ güvenliği

14. ISO/IEC 27035-1 — Bilgi güvenliği olay yönetimi - Bölüm 1: Olay yönetimi ilkeleri
15. ISO/IEC 27040 — Depolama güvenliği
16. ISO/IEC 27701 — Bilgi teknolojisi - Güvenlik Teknikleri - Bilgi güvenliği yönetim sistemleri — Gizlilik Bilgi Yönetim Sistemi (PIMS).

3. TERİMLER VE TARİFLER

Veri
İşlenmemiş bilgi

Bilgi
Bilgi, verilerin işlenmiş hâlidir.

Kimlik doğrulama
Bir tüzel kişiliğin, iddia edilen karakteristiğinin doğru olduğuna dair güvencenin temini.

Etkililik
Planlanan faaliyetlerin gerçekleştirilme ve planlanan sonuçların elde edilme derecesi

Kayıt
Elde edilen sonuçları belirtilen veya gerçekleştiren faaliyetin delillerini sağlayan doküman.

Organizasyon

Hedeflerine ulaşmak için sorumlulukları, yetkileri ve ilişkileri olan kendi işlevleri olan kişi veya kişiler grubu

Politika

Yönetim tarafından resmi olarak genel niyetin ve yönün ifade edilmesi.

Prosedür

Bir prosesin veya bir faaliyetin yürütülmesi için belirlenmiş yol.
[ISO 9000:2005]

Proses

Girdileri çıktılara dönüştüren birbirleri ile ilgili olan veya etkileşimde bulunan faaliyetler dizisi.
[ISO 9000:2005]

Erişim denetimi

Varlıklara erişimin, iş ve güvenlik gereklerine göre yetkilendirilmesi ve sınırlandırılması anlamına gelir.

Varlık

Kuruluş için değeri olan herhangi bir şey.

Not - Aşağıdaki örnekler de dâhil olmak üzere varlıkların birçok çeşidi vardır:
a) Bilgi varlığı,
b) Yazılım, bir bilgisayar programı gibi,
c) Fiziksel, bilgisayar gibi,
d) Hizmetler,
e) Kişiler ve kişi nitelikleri, becerileri ve deneyimi,
f) Maddi olmayan varlıklar, itibar ve imaj gibi.

Bilgi varlığı

Kuruluş için değer ifade eden herhangi değerli bilgi veya veri.

Etki
İş hedeflerinin sağlanan seviyesindeki olumsuz bir değişiklik.

Olay
Özel bir durumlar kümesinin oluşması.
[ISO/IEC Guide 73:2002]

Etkinlik
Planlanmış faaliyetleri gerçekleştirme ve planlanmış sonuçlara ulaşma derecesi.

Verimlilik
Elde edilen sonuçlar ile kaynakların ne kadar iyi kullanıldığı arasındaki ilişki.

Saldırı
Varlığı yok etme, ortaya çıkarma, değiştirme, devre dışı bırakma, çalma veya varlığa yetkisiz erişim teşebbüsü.

Bilgi güvenliği

Bilginin **gizliliğinin, bütünlüğünün** ve **elverişliliğinin** korunması.

Not - Ek olarak; **doğruluk, hesap verilebilirlik, inkâr edememe ve güvenilirlik** gibi diğer özellikleri de kapsar.

Gizlilik

Bilginin yetkisiz kişiler, varlıklar veya prosesler için elverişli yapılmaması ya da açıklanmaması özelliği.

Bütünlük

Varlıkların doğruluğunu ve tamlığını koruma özelliği.

Elverişlilik

Yetkili bir tüzel kişilik tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.

Doğruluk

Bir tüzel kişiliğin, iddia ettiği şey olması özelliği.

Hesap verebilirlik
Kendi eylem ve kararları için bir tüzel kişiliğin sorumluluğu.

İnkâr edememe
Olayın veya faaliyetin olup olmadığının hakkındaki anlaşmazlıkları ve olay içerisindeki kaynakları çözmek amacıyla, iddia edilen olayın veya faaliyetin oluşumunun ve kaynağının ispat edilebilirliği.

Güvenilirlik
Davranış ve sonuçların tutarlılık özelliği.

Yönetim sistemi
Kuruluşun hedeflerini gerçekleştirmek üzere oluşturulan politikaların, prosedürlerin, kılavuzların ve ilgili kaynakların çerçevesi.

Kılavuz
Bir hedefe ulaşmak için neyin yapılması gerektiğini belirten tavsiye.

Bilgi güvenliği olayı

Olası bir bilgi güvenliği politikasının, kontrollerin başarısızlığı veya güvenlikle ilgili olabilecek önceden bilinmeyen bir durumu belirten sistem, hizmet ya da ağ durumunun tanımlanan bir halinin ortaya çıkışı.

Bilgi güvenliği ihlal olayı

İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

Bilgi güvenliği ihlal olayı yönetimi

Bilgi güvenliği ihlal olaylarının tespit edilmesi, raporlanması, değerlendirilmesi, tepki gösterilmesi veilgili işlemlerin prosesleri.

Bilgi güvenliği yönetim sistemi - BGYS

Bilgi güvenliğini kurmayı, gerçekleştirmeyi, işletmeyi, izlemeyi, gözden geçirmeyi, sürdürmeyi ve iyileştirmeyi temel alan iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası

Üst yönetim

Bir kuruluşu_ en üst düzeyde yöneten ve kontrol eden kişi veya grup .

Dış bağlam

Kuruluşun hedeflerine ulaşmak istediği dış ortam

- İster uluslararası, ulusal, bölgesel veya yerel olsun, kültürel, sosyal, politik, yasal, düzenleyici, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam;
- Anahtar sürücüleri ve trendler üzerine etkisi olan *hedeflerin* arasında organizasyonu ;
- Dış paydaşlarla ilişkiler, onların algıları ve değerleri

[KAYNAK: ISO Kılavuzu 31000]

İç bağlam

Organizasyonun hedeflerine ulaşmak istediği iç ortam

- Yönetişim, organizasyon yapısı, roller ve hesap verme sorumlulukları;
- Politikalar, hedefler ve bunları başarmak için mevcut olan stratejiler;
- Kaynaklar ve bilgi (ör. Sermaye, zaman, insanlar, süreçler, sistemler ve teknolojiler) açısından anlaşılan yetenekler ;
- Bilgi sistemleri, bilgi akışları ve karar verme *süreçleri* (hem resmi hem de gayri resmi);
- İç paydaşlarla ilişkiler, onların algıları ve değerleri ;
- Kuruluşun kültürü;
- Kuruluş tarafından benimsenen standartlar, yönergeler ve modeller;
- Sözleşme ilişkilerinin şekli ve kapsamı.

[KAYNAK: ISO Kılavuzu 31000]

Bilgi sistemi

Uygulamalar, hizmetler, bilgi teknolojisi varlıkları veya diğer bilgi işleme bileşenleri kümesi

Paydaş (kabul edilen dönem)
Bir karar veya faaliyetten etkilenebilecek, etkilenebilecek veya etkilenebileceğini algılayabilecek kişi veya kuruluş

Gözden geçirmek
Belirlenen hedeflere_ ulaşmak için konunun uygunluğunu, yeterliliğini ve etkinliğini belirlemek için yapılan faaliyet
[KAYNAK: ISO Kılavuzu 73: 2009

Risklerin, **politikalar, prosedürler**, **kılavuzlar** ile uygulanması veya kuruluş yapısında yönetilmesi. Yönetim; teknik, idari veya yasal mana da olabilir.

Güvenlik açığı

bir varlık veya kontrolün bir veya daha fazla tehdit tarafından istismar edilebilecek zayıflığı .

Tehdit

Bir sisteme veya kuruluşa zarar verebilecek istenmeyen bir olayın olası nedeni

Risk

Belirsizliğin hedefler üzerindeki etkisi

Not 1: Giriş: Etki, beklenen olumlu veya olumsuzdan sapmadır.
Not 2: Belirsizlik, bir olayın anlaşılması veya bilinmesi, bunun sonucu veya olasılığı ile ilgili bilgi eksikliğinin kısmen de olsa durumudur.

Risk kabulü

Belirli bir riski almaya yönelik bilgilendirilmiş karar.

Not 1: Risk kabulü, risk tedavisi olmaksızın veya risk işleme süreci sırasında gerçekleşebilir
Not 2 - Kabul edilen riskler izlemeye ve incelemeye_tabidir .
[KAYNAK: ISO Kılavuzu 73: 2009, 3.7.1.6]

Risk analizi

Riskin niteliğini anlamak ve risk seviyesini belirlemek için süreç .

Not 1 - Risk analizi, risk değerlendirmesi ve risk işleme hakkındaki kararlar için temel sağlar .
Not 2 - Risk analizi, risk tahminini içerir.

Risk değerlendirmesi

Genel proses arasında risk tanımlama , risk analizi ve risk_değerlemesini içerir.

Risk iletişimi ve danışma

Bir kuruluşun bilgi sağlamak, paylaşmak veya elde etmek ve paydaşlarla diyaloğa girmek için risk yönetimi için yürüttüğü sürekli ve yinelemeli süreçler dizisi

Risk kriterleri

Riskin öneminin değerlendirildiği görev tanımları

Not 1 - Risk kriterleri kurumsal hedeflere ve dış bağlama ve iç bağlama dayanmaktadır.
Not 2 - Risk kriterleri standartlardan, kanunlardan, politikalardan ve diğer gerekliliklerden türetilebilir.
[KAYNAK: ISO Kılavuzu 73: 2009, 3.3.1.3]

Risk değerlemesi

Riskin ve / veya büyüklüğünün kabul edilebilir veya tolere edilebilir olup olmadığını belirlemek için risk analizi sonuçlarını risk kriterleri ile karşılaştırma süreci

Risk tanımlama

Risk bulma, tanıma ve tanımlama süreci.

Not 1 - Risk tanımlama, risk kaynaklarının, olayların , nedenlerinin ve potansiyel sonuçlarının tanımlanmasını içerir.

Not 2 - Risk tanımlama, tarihsel verileri, teorik analizi, bilgili ve uzman görüşlerini ve paydaşların ihtiyaçlarını içerebilir,

[KAYNAK: ISO Kılavuzu 73: 2009, 3.5.1]

Risk yönetimi

Risk_ ile ilgili olarak bir kuruluşu yönlendirmek ve kontrol etmek için koordineli faaliyetler.

Risk yönetimi süreci

Yönetim politikalarının, prosedürlerin ve uygulamaların iletişim, danışmanlık, bağlam oluşturma ve riski belirleme, analiz etme, değerlendirme, tedavi etme, izleme ve gözden geçirme faaliyetlerine sistematik uygulaması

Risk tedavisi

Riski değiştirmek için süreç

Not 1 - Risk tedavisi şunları içerebilir:
- riski doğuran faaliyete başlamama veya devam etmeme kararı alarak riskten kaçınmak;
- bir fırsatı değerlendirmek için risk almak veya artırmak;
- risk kaynağının kaldırılması;
- olasılığın değiştirilmesi ;
- sonuçların değiştirilmesi;
- riski başka bir taraf veya taraflarla paylaşmak (sözleşmeler ve risk finansmanı dahil);
- Bilgilendirilmiş seçimle riskin korunması.

Not 2 - Olumsuz sonuçlarla ilgilenen risk tedavileri bazen "risk azaltma", "risk giderme", "risk önleme" ve "risk azaltma" olarak adlandırılır.

Not 3 - Risk tedavisi yeni riskler yaratabilir veya mevcut riskleri değiştirebilir.

[KAYNAK: ISO Kılavuzu 73: 2009, 3.8.1, değiştirildi - "karar", giriş için Not 1'de "seçim" ile değiştirildi.]

Risk sahibi

Bir riski yönetme sorumluluğu ve yetkisine sahip kişi veya kuruluş .

Uygulanabilirlik bildirgesi

Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrolleri ve kontrol hedeflerini açıklayan dokümante edilmiş bildirge.

4. KURULUŞUN BAĞLAMI

4.1 Kuruluşun ve bağlamının anlaşılması

Kuruluş, amaçları ile ilgili olan ve bilgi güvenliği yönetim sisteminin hedeflenen çıktılarını başarma kabiliyetini etkileyebilecek iç ve dış hususları belirlemelidir.

İç Hususlar

İç hususlar kuruluşun hedeflerini gerçekleştirmek için aradığı iç ortamdır.
İç hususlar aşağıdakileri içerir, ancak bunlarla sınırlı değildir:

- ✓ İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler,
- ✓ Yerine getirilecek politikalar, hedefler ve stratejiler,
- ✓ Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),
- ✓ İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri,
- ✓ Kuruluşun kültürü,
- ✓ Bilgi sistemleri, bilgi akışı ve karar alma süreçleri (resmi ve gayrıresmi),
- ✓ Kuruluş tarafından uyarlanan standardlar, kılavuzlar ve modeller ve
- ✓ Sözleşmeye ilişkin ilişkilerin biçim ve genişliği.

Dış Hususlar

Dış hususlar kuruluşun hedeflerini gerçekleştirmede aradığı dış ortamdır.
Dış hususlar aşağıdakileri içerebilir, ancak bunlarla sınırlı değildir:

a) Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam,
b) Kuruluşun hedefleri üzerinde etkisi bulunan kilit sürücüler ve eğilimler ve
c) Dış paydaşlarla ilişkiler ve onların algılamaları ve değerleri.

TÜRK STANDARDLARI ENSTİTÜSÜ

ÖRNEK

Kuruluşun Bağlamı			
İç Bağlam		**Zayıf**	**Güçlü**
a)	Organizasyonun kültürü;		- Yönetim sistemi eğitimleri alınmış -yöetim sistemi kurulu ve çalışıyor - Bilgi güvenliği konusunda farkındalık eğitimleri alınmış
b)	Politikalar, hedefler ve bunlara ulaşmak için yürürlükte olan stratejiler;	- Yeni satın alınmış şirket çalışanları	
c)	Yönetişim, örgüt yapısı, rolleri ve hesap verebilirlikleri	- sorumluluklar net tanımlanmamış	
d)	Kuruluş tarafından benimsenen standartlar, kılavuzlar ve modeller;	----------	----------
e)	Kaynaklar ve bilgi açısından (örn., Sermaye, zaman, kişi, süreçler, sistemler ve teknolojiler) anlaşılan kapasiteler;	-Teknoloji eski, süreçler tam olarak tanımlı değil, - yeni teknoloji için insan kaynağı	- Finansal yön
f)	Fiziki altyapı ve çevre;	- Ağ cihazları, UPS, Omurga , Arşiv	----------
g)	Bilgi sistemleri, bilgi akışları ve karar verme süreçleri (hem resmi hem de gayri resmi); ve		
h)	Önceki denetimler veya önceki risk değerlendirmesi.		

Dış Bağlam		**Zayıf**	**Güçlü**
a)	Sosyal ve kültürel çevre	----------	- kuruluşun bulunduğu yer
b)	Siyasi, yasal, muvzuat		- Yasal şartlaara tam uyum, - ülkede istikrarlı bir siyası durum
c)	Finansal		- Kuruluş kredibiltesi yüksek
d)	Teknolojik	- Dışarıdaki gelişmiş teknoljiye karşı yetersiz sitem	
e)	Ekonomik		
f)	Doğadan kaynaklanan		- Yngın söndürme sitemi, - Depreme dayanıklı güvenli alanlar mevcut, -sel, su baskını vb için gerekli korumalar
g)	Rekabetçi ortam		

4.2 İlgili tarafların ihtiyaç ve beklentilerinin anlaşılması

Kuruluş aşağıdakileri belirleyecektir:

a) Bilgi güvenliği yönetim sistemi ile ilgili taraflar ve
b) Bu ilgili tarafların bilgi güvenliği ile ilgili gereksinimleri.

Not - İlgili tarafların gereksinimleri yasal ve düzenleyici gereksinimleri ve sözleşmeden doğan yükümlülükleri içeriyor olabilir.

ÖRNEK

İlgili tarafların ihtiyaç ve beklentileri	
İç ilgi taraflar	**İhtiyaç ve Beklentiler**
Üst yönetim dahil karar alıcılar	
Süreç sahipleri, sistem sahipleri ve bilgi sahipleri;	
IT	
Çalışanlar ve kullanıcılar	
Bilgi güvenliği uzmanları.	

Dış ilgi taraflar	
Sahipler ve yatırımcılar da dahil olmak üzere hissedarlar	
Düzenleyiciler ve yasa koyucular	
Sanayi kuruluşları	
Rakipler;	
Müşteriler ve tüketiciler; ve	
Eylemci gruplar	

4.3 Bilgi güvenliği yönetim sisteminin kapsamının belirlenmesi

Kuruluş, kapsamını oluşturabilmek için, bilgi güvenliği yönetim sisteminin sınırlarını ve uygulanabilirliğini belirlemelidir.

Kuruluş, bu kapsamı belirlerken aşağıdakileri dikkate almalıdır:

a) Madde 4.1. de belirtilen dış ve iç hususlar,
b) Madde 4.2. de belirtilen şartlar ve
c) Kuruluş tarafından gerçekleştirilen faaliyetler arasındaki arayüzler, bağımlılıklar ve diğer kuruluşlar tarafından gerçekleştirilen faaliyetler.

Kapsam ***yazılı bilgi*** olarak mevcut olmalıdır.

Örnek BGYS Kapsamı

4.4 Bilgi güvenliği yönetim sistemi

Kuruluş, bu standardın şartları çerçevesinde bir bilgi güvenliği yönetim sistemini kurmalı, uygulamalı, sürdürmeli ve sürekli iyileştirmelidir.

5. LİDERLİK

5.1 Liderlik ve bağlılık

Üst yönetim bilgi güvenliği yönetim sistemi ile ilgili olarak aşağıdakileri yerine getirerek, liderlik ve bağlılık göstermelidir:

a) Bilgi güvenliği politikası ve bilgi güvenliği amaçlarının oluşturulmasını ve kuruluşun stratejik yönü ile uyumlu olmasının temin edilmesi,
b) Bilgi güvenliği yönetim sisteminin şartlarının kuruluşun süreçleri ile bütünleştirilmesinin temin edilmesi,
c) Bilgi güvenliği yönetim sistemi için gerekli olan kaynakların erişilebilirliğinin temin edilmesi,
d) Etkin bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sisteminin şartlarına uyum sağlamanın öneminin duyurulması,
e) Bilgi güvenliği yönetim sisteminin hedeflenen çıktılarının başarılmasının temin edilmesi,
f) Bilgi güvenliği yönetim sisteminin etkinliğine katkı sağlamaları için kişilerin yönlendirilmesi ve desteklenmesi,
g) Sürekli iyileştirmenin desteklenmesi ve
h) Kendi sorumluluk alanlarında liderliklerini sergileyebilmeleri için diğer ilgili yönetim rollerinin desteklenmesi.

5.2 Politika

Üst yönetim aşağıdakileri karşılayan bir bilgi güvenliği politikası oluşturmalıdır:

a) Kuruluşun amacına uygun,
b) Bilgi güvenliği amaçlarını içeren (Bk. Madde 6.2) veya bilgi güvenliği amaçlarını belirlemek için bir çerçeve sağlayan,
c) Bilgi güvenliği ile ilgili uygulanabilir şartların karşılanmasına dair bir taahhüt içeren ve
d) Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için bir taahhüt içeren bilgi güvenliği politikası,

Bilgi güvenliği politikası:

e) ***Yazılı bilgi*** olarak mevcut olmalı,
f) Kuruluş içinde duyurulmalı ve
g) Uygun olan ilgili taraflarca erişilebilir olmalıdır.

ÖRNEK

BİLGİ GÜVENLİĞİ POLİTİKASI

5.3 Kurumsal roller, sorumluluklar ve yetkiler

Üst yönetim, bilgi güvenliği ile ilgili olan roller için sorumluluk ve yetkilerin atanmasını ve duyurulmasını temin etmelidir.
Üst yönetim aşağıdakiler için sorumluluk ve yetki ataması yapmalıdır:

a) Bilgi güvenliği yönetim sisteminin bu standardın şartlarına uyum sağlamasını temin etmek ve
b) Üst yönetime bilgi güvenliği yönetim sisteminin performansı hakkında raporlama.

Not - Üst yönetim, kuruluş içinde bilgi güvenliği yönetim sisteminin performansının raporlanması için sorumluluklar ve yetkiler atayabilir.

TÜRK STANDARDLARI ENSTİTÜSÜ

ÖRNEK

6. PLANLAMA

6.1 Risk ve fırsatları ele alan faaliyetler

6.1.1. Genel

Bilgi güvenliği yönetim sistemi planlaması yaparken, kuruluş Madde 4.1 de atıf yapılan hususları ve Madde 4.3. de atıf yapılan şartları göz önünde bulundurmalı ve aşağıdakilerin gerçekleştirilmesi için gerekli olan riskleri ve fırsatları belirlemelidir:

a) Bilgi güvenliği yönetim sisteminin amaçlanan çıktıları sağlayabilmesinin temin edilmesi,
b) İstenmeyen etkilerin önlenmesi veya azaltılması ve
c) Sürekli iyileştirmenin başarılması,

Kuruluş aşağıdakileri planlamalıdır:

d) Bu risk ve fırsatların ele alınması için faaliyetler ve
e) Aşağıdakilerin nasıl gerçekleştirileceği,
    1) Faaliyetleri, bilgi güvenliği yönetim sistemi süreçleri ile bütünleştirme ve uygulama,
    2) Faaliyetlerin etkinliğinin değerlendirilmesi.

6.1.2. Bilgi güvenliği risk değerlendirmesi

Kuruluş aşağıda belirtilen şartları yerine getiren bir bilgi güvenliği risk değerlendirmesi sürecini tanımlamalı ve uygulamalıdır:

a) Aşağıdakileri içeren bilgi güvenliği risk kriterlerinin oluşturulması ve sürdürülmesi:
   1) Risk kabul kriterleri ve
   2) Bilgi güvenliği risk değerlendirmesi yapılması için kriterler,
b) Tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesinin temin edilmesi,
c) Bilgi güvenliği risklerinin tespit edilmesi:
   1) Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki bilginin gizlilik, bütünlük ve erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi için bilgi güvenliği risk değerlendirme prosesinin uygulanması ve
   2) Risk sahiplerinin belirlenmesi,

d) Bilgi güvenliği risklerinin analiz edilmesi:
   1) Madde 6.1.2 c) 1) de belirlenen riskler gerçekleştiği takdirde muhtemel sonuçların değerlendirilmesi,
   2) Madde 6.1.2 c) 1) de belirlenen risklerin gerçekleşmesi ihtimalinin gerçekçi bir şekilde değerlendirilmesi ve
   3) Risk seviyelerinin belirlenmesi,

e) Bilgi güvenliği risklerinin değerlendirilmesi:
   1) Risk analizi sonuçlarının Madde 6.1.2 a) da oluşturulan risk kriterleri ile karşılaştırılması ve
   2) Analiz edilen risklerin risk işleme için önceliklendirilmesi.

Kuruluş bilgi güvenliği risk değerlendirme süreci ile ilgili olarak ***yazılı bilgileri*** muhafaza etmelidir.

ÖRNEK

Kuruluşu etkileyen ve dikkate alınması gereken risk ve fırsatlara örnekler:

TÜRK STANDARDLARI ENSTİTÜSÜ

PRATİK ÇALIŞMA-2

BG RİSK VE FIRSATLAR

EK Doküman

6.1.3. Bilgi güvenliği risk işleme

Kuruluş aşağıdakileri gerçekleştirmek için bir bilgi güvenliği risk işleme süreci tanımlamalı ve uygulamalıdır:

a) Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk işleme seçeneklerinin seçilmesi,
b) Seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanmasında gerekli olan tüm kontrollerin belirlenmesi,
c) Yukarıdaki Madde 6.1.3b) de belirlenen kontroller ile Ek A daki kontrollerin karşılaştırılması ve gerekli hiçbir kontrolün gözden kaçırılmadığının doğrulanması,
d) Gerekli kontrolleri (Bk. Madde 6.1.3b) ve c)), bunların dahil edilmesinin gerekçelendirmesi, uygulanıp uygulanmadıklarını ve Ek A dan kontrollerin dışarıda bırakılmasının gerekçelendirmesini içeren bir **Uygulanabilirlik Bildirgesi üretilmesi**,

e) Bir bilgi güvenliği risk işleme planının formüle edilmesi ve
f) Bilgi güvenliği risk işleme planına dair risk sahiplerinin onayının alınması ve artık bilgi güvenliği risklerinin kabulü

Kuruluş, bilgi güvenliği risk işleme süreci ile ilgili ***yazılı bilgileri*** muhafaza etmelidir.

TÜRK STANDARDLARI ENSTİTÜSÜ

ÖRNEK

logo	*UYGULANABİLİRLİK BİLDİRGESİ*	**Dokuman Kodu:** **Yayın Tarihi :** **Rev. No:** **Rev. Tarihi:** **Sayfa x/y**

Kontrol Madde no:	Kontrol Maddesi	Kontrol	Uygulanıyor / Uygulanmıyor		Referans Dokuman(lar)
			Evet	Hayır	
A.5 Bilgi güvenliği politikaları					
A.5.1 Bilgi güvenliği için yönetimin yönlendirmesi					
Amaç: Bilgi güvenliği için, iş gereksinimleri ve ilgili yasalar ve düzenlemelere göre yönetimin yönlendirmesi ve desteğini sağlamak.					
A.5.1.1	**Bilgi güvenliği için politikalar**	Bir dizi bilgi güvenliği politikaları, yönetim tarafından tanımlanmalı, onaylanmalı ve yayınlanarak çalışanlara ve ilgili dış taraflara bildirilmelidir.	**Evet**		
A.5.1.2	**Bilgi güvenliği için politikaların gözden geçirilmesi**	Bilgi güvenliği politikaları, belirli aralıklarla veya önemli değişiklikler ortaya çıktığında sürekli uygunluk ve etkinliği sağlamak amacıyla gözden geçirilmelidir.	**Evet**		
A.6 Bilgi güvenliği organizasyonu					
A.6.1 İç organizasyon					
Amaç: Kuruluş içerisinde bilgi güvenliği operasyonu ve uygulamasının başlatılması ve kontrol edilmesi amacıyla bir yönetim çerçevesi kurmak.					
A.6.1.1					
A.6.1.2					

A.14.2.7	**Dışarıdan sağlanan geliştirme**	Kuruluş dışarıdan sağlanan sistem geliştirme faaliyetini denetlemeli ve izlemelidir.		**Hayır**	

A.18.2 Bilgi güvenliği gözden geçirmeleri					
Amaç: Bilgi güvenliğinin kurumsal politika ve prosedürler uyarınca gerçekleştirilmesini ve yürütülmesini sağlamak.					
A.18.2.1					

K.2					
K.2.1					
K.2.1.1					

Hazırlayan	Kontrol Eden	Onaylayan

TÜRK STANDARDLARI ENSTİTÜSÜ

ÖRNEK

logo	*Risk Yönetim Tablosu*	Dokuman Kodu: Yayın Tarihi : Rev. No: Rev. Tarihi: Sayfa X(Y

Risk Değerlendirme

Risk Tanımlama				Risk Analizi				Risk Değerleme	Riskin Sahibi
R.Kaynağı	olay	sebep	sonuç	Mevcut kontrol(ler)	Olasılık(O)	Etki€	Risk(R=O.E)		
elektrik besleme	Disk arızası	Elektrik dalgalanması	veri kaybı						
Personel	yanlış kişiye gizli bilgi göndermek	dikkat eksikliği	gizli bilgiye erişim						
ortam ısısı	cihazın hatalı okunması	çevresel koşullardaki değişiklik	veri bütünlüğünün bozzulması						

TÜRK STANDARDLARI ENSTİTÜSÜ

Risk İşleme									
Risk İşleme Seçenekleri	Uygulanacak kontrol(ler)	Yapılacak Faaliyet		Gerekli Kaynaklar	sorumlusu	Bitiş tarihi	Tahmini		
							Olasılık(O)	Etki€	Risk(R=O.E)

Hazırlayan	Kontrol Eden	Onaylayan

6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama

Kuruluş, uygun işlevler ve seviyelerde bilgi güvenliği amaçlarını tesis etmelidir.

Bilgi güvenliği amaçları aşağıdakileri sağlamalıdır:

a) Bilgi güvenliği politikası ile tutarlı olmalı,
b) Ölçülebilir olmalı (uygulanabilirse),
c) Uygulanabilir bilgi güvenliği şartlarını ve risk değerlendirme ve risk işlemenin sonuçlarını dikkate almalı,
d) Duyurulmalı ve
e) Uygun şekilde güncellenmelidir.

Kuruluş bilgi güvenliği amaçları ile ilgili ***yazılı bilgileri*** muhafaza etmelidir.

Kuruluş bilgi güvenliği amaçlarını nasıl başaracağını planlarken, aşağıdakileri belirlemelidir:

f) Ne yapılacağı,
g) Hangi kaynakların gerekli olacağı,
h) Kimin sorumlu olacağı,
i) Ne zaman tamamlanacağı ve
j) Sonuçların nasıl değerlendirileceği.

TÜRK STANDARDLARI ENSTİTÜSÜ

ÖRNEK

logo	Hedefler	Dokuman Kodu: Yayın Tarihi : Rev. No: Rev. Tarihi: Sayfa X{Y

Sıra no:	*Hedefler*	Gerçekleştirmek için yapılacak faaliyet	Gerekli kaynaklar	Sorumlusu	Bitiş tarihi	Sonuçların değerlendirilmesi
1	BG alanındaki farkındalığı %75 den % 90 çıkarmak	ilgili personele farkındalık eğitimleri verilecektir	Finans, Eğitim için gerekli yetişmiş eğitmen, eğitimin verileceği yer, eğitim dökümanı vb.	Eğitim birimi	x.y.z	eğitim öncesi ve sonrası sınav yapılacak
2	İşletim sistemleri, veri tabanı uygulamaları ve ağ cihazlarının güncelleme oranları %85 den % 95 e çıkarmak	güncelleme sorumlusu atanacak ve belli peryotlarla durum izlenecektir.	Bu iş için atanmış Personel	Sistem yöneticisi, Ağ yöneticisi, veri tabanı yöneticisi	x.y.z	
3						
4						
5						
17						
18						

Hazırlayan	Kontrol Eden	Onaylayan

7. DESTEK

7.1 Kaynaklar

Kuruluş bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan kaynakları belirlemeli ve sağlamalıdır.

KAYNAKLAR İÇİN ÖRNEKLER

- ✓İnsan
- ✓Ekipman
- ✓Makine ve teçhizat
- ✓Bina ve tesis
- ✓Teknoloji
- ✓Çalışma ortamı
- ✓Finans
- ✓Zaman
- ✓Yazılım
- ✓Donanım
- ✓Bilgi, v.b.

7.2 Yeterlilik

Kuruluş aşağıdakileri yapmalıdır:

a) Bilgi güvenliği performansını etkileyen kendi kontrolü altında çalışan kişilerin gerekli yeterliliklerinin belirlenmesi,
b) Uygun öğretim, eğitim veya tecrübe temelinde bu kişilerin yeterliliklerinin temin edilmesi,
c) Uygun olduğu durumlarda, gerekli yeterliliğin sağlanması için girişimde bulunulması ve bu girişimlerin etkinliğinin değerlendirilmesi ve
d) Yeterliliğin delili olarak uygun ***yazılı bilgilerin*** muhafaza edilmesi.

7.3 Farkındalık

Kuruluşun kontrolü dâhilinde görev yapan kişiler aşağıdakilerin farkında olmalıdır:

a) Bilgi güvenliği politikası,
b) İyileştirilmiş bilgi güvenliği performansının faydaları da dâhil bilgi güvenliği yönetim sisteminin etkinliğine yaptıkları katkı ve
c) Bilgi güvenliği yönetim sistemi şartlarına uyum sağlamama'nın sonuçları.

FARKINDALIK ARTIRMA YÖNTEMLERİ

- ✓ İç iletişim,
- ✓ Görsel işaretler ve afişler,
- ✓ Kampanyalar,
- ✓ Eğitim/öğretim
- ✓ Danışmanlık
- ✓ Seminerler

7.4 İLETİŞİM

7.4 İletişim

Kuruluş aşağıdakileri içeren bilgi güvenliği yönetim sistemi ile ilgili dâhili ve harici iletişim ihtiyaçlarını belirlemelidir:

a) İletişimin konusu,
b) Ne zaman iletişim kurulacağı,
c) Kiminle iletişim kurulacağı,
d) Kimin iletişim kuracağı ve
e) İletişimin hangi süreçten etkileneceği.

TÜRK STANDARDLARI ENSTİTÜSÜ

7.5 YAZILI BİLGİLER

7.5.1 Genel

Kuruluşun bilgi güvenliği yönetim sistemi aşağıdakileri içermelidir:

a) Bu standardın gerektirdiği yazılı bilgiler ve
b) Kuruluş tarafından bilgi güvenliği yönetim sisteminin etkinliği için gerekli olduğu belirlenen yazılı bilgiler.

Bir bilgi güvenliği yönetim sistemi için yazılı bilgilerin boyutu aşağıdakiler temelinde bir kuruluştan diğer kuruluşa değişebilir:

1) Kuruluşun büyüklüğü ve faaliyetlerinin, süreçlerinin, ürünlerinin ve hizmetlerinin türleri,
2) Süreçlerin ve etkileşimlerinin karmaşıklığı ve
3) Kişilerin yeterliliği.

7.5.2 Oluşturma ve güncelleme

Kuruluş, yazılı bilgileri oluştururken ve güncellerken, aşağıdakileri uygun bir şekilde temin etmelidir:

a) Tanımlama ve tarif etme (örneğin, bir başlık, tarih, yazar veya referans numarası),
b) Biçim (örneğin; dil, yazılım sürümü, grafikler) ve ortam (örneğin, kâğıt, elektronik) ve
c) Uygunluğun ve doğruluğun gözden geçirilmesi ve onaylanması.

7.5.3 Yazılı bilgilerin kontrolü

Bilgi güvenliği yönetim sistemi ve bu standardın gerektirdiği yazılı bilgiler aşağıdakileri temin etmek için kontrol edilmelidir:

a) Gereken yerde ve zamanda kullanım için erişilebilir ve uygun olması ve
b) Doğru bir şekilde korunması (örneğin, gizlilik kaybından, uygun olmayan kullanımdan veya bütünlük kaybından).

Yazılı bilgilerin kontrolü için, kuruluş uygunluğuna göre aşağıdaki faaliyetleri ele almalıdır:

c) Dağıtım, erişim, getirme ve kullanım,
d) Okunaklılığın korunması da dâhil olmak üzere saklama ve koruma,
e) Değişikliklerin kontrolü (örneğin sürüm kontrolü) ve
f) Muhafaza etme ve yok etme.

Kuruluş tarafından bilgi güvenliği yönetim sisteminin planlaması ve işletimi için gerekli olduğu belirlenen ***dış kaynaklı yazılı bilgiler***, uygun şekilde tespit edilmeli ve kontrol edilmelidir.

8. İŞLETİM

8.1 İşletimsel planlama ve kontrol

Kuruluş bilgi güvenliği şartlarını karşılamak ve Madde 6.1'de belirlenen faaliyetleri gerçekleştirmek için gerekli olan süreçleri planlamalı, uygulamalı ve kontrol etmelidir. Kuruluş, Madde 6.2'de belirlenen bilgi güvenliği amaçlarını başarmak için aynı zamanda planları uygulamalıdır.

Kuruluş, süreçlerin planlandığı gibi yürütüldüğünden emin olduğu noktaya kadar ***yazılı bilgileri*** saklamalıdır.

Kuruluş, planlanan değişiklikleri kontrol etmeli ve istenmeyen değişikliklerin sonuçlarını gözden geçirerek, gerekiyor ise kötü etkileri azaltmak için eyleme geçmelidir.

Kuruluş, dış kaynaklı süreçlerin belirlenmesini ve kontrol edilmesini temin etmelidir.

8.2 Bilgi güvenliği risk değerlendirme

Kuruluş, Madde 6.1.2 a) da belirtilen kriterleri de dikkate alarak, bilgi güvenliği risk değerlendirmelerini planlanan aralıklarda veya önemli değişiklikler önerildiğinde veya meydana geldiğinde gerçekleştirmelidir.

Kuruluş, bilgi güvenliği risk değerlendirmesinin sonuçlarına dair ***yazılı bilgileri*** muhafaza etmelidir.

8.3 Bilgi güvenliği risk işleme

Kuruluş, bilgi güvenliği risk işleme planını uygulamalıdır.

Kuruluş, bilgi güvenliği risk işlemesinin sonuçlarına ait ***yazılı bilgileri*** muhafaza etmelidir.

9. PERFORMANS DEĞERLENDİRME

9.1 İzleme, ölçme, analiz ve değerlendirme

Kuruluş, bilgi güvenliği performansı ve bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmelidir.

Kuruluş aşağıdakileri belirlemelidir:

a) Bilgi güvenliği süreçleri ve kontrolleri dâhil olmak üzere neyin izlenmesi ve ölçülmesinin gerekli olduğu,
b) Geçerli sonuçları temin etmek için, uygun İzleme, ölçme, analiz ve değerlendirme yöntemleri,

Not - Seçilen yöntemlerin geçerli kabul edilebilmesi için karşılaştırılabilir ve tekrar üretilebilir sonuçlar üretmesi gerekmektedir.

c) İzleme ve ölçmenin ne zaman yapılacağı,
d) İzlemeyi ve ölçmeyi kimin yapacağı,
e) İzleme ve ölçme sonuçlarının ne zaman analiz edileceği ve değerlendirileceği ve
f) Bu sonuçları kimin analiz edeceği ve değerlendireceği.

Kuruluş, izleme ve ölçme sonuçlarına dair delil olarak uygun ***yazılı bilgileri*** muhafaza etmelidir.

ÖRNEK

İzleme Ve Ölçüm Örnekleri

- ✓ Tahsis edilen kaynaklar / bütçelenmiş bir süre içinde kullanılan kaynaklar
- ✓ Gözden geçirilen yüksek ve orta dereceli riskler / Toplam yüksek ve orta dereceli riskler
- ✓ Yıl içinde gözden geçirilen bilgi güvenliği politikalarının sayısı / Toplam Bilgi Güvenliği politikalarının sayısı * 100
- ✓ [BGYS eğitimi alan çalışan sayısı / BGYS eğitimi alması gereken çalışan sayısı] * 100
- ✓ Phishing testinde bağlantıya tıklamayan personel sayısı / Testte katılan personelin sayısı*100
- ✓ Bu yıl içinde bilgi sistemlerinin bulunduğu tesislere yetkisiz giriş sayısı / Bir önceki yıl bilgi sistemlerinin bulunduğu tesislere yetkisiz giriş sayısı

ÖRNEK

İzleme Ve Ölçüm Örnekleri

- ✓ Zamanında Yapılan Bakımlar / Planlanan Toplam Bakımlar*100
- ✓Kötü amaçlı yazılımların neden olduğu güvenlik olaylarının sayısı / Kötü amaçlı yazılımların neden olduğu tespit edilen ve engellenen saldırıların sayısı.
- ✓Anti virüs yazılımı güncel olmayan (Mesela bir haftadan eski güncellik) sunucu/iş istasyonu/bilgisayar sayısı / Toplam sunucu/iş istasyonu/bilgisayar sayısı
- ✓Kritik olarak nitelendirilen ve sızma testi ya da açıklık testi yapılan bilgi sistemleri / Kritik olarak nitelendirilen bilgi sistemleri

9.2 İç tetkik

Kuruluş, bilgi güvenliği yönetim sisteminin, aşağıdaki hususları yerine getirip getirmediği konusunda bilgi elde etmek için planlanan aralıklarda iç tetkikler gerçekleştirmelidir:

a) Aşağıdakilerle uyumlu olup olmadığı,

   1) Bilgi güvenliği yönetim sistemi ile ilgili olarak kuruluşun kendi şartları ve
   2) Bu standardın şartları,

b) Etkin bir şekilde uygulanması ve sürdürülmesi.

Kuruluş aşağıdakileri gerçekleştirmelidir:

c) Sıklık, yöntemler, sorumluluklar, gereksinimleri planlama ve raporlama da dâhil olmak üzere bir tetkik programının/programlarının planlanması, oluşturulması, uygulanması ve sürdürülmesi. Tetkik programı/programları ilgili süreçlerin önemini ve önceki tetkiklerin sonuçlarını dikkate almalıdır,
d) Her bir tetkik için tetkik kriterlerinin ve kapsamın tanımlanması,
e) Tetkik sürecinin tarafsızlığı ve objektifliğini temin edecek şekilde tetkikçilerin seçimi ve tetkiklerin yürütülmesi,
f) Tetkik sonuçlarının uygun yönetim kademesine raporlanmasının temin edilmesi ve
g) Tetkik programı/programları ve tetkik sonuçlarının delil teşkil eden ***yazılı bilgilerinin*** muhafaza edilmesi.

9.3 Yönetimin gözden geçirmesi

Üst yönetim bilgi güvenliği yönetim sisteminin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için planlı aralıklarla gözden geçirmelidir.

Yönetimin gözden geçirmesi aşağıdakileri ele almalıdır:

a) Önceki yönetimin gözden geçirmelerinden gelen görevlerin durumu,
b) Bilgi güvenliği yönetim sistemini ilgilendiren dış ve iç konulardaki değişiklikler,
c) Aşağıdakiler deki gelişmeler dâhil bilgi güvenliği performansına dair geri bildirim:
    1) Uygunsuzluklar ve düzeltici faaliyetler,
    2) İzleme ve ölçme sonuçları,
    3) Tetkik sonuçları ve
    4) Bilgi güvenliği amaçlarının yerine getirilmesi,

d) İlgili taraflardan geri bildirimler,
e) Risk değerlendirme sonuçları ve risk işleme planının durumu ve
f) Sürekli iyileştirme için fırsatlar.

Yönetimin gözden geçirmesi çıktıları, sürekli iyileştirme fırsatlarına ve bilgi güvenliği yönetim sisteminde gerekli olan değişiklikler için tüm ihtiyaçlara dair kararları içermelidir.

Kuruluş, yönetimin gözden geçirmesinin sonuçlarının delili olarak ***yazılı bilgileri*** muhafaza etmelidir.

10. İYİLEŞTİRME

10.1 Uygunsuzluk ve düzeltici faaliyet

Bir uygunsuzluk oluştuğunda, kuruluş aşağıdakileri yerine getirmelidir:

a) Uygunsuzluğa tepki verilmesi ve mümkün olması durumunda:

   1) edilmesi ve düzeltmek için eyleme geçilmesi ve
   2) Sonuçları ile ilgilenilmesi,

b) Aşağıdakilerin yerine getirilmesi yoluyla, uygunsuzluğun başka bir yerde tekrar etmemesi veya oluşmaması için nedenlerinin giderilmesi amacıyla eyleme geçme ihtiyacının değerlendirilmesi:

   1) Uygunsuzluğu gözden geçirerek,
   2) Uygunsuzluğun nedenleri belirlenerek ve
   3) Benzer uygunsuzlukların var olup olmadığını veya olasılıkla gerçekleşip gerçekleşmeyeceğini belirleyerek,

c) Gerekli tüm faaliyetlerin uygulanması,
d) Tüm düzeltici faaliyetlerin etkinliğinin gözden geçirilmesi ve
e) Gerekli olan durumlarda bilgi güvenliği yönetim sisteminde değişikliklerin yapılması.

Düzeltici faaliyetler, karşılaşılan uygunsuzlukların etkilerine uygun olmalıdır.

Kuruluş aşağıdakilerin delili olarak ***yazılı bilgileri*** muhafaza etmelidir:

f) Uygunsuzlukların doğası ve gerçekleştirilen müteakip eylemler ve
g) Herhangi bir düzeltici faaliyetin sonuçları.

10.2 Sürekli iyileştirme

Kuruluş, bilgi güvenliği yönetim sisteminin uygunluğunu, doğruluğunu ve etkinliğini sürekli olarak iyileştirmelidir.

TÜRK STANDARDLARI ENSTİTÜSÜ

ÖRNEK

İyileştirme Örnekler

Ek A

Referans kontrol amaçları ve kontroller

Ek A ‘da listelenen kontrol amaçları ve kontroller, Madde 6.1.3 bağlamında kullanılmak üzere, doğrudan ISO/IEC 27002:2013 [1] madde 5’ten madde 18’e kadar listelenenlerden çıkarılmış ve sıraya konulmuştur.

Ek A - amaçları ve kontroller

A.5 Bilgi güvenliği politikaları

A.5.1 Bilgi güvenliği için yönetimin yönlendirmesi

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

A.5.1.1 Bilgi güvenliği için politikalar

Bir dizi bilgi güvenliği politikaları, yönetim tarafından tanımlanmalı, onaylanmalı ve yayınlanarak çalışanlara ve ilgili dış taraflara bildirilmelidir.

A.5.1.2 Bilgi güvenliği için politikaların gözden geçirilmesi

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

A.6 Bilgi güvenliği organizasyonu

A.6.1 İç organizasyon

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

A.6.1.1 Bilgi güvenliği rolleri ve sorumlulukları

Tüm bilgi güvenliği sorumlulukları tanımlanmalı ve tahsis edilmelidir.

A.6.1.2 Görevlerin ayrılığı

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

A.6.1.3 Otoritelerle iletişim

İlgili otoritelerle uygun iletişim kurulmalıdır.

A.6.1.4 Özel ilgi grupları ile iletişim

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

A.6.1.5 Proje yönetiminde bilgi güvenliği

Proje yönetiminde, proje çeşidine bakılmaksızın bilgi güvenliği ele alınmalıdır.

A.6.2 Mobil cihazlar ve uzaktan çalışma

Amaç: Uzaktan çalışma ve mobil cihazların güvenliğini sağlamak.

A.6.2.1 Mobil cihaz politikası

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

A.6.2.2 Uzaktan çalışma

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

A.7 İnsan kaynakları güvenliği

A.7.1 İstihdam öncesi

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

A.7.1.1 Tarama

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

A.7.1.2 İstihdam hüküm ve koşulları

Çalışanlar ve yükleniciler ile yapılan sözleşmeler kendilerinin ve kuruluşun bilgi güvenliği sorumluluklarını belirtmelidir.

A.7.2 Çalışma esnasında

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

A.7.2.1 Yönetimin sorumlulukları

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

A.7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi

Kuruluştaki tüm çalışanlar ve ilgili olduğu durumda, yükleniciler, kendi iş fonksiyonları ile ilgili, kurumsal politika ve prosedürlere ilişkin uygun farkındalık eğitim ve öğretimini ve bunların düzenli güncellemelerini almalıdırlar.

A.7.2.3 Disiplin prosesi

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

A.7.3 İstihdamın sonlandırılması ve değiştirilmesi

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

A.7.3.1 İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi

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

A.8 Varlık yönetimi

A.8.1 Varlıkların sorumluluğu

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

A.8.1.1 Varlıkların envanteri

Bilgi ve bilgi işleme olanakları ile ilgili varlıklar belirlenmeli ve bu varlıkların bir envanteri çıkarılmalı ve idame ettirilmelidir.

A.8.1.2 Varlıkların sahipliği

Envanterde tutulan tüm varlıklara sahip atamaları yapılmalıdır.

A.8.1.3 Varlıkların kabul edilebilir kullanımı

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

A.8.1.4 Varlıkların iadesi

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

A.8.2 Bilgi sınıflandırma

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

A.8.2.1 Bilgi sınıflandırması

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

A.8.2.2 Bilgi etiketlemesi

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

A.8.2.3 Varlıkların kullanımı

Varlıkların kullanımı için prosedürler, kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.

8.3 Ortam işleme

Amaç: Ortamda depolanan bilginin yetkisiz ifşası, değiştirilmesi, kaldırılması ve yok edilmesini engellemek.

8.3.1 Taşınabilir ortam yönetimi

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

8.3.2 Ortamın yok edilmesi

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

8.3.3 Fiziksel ortam aktarımı

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

A.9 Erişim kontrolü

A.9.1 Erişim kontrolünün iş gereklilikleri

Amaç: Bilgi ve bilgi işleme olanaklarına erişimi kısıtlamak

A.9.1.1 Erişim kontrol politikası

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

A.9.1.2 Ağlara ve ağ hizmetlerine erişim

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

A.9.2 Kullanıcı erişim yönetimi

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

A.9.2.1 Kullanıcı kaydetme ve kayıt silme

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

A.9.2.2 Kullanıcı erişimine izin verme

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

A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi

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

A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi

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

A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi

Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirmelidir.

A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi

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

A.9.3 Kullanıcı sorumlulukları

Amaç: Kullanıcıları kendi kimlik doğrulama bilgilerinin korunması konusunda sorumlu tutmak

A.9.3.1 Gizli kimlik doğrulama bilgisinin kullanımı

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

A.9.4 Sistem ve uygulama erişim kontrolü

Amaç: Sistem ve uygulamalara yetkisiz erişimi engellemek

A.9.4.1 Bilgiye erişimin kısıtlanması

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

A.9.4.2 Güvenli oturum açma prosedürleri

Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir.

A.9.4.3 Parola yönetim sistemi

Parola yönetim sistemleri etkileşimli olmalı ve yeterli güvenlik seviyesine sahip parolaları temin etmelidir.

A.9.4.4 Ayrıcalıklı destek programlarının kullanımı

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

A.9.4.5 Program kaynak koduna erişim kontrolü

Program kaynak koduna erişim kısıtlanmalıdır.

A.10 Kriptografi

A.10.1 Kriptografik kontroller

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

A.10.1.1 Kriptografik kontrollerin kullanımına ilişkin politika

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

A.10.1.2 Anahtar yönetimi

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

A.11 Fiziksel ve çevresel güvenlik

A.11.1 Güvenli alanlar

Amaç: Yetkisiz fiziksel erişimi, kuruluşun bilgi ve bilgi işleme olanaklarına hasar verilmesi ve müdahale edilmesini engellemek

A.11.1.1 Fiziksel güvenlik sınırı

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

A.11.1.2 Fiziksel giriş kontrolleri

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

A.11.1.3 Ofislerin, odaların ve tesislerin güvenliğinin sağlanması

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

A.11.1.4 Dış ve çevresel tehditlere karşı koruma

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

A.11.1.5 Güvenli alanlarda çalışma

Güvenli alanlarda çalışma için prosedürler tasarlanmalı ve uygulanmalıdır.

A.11.1.6 Teslimat ve yükleme alanları

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 olanaklarından ayrılmalıdır.

A.11.2 Teçhizat

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

A.11.2.1 Teçhizat yerleştirme ve koruma

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

A.11.2.2 Destekleyici altyapı hizmetleri

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

A.11.2.3 Kablo güvenliği

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

A.11.2.4 Teçhizat bakımı

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

A.11.2.5 Varlıkların taşınması

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

A.11.2.6 Kuruluş dışındaki teçhizat ve varlıkların güvenliği

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

A.11.2.7 Teçhizatın güvenli yok edilmesi veya tekrar kullanımı

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.

A.11.2.8 Gözetimsiz kullanıcı teçhizatı

Kullanıcılar, gözetimsiz teçhizatın uygun şekilde korunmasını temin etmelidir.

A.11.2.9 Temiz masa temiz ekran politikası

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

A.12 İşletim güvenliği

A.12.1 İşletim prosedürleri ve sorumlulukları

Amaç: Bilgi işleme olanaklarının doğru ve güvenli işletimlerini temin etmek

A.12.1.1 Yazılı işletim prosedürleri

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

A.12.1.2 Değişiklik yönetimi

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

A.12.1.3 Kapasite yönetimi

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

A.12.1.4 Geliştirme, test ve işletim ortamların birbirinden ayrılması

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

A.12.2 Kötücül yazılımlardan koruma

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

A.12.2.1 Kötücül yazılımlara karşı kontroller

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

A.12.3 Yedekleme

Amaç: Veri kaybına karşı koruma sağlamak

A.12.3.1 Bilgi yedekleme

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

A.12.4 Kaydetme ve izleme

Amaç: Olayları kaydetme ve kanıt üretmek

A.12.4.1 Olay kaydetme

Kullanıcı işlemleri, kural dışılıklar, hatalar ve bilgi güvenliği olaylarını kaydeden olay kayıtları üretilmeli, saklanmalı ve düzenli olarak gözden geçirilmelidir.

A.12.4.2 Kayıt bilgisinin korunması

Kaydetme olanakları ve kayıt bilgileri kurcalama ve yetkisiz erişime karşı korunmalıdır.

A.12.4.3 Yönetici ve operatör kayıtları

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

A.12.4.4 Saat senkronizasyonu

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

A.12.5 İşletimsel yazılımının kontrolü

Amaç: İşletimsel sistemlerin bütünlüğünü temin etmek

A.12.5.1 İşletimsel sistemler üzerine yazılım kurulumu

İşletimsel sistemler üzerine yazılım kurulumunun kontrolü için prosedürler uygulanmalıdır.

A.12.6 Teknik açıklık yönetimi

Amaç: Teknik açıklıkların kullanılmasını engellemek

A.12.6.1 Teknik açıklıkların yönetimi

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

A.12.6.2 Yazılım kurulumu kısıtlamaları

Kullanıcılar tarafından yazılım kurulumuna dair kurallar oluşturulmalı ve uygulanmalıdır.

A.12.7 Bilgi sistemleri tetkik hususları

Amaç: Tetkik faaliyetlerinin işletimsel sistemler üzerindeki etkilerini asgariye indirmek.

A.12.7.1 Bilgi sistemleri tetkik kontrolleri

İşletimsel sistemlerin doğrulanmasını kapsayan tetkik gereksinimleri ve faaliyetleri, iş proseslerindeki kesintileri asgariye indirmek için dikkatlice planlanmalı ve üzerinde anlaşılmalıdır.

A.13 Haberleşme güvenliği

A.13.1 Ağ güvenliği yönetimi

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

A.13.1.1 Ağ kontrolleri

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

A.13.1.2 Ağ hizmetlerinin güvenliği

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.

A.13.1.3 Ağlarda ayrım

Ağlarda, bilgi hizmetleri, kullanıcıları ve bilgi sistemleri grupları ayrılmalıdır.

A.13.2 Bilgi transferi

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

A.13.2.1 Bilgi transfer politikaları ve prosedürleri

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

A.13.2.2 Bilgi transferindeki anlaşmalar

Anlaşmalar, kuruluş ve dış taraflar arasındaki iş bilgileri'nin güvenli transferini ele almalıdır.

A.13.2.3 Elektronik mesajlaşma

Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.

A.13.2.4 Gizlilik ya da ifşa etmeme anlaşmaları

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

A.14 Sistem temini, geliştirme ve bakımı

A.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 gereksinimlerini de içerir.

A.14.1.1 Bilgi güvenliği gereksinimleri analizi ve belirtimi

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

A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması

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

A.14.1.3 Uygulama hizmet işlemlerinin korunması

Uygulama hizmet işlemlerindeki bilgi eksik iletim, yanlış yönlendirme, yetkisiz mesaj değiştirme, yetkisiz ifşayı, yetkisiz mesaj çoğaltma ya da mesajı yeniden oluşturmayı önlemek için korunmalıdır.

A.14.2 Geliştirme ve destek süreçlerinde güvenlik

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

A.14.2.1 Güvenli geliştirme politikası

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

A.14.2.2 Sistem değişiklik kontrolü prosedürleri

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

A.14.2.3 İşletim platformu değişikliklerden sonra uygulamaların teknik gözden geçirmesi

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

A.14.2.4 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar

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

A.14.2.5 Güvenli sistem mühendisliği prensipleri

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

A.14.2.6 Güvenli geliştirme ortamı

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

A.14.2.7 Dışarıdan sağlanan geliştirme

Kuruluş dışarıdan sağlanan sistem geliştirme faaliyetini denetlemeli ve izlemelidir.

A.14.2.8 Sistem güvenlik testi

Güvenlik işlevselliğinin test edilmesi, geliştirme süresince gerçekleştirilmelidir.

A.14.2.9 Sistem kabul testi

Kabul test programları ve ilgili kriterler, yeni bilgi sistemleri, yükseltmeleri ve yeni versiyonları için belirlenmelidir.

A.14.3 Test verisi

Amaç: Test için kullanılan verinin korunmasını sağlamak.

A.14.3.1 Test verisinin korunması

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

A.15 Tedarikçi ilişkileri

A.15.1 Tedarikçi ilişkilerinde bilgi güvenliği

Amaç: Kuruluşa ait tedarikçiler tarafından erişilen varlıkların korunmasını sağlamak.

A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası

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

A.15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme

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.

A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri

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

A.15.2 Tedarikçi hizmet sağlama yönetimi

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

A.15.2.1 Tedarikçi hizmetlerini izleme ve gözden geçirme

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

A.15.2.2 Tedarikçi hizmetlerindeki değişiklikleri yönetme

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.

A.16 Bilgi güvenliği ihlal olayı yönetimi

A.16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirilmelerin yönetimi

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

A.16.1.1 Sorumluluklar ve prosedürler

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

A.16.1.2 Bilgi güvenliği olaylarının raporlanması

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

A.16.1.3 Bilgi güvenliği açıklıklarının raporlanması

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.

A.16.1.4 Bilgi güvenliği olaylarında değerlendirme ve karar verme

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

A.16.1.5 Bilgi güvenliği ihlal olaylarına yanıt verme

Bilgi güvenliği ihlal olaylarına, yazılı prosedürlere uygun olarak yanıt verilmelidir.

A.16.1.6 Bilgi güvenliği ihlal olaylarından ders çıkarma

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

A.16.1.7 Kanıt toplama

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

A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları

A.17.1 Bilgi güvenliği sürekliliği

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

A.17.1.1 Bilgi güvenliği sürekliliğinin planlanması

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

A.17.1.2 Bilgi güvenliği sürekliliğinin uygulanması

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

A.17.1.3 Bilgi güvenliği sürekliliği'nin doğrulanması, gözden geçirilmesi ve değerlendirilmesi

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

A.17.2 Yedek fazlalıklar

Amaç: Bilgi işleme olanaklarının erişilebilirliğini temin etmek.

A.17.2.1 Bilgi işleme olanaklarının erişilebilirliği

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

A.18 Uyum

A.18.1 Yasal ve sözleşmeye tabi gereksinimlerle uyum

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

A.18.1.1 Uygulanabilir yasaları ve sözleşmeye tabi gereksinimleri tanımlama

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

A.18.1.2 Fikri mülkiyet hakları

Fikri mülkiyet hakları ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalardan doğan şartlara uyum sağlamak için uygun prosedürler gerçekleştirilmelidir.

A.18.1.3 Kayıtların korunması

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

A.18.1.4 Kişi tespit bilgisinin gizliliği ve korunması

Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde ilgili yasa ve düzenlemeler ile sağlanmalıdır.

A.18.1.5 Kriptografik kontrollerin düzenlemesi

Kriptografik kontroller tüm ilgili sözleşmeler, yasa ve düzenlemelere uyumlu bir şekilde kullanılmalıdır.

A.18.2 Bilgi güvenliği gözden geçirmeleri

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

A.18.2.1 Bilgi güvenliğinin bağımsız gözden geçirmesi

Kuruluşun bilgi güvenliğine ve uygulamasına(örn. bilgi güvenliği için kontrol hedefleri, kontroller, politikalar, prosesler ve prosedürler) yaklaşımı belirli aralıklarla veya önemli değişiklikler meydana geldiğinde bağımsız bir şekilde gözden geçirilmelidir.

A.18.2.2 Güvenlik politikaları ve standartları ile uyum

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

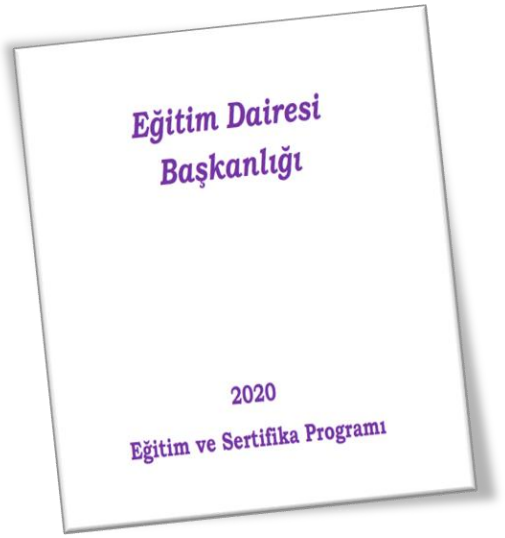
A.18.2.3 Teknik uyum gözden geçirmesi

Kuruluşun bilgi güvenliği politika ve standartları ile uyumu için bilgi sistemleri düzenli bir şekilde gözden geçirilmelidir.

EĞİTİM PROGRAMLARIMIZ VE DETAYLI BİLGİ İÇİN

www.tse.org.tr

➔ Hizmetlerimiz / Eğitimler/ Eğitim ve Sertifika Programı



TEŞEKKÜR EDERİZ…