ISO/27001 EK-A MADDELERİ

	A.5 Bilgi güvenliği politikaları		
1	**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	*Kontrol* 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	*Kontrol* 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	*Kontrol* Tüm bilgi güvenliği sorumlulukları tanımlanmalı ve tahsis edilmelidir.
	A.6.1.2	Görevlerin ayrılığı	*Kontrol* Çelişen görevler ve sorumluluklar, yetkilendirilmemiş veya kasıtsız değişiklik fırsatlarını veya kuruluş varlıklarının yanlış kullanımını azaltmak amacıyla ayrılmalıdır.
	A.6.1.3	Otoritelerle iletişim	*Kontrol* ilgili otoritelerle uygun iletişim kurulmalıdır.
	A.6.1.4	Özel ilgi grupları ile iletişim	*Kontrol* Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel demekler ile uygun iletişim kurulmalıdır.
	A.6.1.5	Proje yönetiminde bilgi güvenliği	*Kontrol* 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	*Kontrol* Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.
	A.6.2.2	Uzaktan çalışma	*Kontrol* Uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak amacı ile bir politika ve destekleyici güvenlik önlemleri uygulanmalıdır.

2	**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	*Kontrol* 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	*Kontrol* 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	*Kontrol* Yönetim, çalışanlar ve yüklenicilerin, kuruluşun yerleşik politika ve prosedürlerine göre bilgi güvenliğini uygulamalarını istemelidir.
	A.7.2.2	Bilgi güvenliği farkındalığı, eğitim ve öğretimi	*Kontrol* 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	*Kontrol* Bir bilgi güvenliği ihlal olayını gerçekleştiren çalışanlara yönelik önlem almak için resmi ve bildirilmiş birdisiplin 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	*Kontrol* 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	*Kontrol* Bilgi ve bilgi işleme olanakları ile ilgili varlıklar belirlenmeli ve bu varlıkların bir envanteri çıkarılmalı ve idame ettirilmelidir.
	A.8.1.2	Varlıkların sahipliği	*Kontrol* Envanterde tutulan tüm varlıklara sahip atamaları yapılmalıdır.
	A.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.
	A.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.

A.8.2 Bilgi sınıflandırma		
Amaç: Bilginin kurum için önemi derecesinde uygun seviyede korunmasını temin etmek.		
A.8.2.1	Bilgi sınıflandırması	*Kontrol* Bilgi, yasal şartlar, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre sınıflandırılmalıdır.
A.8.2.2	Bilgi etiketlemesi	*Kontrol* Bilgi etiketleme için uygun bir prosedür kümesi kuruluş tarafından benimsenen sınıflandırma düzenine göre geliştirilmeli ve uygulanmalıdır.
A.8.2.3	Varlıkların kullanımı	*Kontrol* 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.		
08.03.2001	Taşınabilir ortam yönetimi	*Kontrol* Taşınabilir ortam yönetimi için prosedürler kuruluş tarafından benimsenen sınıflandırma düzenine göre uygulanmalıdır.
08.03.2002	Ortamın yok edilmesi	*Kontrol* Ortam artık ihtiyaç kalmadığında resmi prosedürler kullanılarak güvenli bir şekilde yok edilmelidir.
08.03.2003	Fiziksel ortam aktarımı	*Kontrol* 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	*Kontrol* 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	*Kontrol* Erişim haklarının atanmasını sağlamak için, resmi bir kullanıcı kaydetme ve kayıt silme prosesi uygulanmalıdır.
A.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.
A.9.2.3	Ayrıcalıklı erişim haklarının yönetimi	*Kontrol* Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımı kısıtlanmalı ve kontrol edilmelidir.
A.9.2.4	Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi	*Kontrol* Gizli kimlik doğrulama bilgisinin tahsis edilmesi, resmi bir yönetim prosesi yoluyla kontrol edilmelidir.

4	A.9.2.5	Kullanıcı erişim haklarının gözden geçirilmesi	*Kontrol* Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirmelidir.
	A.9.2.6	Erişim haklarının kaldırılması veya düzenlenmesi	*Kontrol* 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	*Kontrol* 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	*Kontrol* Bilgi ve uygulama sistem fonksiyonlarına erişim, erişim kontrol politikası doğrultusunda kısıtlanmalıdır.
	A.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.
	A.9.4.3	Parola yönetim sistemi	*Kontrol* Parola yönetim sistemleri etkileşimli olmalı ve yeterli güvenlik seviyesine sahip parolaları temin etmelidir.
	A.9.4.4	Ayrıcalıklı destek programlarının kullanımı	*Kontrol* 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	*Kontrol* 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	*Kontrol* Bilginin korunması için kriptografik kontrollerin kullanımına dair bir politika geliştirilmeli ve uygulanmalıdır.
	A.10.1.2	Anahtar yönetimi	*Kontrol* Kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair bir politika geliştirilmeli ve tüm yaşam çevirimleri süresince uygulanmalıdır.

5

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	*Kontrol* Hassas veya kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmalı ve kullanılmalıdır.
A.11.1.2	Fiziksel giriş kontrolleri	*Kontrol* 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	*Kontrol* Ofisler, odalar ve tesisler için fiziksel güvenlik tasarlanmalı ve uygulanmalıdır.
A.11.1.4	Dış ve çevresel tehditlere karşı koruma	*Kontrol* Doğal felaketler, kötü niyetli saldırılar veya kazalara karşı fiziksel koruma tasarlanmalı ve uygulanmalıdır.
A.11.1.5	Güvenli alanlarda çalışma	*Kontrol* Güvenli alanlarda çalışma için prosedürler tasarlanmalı ve uygulanmalıdır.
A.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 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	*Kontrol* Teçhizat, çevresel tehditlerden ve tehlikelerden ve yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmeli ve korunmalıdır.
A.11.2.2	Destekleyici altyapı hizmetleri	*Kontrol* Teçhizat destekleyici altyapı hizmetlerindeki hatalardan kaynaklanan enerji kesintileri ve diğer kesintilerden korunmalıdır.
A.11.2.3	Kablo güvenliği	*Kontrol* Veri veya destekleyici bilgi hizmetlerini taşıyan enerji ve telekomünikasyon kabloları, dinleme, girişim oluşturma veya hasara karsı korunmalıdır.
A.11.2.4	Teçhizat bakımı	*Kontrol* Teçhizatın bakımı, sürekli erişilebilirliğini ve bütünlüğünü temin etmek için doğru şekilde yapılmalıdır.
A.11.2.5	Varlıkların taşınması	*Kontrol* Teçhizat, bilgi veya yazılım ön yetkilendirme olmaksızın kuruluş dışına çıkarılmamalıdır.

6	A.11.2.6	Kuruluş dışındaki teçhizat ve varlıkların güvenliği	*Kontrol* 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	*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.
	A.11.2.8	Gözetimsiz kullanıcı teçhizatı	*Kontrol* Kullanıcılar, gözetimsiz teçhizatın uygun şekilde korunmasını temin etmelidir.
	A.11.2.9	Temiz masa temiz ekran politikası	*Kontrol* 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	*Kontrol* İşletim prosedürleri yazılı hale getirilmeli ve ihtiyacı olan tüm kullanıcılara sağlanmalıdır.
	A.12.1.2	Değişiklik yönetimi	*Kontrol* Bilgi güvenliğini etkileyen, kuruluş, iş prosesleri, bilgi işleme olanakları ve sistemlerdeki değişiklikler kontrol edilmelidir.
	A.12.1.3	Kapasite yönetimi	*Kontrol* 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	*Kontrol* 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	*Kontrol* 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	*Kontrol* 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		

7	A.12.4.1	Olay kaydetme	*Kontrol* 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	*Kontrol* Kaydetme olanakları ve kayıt bilgileri kurcalama ve yetkisiz erişime karşı korunmalıdır.
	A.12.4.3	Yönetici ve operatör kayıtları	*Kontrol* Sistem yöneticileri ve sistem operatörlerinin işlemleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.
	A.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.
	A.12.5 İşletimsel yazılımının kontrolü		
	Amaç: İşletimsel sistemlerin bütünlüğünü temin etmek		
	A.12.5.1	İşletimsel sistemler üzerine yazılım kurulumu	*Kontrol* 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	*Kontrol* 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	*Kontrol* 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	*Kontrol* 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	*Kontrol* Sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağlar yönetilmeli ve kontrol edilmelidir.
	A.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.

8	A.13.1.3	Ağlarda ayrım	*Kontrol* 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	*Kontrol* Tüm iletişim olanağı türlerinin kullanımıyla bilgi transferini korumak için resmi transfer politikaları, prosedürleri ve kontrolleri mevcut olmalıdır.
	A.13.2.2	Bilgi transferindeki anlaşmalar	*Kontrol* Anlaşmalar, kuruluş ve dış taraflar arasındaki iş bilgileri'nin güvenli transferini ele almalıdır.
	A.13.2.3	Elektronik mesajlaşma	*Kontrol* Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.
	A.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.
	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	*Kontrol* Bilgi güvenliği ile ilgili gereksinimler, yeni bilgi sistemleri gereksinimlerine veya varolan bilgi sistemlerinin iyileştirmelerine dâhil edilmelidir.
	A.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.
	A.14.1.3	Uygulama hizmet işlemlerinin korunması	*Kontrol* 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 Ge	**iştirme 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	*Kontrol* Yazılım ve sistemlerin geliştirme kuralları belirlenmeli ve kuruluş içerisindeki geliştirmelere uygulanmalıdır.
	A.14.2.2	Sistem değişiklik kontrolü prosedürleri	*Kontrol* 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	*Kontrol* İşletim platformları değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş için kritik uygulamalar gözden geçirilmeli ve test edilmelidir.

9	A.14.2.4	Yazılım paketlerindeki değişikliklerdeki kısıtlamalar	*Kontrol* Yazılım paketlerine yapılacak değişiklikler, gerek duyulanlar hariç önlenmeli ve tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.
	A.14.2.5	Güvenli sistem mühendisliği prensipleri	*Kontrol* Güvenli sistem mühendisliği prensipleri belirlenmeli, yazılı hale getirilmeli ve tüm bilgi sistemi uygulama çalışmalarına uygulanmalıdır.
	A.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.
	A.14.2.7	Dışarıdan sağlanan geliştirme	*Kontrol* Kuruluş dışarıdan sağlanan sistem geliştirme faaliyetini denetlemeli ve izlemelidir.
	A.14.2.8	Sistem güvenlik testi	*Kontrol* Güvenlik işlevselliğinin test edilmesi, geliştirme süresince gerçekleştirilmelidir.
	A.14.2.9	Sistem kabul testi	*Kontrol* 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	*Kontrol* 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	*Kontrol* 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	*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.
	A.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.
	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	*Kontrol* Kuruluşlar düzenli aralıklarla tedarikçi hizmet sunumunu izlemeli, gözden geçirmeli ve tetkik etmelidir.

10	A.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.
	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	*Kontrol* 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	*Kontrol* Bilgi güvenliği olayları uygun yönetim kanalları aracılığı ile olabildiğince hızlı bir şekilde raporlanmalıdır.
	A.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.
	A.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.
	A.16.1.5	Bilgi güvenliği ihlal olaylarına yanıt verme	*Kontrol* Bilgi güvenliği ihlal olaylarına, yazılı prosedürlere uygun olarak yanıt verilmelidir.
	A.16.1.6	Bilgi güvenliği ihlal olaylarından ders çıkarma	*Kontrol* 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	*Kontrol* 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: Bilg	Bilgi güvenliği sürekliliği, kuruluşun iş sürekliliği yönetim sistemlerinin içerisine dahil edilmelidir..	
	A.17.1.1	Bilgi güvenliği sürekliliğinin planlanması	*Kontrol* 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	*Kontrol* Kuruluş, olumsuz bir olay süresince bilgi güvenliği için istenen düzeyde sürekliliğin sağlanması için prosesleri, prosedürleri ve kontrolleri kurmalı, yazılı hale getirmeli, uygulamalı ve sürdürmelidir.

11	A.17.1.3	Bilgi güvenliği sürekliliği'nin doğrulanması, gözden geçirilmesi ve değerlendirilmesi	*Kontrol* 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	*Kontrol* 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	*Kontrol* 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	*Kontrol* 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	*Kontrol* 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	*Kontrol* Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde ilgili yasa ve düzenlemeler ile sağlanmalıdır.
	A.18.1.5	Kriptografik kontrollerin düzenlemesi	*Kontrol* 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	*Kontrol* 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	*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.
	A.18.2.3	Teknik uyum gözden geçirmesi	*Kontrol* Kuruluşun bilgi güvenliği politika ve standartları ile uyumu için bilgi sistemleri düzenli bir şekilde gözden geçirilmelidir.