|  |  |
| --- | --- |
| Müşteri Kuruluş | æfirmaadiæ |
| Adres | æfirmaadresiæ |
| İletişim Bilgileri | æfirmatelefonæ æfirmafaksæ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kapsam | æbelgelendirmekapsamiæ | | | |
| Standard | ISO/IEC 27001:2023 | | | |
| Denetim Tipi | İlk Belgelendirme | Gözetim | Yeniden Belgelen. | Özel |

|  |  |
| --- | --- |
| Başdenetçi | æbasdenetciadiæ |
| Denetçi | ædenetciadi1æ |
| Denetçi | ædenetciadi2æ |
| Teknik Uzman | æteknikuzmanadi1æ |
| Teknik Uzman | æteknikuzmanadi2æ |
| Gözlemci | ægozlemciadi1æ |
| Değerlendirici | ægozlemciadi1æ |

|  |  |
| --- | --- |
| Müşteri KuruluşYetkili Temsilcisi | æyonetimtemsilcisiadiæ |

|  |
| --- |
| Bu raporun içeriği, müşteri kuruluşun kendisi ve Aliment dışında gizlidir.  Bu raporun tamamı veya bir kısmının müşteri kuruluşun çalışanları veya Aliment dışında çoğaltılması ve dağıtılması, dağıtımdan önce yazılı mutabakat ile mümkündür (TÜRKAK gibi kurumlar hariç).  Bu raporda yer alan uygunsuzluklar, örnekleme usulü yapılan çalışma sonucunu yansıtır ve bu sebeple başka uygunsuzluk olmadığı anlamını taşımaz. |

|  |  |  |  |
| --- | --- | --- | --- |
| Denetim Tarihi | ædenetimtarihleriæ | Denetim/Gün Sayısı | ædenetimzamaniæ |

|  |  |
| --- | --- |
| Denetim Hedefi | 1. Denetim kriterleri kullanılarak, müşterinin yönetim sisteminin veya bir bölümünün uygunluğunun tayini, 2. Yönetim sisteminin yeteneği ile müşterinin uygulanabilir, yasal, düzenleyici ve sözleşme gerekliliklerini karşıladığından emin olunmasının tayini, 3. Müşterinin, belirlenen hedeflere ulaşılabileceği beklentisini güvence altına almak için yönetim sisteminin etkinliğinin tayini, 4. Uygun olması durumunda, yönetim sisteminin potansiyel iyileştirme alanlarının tanımı. |
| Denetim Kriterleri | El kitabı, prosesler, prosedürler, yönetmelik vb. |

|  |  |  |
| --- | --- | --- |
| Denetlenen Adresler | | Tarihler |
| Saha Adresleri | æsubeadresiaæ |  |
| æsubeadresibæ |  |
| æsubeadresicæ |  |

\* Saha sayısı 3’ten fazla ise gerektiği kadar satır eklenebilir.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Çalışan Sayısı | ætamzamanlicalisansayisiæ | Taşeron Çalışan Sayısı | ætaseroncalisansayisiæ | Toplam  Çalışan Sayısı | ætoplamcalisansayisiæ |

|  |
| --- |
| Rapor Özeti |
| æfirmaadiæ’ in, EYS kurulmasında ve işletilmesi konusunda ihtiyaç duyulan dokümantasyonu oluşturduğu ve sistemin, bazı eksiklikleri ile etkin bir şekilde yürütüldüğü gözlemlendi.  æfirmaadiæ’ in üst yönetiminin ve personelin bakış açısı ve alt yapı olarak, EYS şartlarına hazır olduğu gözlemlendi.  Denetim esnasında, 20 adet uygunsuzluk tespit edilmiş olup, bunlardan 6 tanesi majör/kritik, 14 tanesi minör uygunsuzluk olarak belirlendi.  Denetim esnasında, æfirmaadiæ’ in, yönetim sisteminin bazı yönlerini geliştirmesi gerektiği gözlenmiş bunların bir kısmı raporda uygunsuzluk/iyileştirmeye açık alan olarak belirtildi. |

|  |  |  |  |
| --- | --- | --- | --- |
| Toplam majör uygunsuzluk |  | Toplam minör uygunsuzluk |  |

|  |  |
| --- | --- |
| Genel | |
| Varsa denetim planından herhangi bir sapma ve nedenleri | Denetim planından herhangi bir sapma söz konusu olmamıştır. |
| Varsa denetim programını etkileyen durumlar | Denetim programında değişiklik gerektirecek her hangi bir durum görülmemiştir. |
| Varsa son denetimden sonra müşterinin yönetim sistemini etkileyen değişiklikler | Son denetimden sonra, æfirmaadiæ’ nin yönetim sistemini etkileyen her hangi bir değişiklik uygulaması görülmemiştir. |
| Varsa çözümlenmemiş hususlar | Çözümlenmemiş her hangi bir husus bulunmamaktadır. |
| Önceki denetimde tespit edilmiş olan uygunsuzluklara ait düzeltici faaliyetlerin etkinlik kontrolü | Önceki denetimde Aşama 1’ de tespit edilmiş olan 4 adet uygunsuzluğa ait düzeltici faaliyetlerin etkinlik kontrolü yapılmış ve tamamının 3 tanesinin kapatıldığı, 1 tanesinin de kapatılmadığı tespit edilmiş ve Aşama 2’ de tekrar uygunsuzluk açılmıştır. |
| Sertifika, marka ve logo kullanımı | Sertifika, marka ve logo kullanımının uygun olduğu görülmüştür. |
| Yönetim sistem/lerinin uygulanabilir gereklilikler ve beklenen çıktıları karşılama yeteneği | Yönetim sistem/lerinin uygulanabilir şartlar ve beklenen çıktıları karşılayacak yapıda oluşturulduğu ve uygulandığı görülmüştür. |
| İç denetim ve yönetimin gözden geçirmesi prosesleri | 2020 yılı iç denetimlerinin, tarihleri arasında yapıldığı görüldü.  Toplam 3 bölüm/birimde iç denetim gerçekleştirildiği görüldü.  İç denetimlerde, 1 adet uygunsuzluk belirlendiği görüldü.  2020 yılında 12.05.2020 tarihinde gerçekleştirildiği görüldü.  İlgili standardların girdi ve çıktılarının ele alındığı görüldü. |
| Kapsam ve sınırların teyidi |  |
| Uygulandı ise denetim tipi | Birleşik  Ortak  Entegre |
| Denetim hedeflerine ulaşma durumu | Denetimde;   1. Denetim kriterleri kullanılarak, müşterinin yönetim sisteminin veya bir bölümünün uygunluğunun tayini, 2. Yönetim sisteminin yeteneği ile müşterinin uygulanabilir, yasal, düzenleyici ve sözleşme şartlarını karşıladığından emin olunmasının tayini, 3. Müşterinin, belirlenen hedeflere ulaşılabileceği beklentisini güvence altına almak için yönetim sisteminin etkinliğinin tayini, 4. Uygun olması durumunda, yönetim sisteminin potansiyel iyileştirme alanlarının tanımı.   görüldüğünden, denetim hedeflerine ulaşılmıştır. |

|  |  |
| --- | --- |
| Gözlemler | |
| No | Olumlu Yönler |
|  |  |
|  |  |
|  |  |
|  |  |
| No | İyileştirmeye Açık Alanlar |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Bulgular | | | |
| No | Standard/Madde No | Uygunsuzluk Sınıfı | Uygunsuzluk Açıklaması |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |
| --- | --- |
| Denetim Sonucuna İlişkin Denetim Ekibinin Tavsiye Kararı | |
| İlk  Belgelendirme | Sertifika verilmesi |
| Sertifika verilmemesi |
| Takip denetimi yapılması |
| Gözetim | Belgelendirmenin sürdürülmesi |
| Belgelendirmenin askıya alınması |
| Takip denetimi yapılması |
| Yeniden  Belgelendirme | Belgelendirmenin yenilenmesi |
| Belgelendirmenin yenilenmemesi |
| Takip denetimi yapılması |
| Diğer | Kapsam değişikliği yapılması |
| Adres değişikliği yapılması |

|  |
| --- |
| Aliment, gerçekleştirilen her denetimden sonra, denetim raporlarını, müşteri kuruluşa iletmektedir.  Belgelendirme sözleşmesi gereği raporları, 3 yıllık belgelendirme çevrimi boyunca muhafaza etmeniz ve talep edilmesi durumunda ibraz etmeniz gerekmektedir. |

|  |
| --- |
| Başdenetçi |
| æbasdenetciadiæ |
| İmza |
|  |

| ISO/IEC 27001:2022 | | |
| --- | --- | --- |
| Gereklilikler | | Bulgular |
| 4 4.1*\** | KURULUŞUN BAĞLAMI Kuruluş ve bağlamının anlaşılması Kuruluş, amacı ile ilgili olan ve bilgi güvenliği yönetim sisteminin amaçlanan sonuçlarına/çıktılarına ulaşma kabiliyetini etkileyen iç ve dış hususları belirlemiş midir?  *NOT Bu konuların belirlenmesi, ISO 31000:2018, Madde 5.4.1'de ele alınan kuruluşun dış ve iç bağlamının oluşturulması anlamına gelir.* |  |
| 4.2*\** | 4.2 İlgili tarafların ihtiyaç ve beklentilerini anlaşılması  Kuruluş aşağıdakileri belirlemiş midir?  a) Bilgi güvenliği yönetim sistemi ile ilgili olan ilgili taraflar,  b) Bu ilgili tarafların ilgili gereklilikleri,  c) Bu gerekliliklerden hangisinin bilgi güvenliği yönetim sisteminde ele alınacağı.  *NOT İlgili tarafların gereklilikleri, yasal ve düzenleyici gereklilikleri ve sözleşmeden doğan yükümlülükleri içerebilir.* |  |
| 4.3*\** | 4.3 Bilgi güvenliği yönetim sisteminin kapsamının belirlenmesi  Kuruluş, kapsamını oluşturmak için bilgi güvenliği yönetim sisteminin sınırlarını ve uygulanabilirliğini belirlemiş midir?  Bu kapsamı belirlerken, kuruluş aşağıdakileri dikkate almış mıdır?  a) Madde 4.1'de atıfta bulunulan dış ve iç hususlar,  b) Madde 4.2'de atıfta bulunulan gereklilikler,  c) Kuruluş tarafından gerçekleştirilen faaliyetler ile diğer kuruluşlar tarafından gerçekleştirilen faaliyetler arasındaki arayüzler ve bağımlılıklar.  Kapsam, dokümante edilmiş bilgi olarak mevcut mudur? |  |
| 4.4 | 4.4 Bilgi güvenliği yönetim sistemi  Kuruluş, ISO/IEC 27001:2022 standardının gerekliliklerine uygun olarak, ihtiyaç duyulan prosesler ve etkileşimleri de dahil olmak üzere bir bilgi güvenliği yönetim sistemi kurmuş, uygulamakta, sürdürmekte ve sürekli olarak iyileştirmekte midir? |  |
| 5 5.1 | 5 Liderlik  5.1 Liderlik ve bağlılık  Üst yönetim, aşağıdakileri yaparak bilgi güvenliği yönetim sistemi ile ilgili olarak liderlik ve bağlılık göstermekte midir?  a) Bilgi güvenliği politikasının ve bilgi güvenliği hedeflerinin oluşturulmasını ve kuruluşun stratejik yönü ile uyumlu olmasının sağlaması,  b) Bilgi güvenliği yönetim sistemi gerekliliklerinin kuruluşun proseslerine entegrasyonunun sağlanması,  c) Bilgi güvenliği yönetim sistemi için ihtiyaç duyulan kaynakların mevcut olmasının sağlanması,  d) Etkili bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sistemi gerekliliklerine uygunluğun öneminin duyurulması,  e) Bilgi güvenliği yönetim sisteminin amaçlanan sonuca/çıktılara ulaşmasının sağlanması,  f) Bilgi güvenliği yönetim sisteminin etkinliğine katkıda bulunmaları için kişilerin yönlendirilmesi ve desteklenmesi,  g) Sürekli iyileştirmenin teşvik edilmesi ve  h) Sorumluluk alanları için geçerli olduğu şekliyle liderliklerini göstermek için diğer ilgili yönetim rollerinin desteklenmesi.  *NOT Bu dokümanda "iş"e yapılan atıf, geniş bir şekilde, kuruluşun varoluş amaçlarının temelini oluşturan faaliyetler anlamına gelecek şekilde yorumlanabilir.* |  |
| 5.2 | 5.2 Politika  Üst yönetim, aşağıdaki hususları sağlayan bir bilgi güvenliği politikası oluşturmuş mudur?  a) Kuruluşun amacına uygun,  b) Bilgi güvenliği hedeflerini içeren (Madde 6.2’ye bakınız) veya bilgi güvenliği hedeflerinin belirlenmesi için çerçeve sağlayan,  c) Bilgi güvenliği ile ilgili uygulanabilir gereklilikleri karşılama taahhüdünü içeren,  d) Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi taahhüdünü içeren.  Bilgi güvenliği politikası:  e) Dokümante edilmiş bilgi olarak mevcut olmalıdır,  f) Kuruluş içinde duyurulmuş mudur?  g) Uygun olduğu şekilde, ilgili tarafların erişimine açık mıdır? |  |
| 5.3 | 5.3 Kurumsal roller, sorumluluklar ve yetkiler  Üst yönetim, bilgi güvenliği ile ilgili roller için sorumlulukların ve yetkilerin atanmasını (belirlenmesini) ve kuruluş içinde duyurulmasını sağlamış mıdır?  Üst yönetim, aşağıdaki hususlar için sorumluluk ve yetki ataması yapmış mıdır?  a) Bilgi güvenliği yönetim sisteminin ISO/IEC 27001:2022 standardının gerekliliklerine uygunluğunu sağlamak,  b) Bilgi güvenliği yönetim sisteminin performansı hakkında üst yönetime raporlama yapmak.  *NOT Üst yönetim, kuruluş içindeki bilgi güvenliği yönetim sisteminin performansını raporlamak için sorumluluklar ve yetkiler de atayabilir.* |  |
| 6 6.1\* | 6 Planlama  6.1 Riskleri ve fırsatları ele almaya yönelik faaliyetler  6.1.1 Genel  Kuruluş, bilgi güvenliği yönetim sistemini planlarken, Madde 4.1'de atıfta bulunulan konuları ve Madde 4.2'de atıfta bulunulan gereklilikleri dikkate almış ve aşağıdaki konulara yönelik olarak ele alınması gereken riskleri ve fırsatları belirlemiş midir?  a) Bilgi güvenliği yönetim sisteminin amaçlanan sonuca/çıktılara ulaşabilmesini sağlamak,  b) İstenmeyen etkileri önlemek veya azaltmak,  c) Sürekli iyileştirme sağlamak.  Kuruluş aşağıdakileri planlamalıdır:  d) Bu riskleri ve fırsatları ele alacak faaliyetleri ve  e) Aşağıdaki hususların nasıl gerçekleştirileceğini  1) Faaliyetlerin bilgi güvenliği yönetim sistemi proseslerine entegre edilmesi ve uygulanması ve  2) Bu faaliyetlerin etkinliğinin değerlendirilmesini. |  |
|  | 6.1.2 Bilgi güvenliği risk değerlendirmesi  Kuruluş, aşağıdaki hususları sağlayan bir bilgi güvenliği risk değerlendirme prosesi tanımlamış ve uygulamakta mıdır?  a) Aşağıdakileri içeren bilgi güvenliği risk kriterlerini oluşturur ve sürdürür:  1) Risk kabul kriterleri ve  2) Bilgi güvenliği risk değerlendirmelerini gerçekleştirme kriterleri,  b) Tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesini sağlar,  c) Bilgi güvenliği risklerini tanımlar:  1) Bilgi güvenliği yönetim sistemi kapsamındaki bilgilerin gizlilik, bütünlük ve kullanılabilirlik kaybıyla ilişkili riskleri belirlemek için bilgi güvenliği risk değerlendirme prosesinin uygulanması ve  2) Risk sahiplerinin belirlenmesi,  d) Bilgi güvenliği risklerini analiz eder:  1) Madde 6.1.2 c) 1)'de tanımlanan risklerin gerçekleşmesi durumunda ortaya çıkacak potansiyel sonuçların değerlendirilmesi,  2) Madde 6.1.2 c) 1)'de tanımlanan risklerin gerçekleşme olasılığının gerçekçi olarak değerlendirilmesi ve  3) Risk seviyelerinin belirlenmesi,  e) Bilgi güvenliği risklerini aşağıdaki şekilde değerlendirir:  1) Risk analizinin sonuçlarının Madde 6.1.2 a)'da belirlenen risk kriterleri ile karşılaştırılması ve  2) Risk işleme için analiz edilen risklere öncelik verilmesi.  Kuruluş, bilgi güvenliği risk değerlendirme prosesi hakkında dokümante edilmiş bilgileri muhafaza etmekte midir? |  |
|  | 6.1.3 Bilgi güvenliği risk işleme  Kuruluş, aşağıdakiler için bir bilgi güvenliği risk işleme prosesi tanımlamalı ve uygulamakta mıdır?  a) Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk işleme seçeneklerini seçmek,  b) Seçilen bilgi güvenliği risk işleme seçeneğinin/seçeneklerinin uygulanması için gerekli olan tüm kontrolleri belirlemek,  *NOT 1 Kuruluşlar, kontrolleri gerektiği gibi tasarımlayabilir veya herhangi bir kaynaktan belirleyebilir.*  c) Yukarıdaki Madde 6.1.3 b)'de belirlenen kontrolleri Ek A'dakilerle karşılaştırmak ve gerekli kontrollerin hiçbirinin atlanmadığını doğrulamak,  *NOT 2 Ek A, olası bilgi güvenliği kontrollerinin bir listesini içerir. Bu dokümanın kullanıcıları, gerekli bilgi güvenliği kontrollerinin gözden kaçırılmadığından emin olmak için Ek A 'ya yönlendirilir.*  *NOT 3 Ek A'da listelenen bilgi güvenliği kontrolleri kapsamlı değildir ve gerekirse ilave bilgi güvenliği kontrolleri dahil edilebilir.*  d) Aşağıdakileri içeren bir Uygulanabilirlik Bildirgesi hazırlamak:  − Gerekli kontroller (Madde 6.1.3 b) ve c)’ye bakınız),  − Bunların dahil edilmesinin gerekçesi,  − Gerekli kontrollerin uygulanıp uygulanmadığı ve  − Ek A’da belirtilen kontrollerden herhangi birinin hariç tutulmasının gerekçesi.  e) Bir bilgi güvenliği risk işleme planı oluşturmak ve  f) Risk sahiplerinin bilgi güvenliği risk işleme planına ilişkin onayını ve artık bilgi güvenliği risklerinin kabulünü almak.  Kuruluş, bilgi güvenliği risk işleme prosesi hakkında dokümante edilmiş bilgileri muhafaza etmekte midir?  *NOT 4 Bu dokümandaki bilgi güvenliği risk değerlendirmesi ve risk işleme prosesi, ISO 31000'te sağlanan ilkeler ve genel kılavuz bilgilerle uyumludur.* |  |
| 6.2\* | 6.2 Bilgi güvenliği hedefleri ve bunlara ulaşmak için planlama  Kuruluş, ilgili fonksiyon ve seviyelerde bilgi güvenliği hedefleri oluşturmuş mudur?  Bilgi güvenliği hedefleri, aşağıdakileri sağlamakta mıdır?  a) Bilgi güvenliği politikası ile tutarlı olmalı,  b) Ölçülebilir olmalı (uygulanabilirse),  c) Geçerli bilgi güvenliği gerekliliklerini ve risk değerlendirmesi ve risk işleme sonuçlarını dikkate almalı,  d) İzlenmeli,  e) Duyurulmalı,  f) Uygun şekilde güncellenmeli,  g) Dokümante edilmiş bilgi olarak mevcut mudur?  Kuruluş, bilgi güvenliği hedefleri hakkında dokümante edilmiş bilgileri muhafaza etmekte midir?  Kuruluş bilgi güvenliği hedeflerine nasıl ulaşılacağını planlarken, aşağıdakileri belirlemiş midir?  h) Neyin yapılacağı,  i) Hangi kaynakların gerekli olacağı,  j) Kimin sorumlu olacağı,  k) Ne zaman tamamlanacağı ve  l) Sonuçların nasıl değerlendirileceği. |  |
| 6.3 | 6.3 Değişikliklerin planlanması  Kuruluş, bilgi güvenliği yönetim sisteminde değişiklik ihtiyacı belirlediğinde, değişiklikler planlı bir şekilde gerçekleştirilmekte midir? |  |
| 7 7.1 | 7 Destek  7.1 Kaynaklar  Kuruluş, bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için ihtiyaç duyulan kaynakları belirlemiş ve sağlamış mıdır? |  |
| 7.2 | 7.2 Yetkinlik  Kuruluş aşağıdakileri yapmış mıdır?  a) Bilgi güvenliği performansını etkileyen kendi kontrolü altında çalışan kişinin/kişilerin gerekli yetkinliğini belirlemeli,  b) Bu kişilerin uygun eğitim, öğretim veya deneyim temelinde yetkin olmalarını sağlamalı,  c) Uygun olduğu durumlarda, gerekli yetkinliği elde etmek için önlemler almalı ve alınan önlemlerin etkinliğini değerlendirmeli ve  d) Yetkinliğin kanıtı olarak uygun dokümante edilmiş bilgileri muhafaza etmekte midir?  *NOT Uygulanabilir faaliyetler aşağıdakileri içerebilir, örneğin: mevcut çalışanlara eğitim verilmesi, onlara rehberlik edilmesi veya görev değişikliği yapılması veya yetkili kişilerin işe alınması veya sözleşme yapılması.* |  |
| 7.3 | 7.3 Farkındalık  Kuruluşun kontrolü altında çalışan kişiler aşağıdaki hususların farkında olması sağlanmış mıdır?  a) Bilgi güvenliği politikası,  b) İyileştirilmiş bilgi güvenliği performansının faydaları da dahil olmak üzere, bilgi güvenliği yönetim sisteminin etkinliğine katkıları ve  c) Bilgi güvenliği yönetim sistemi gerekliliklerine uymamanın sonuçları. |  |
| 7.4 | 7.4 İletişim  Kuruluş, aşağıdakiler dahil olmak üzere bilgi güvenliği yönetim sistemi ile ilgili iç ve dış iletişim ihtiyacını belirlemiş midir?  a) Ne iletileceği,  b) Ne zaman iletişim kurulacağı,  c) Kiminle iletişim kurulacağı,  d) Nasıl iletişim kurulacağı. |  |
| 7.5\* | 7.5 Dokümante edilmiş bilgi  7.5.1 Genel  Kuruluşun bilgi güvenliği yönetim sistemi aşağıdakileri içermekte midir?  a) Bu dokümanın gerektirdiği dokümante edilmiş bilgiler ve  b) Bilgi güvenliği yönetim sisteminin etkinliği için gerekli olduğu kuruluş tarafından belirlenen dokümante edilmiş bilgiler.  *NOT Bilgi güvenliği yönetim sistemi için belgelenen bilgilerin kapsamı, aşağıda belirtilen hususlardan dolayı bir kuruluştan diğerine farklılık gösterebilir:*  *1) Kuruluşun büyüklüğü ve faaliyet, proses, ürün ve hizmet türleri,*  *2) Proseslerin ve etkileşimlerin karmaşıklığı ve*  *3) Kişilerin yetkinliği.*  7.5.2 Oluşturma ve güncelleme  Kuruluş, dokümante edilmiş bilgileri oluştururken ve güncellerken aşağıdakilerin uygunluğunu sağlamakta mıdır?  a) Tanımlama ve açıklama (örneğin; bir başlık, tarih, yazarı veya referans numarası),  b) Biçim (örneğin; dil, yazılım sürümü, grafikler) ve ortam (örneğin; kâğıt, elektronik) ve  c) Uygunluk ve yeterliliğin gözden geçirilmesi ve onaylanması.  7.5.3 Dokümante edilmiş bilgilerin kontrolü  Bilgi güvenliği yönetim sistemi ve ISO/IEC 27001:2022 standardın tarafından gerekli görülen dokümante edilmiş bilgiler, aşağıdaki hususları sağlamak için kontrol edilmelidir:  a) İhtiyaç duyulan yerde ve zamanda kullanıma hazır ve kullanıma uygun olması ve  b) Yeterince korunması (örneğin; gizlilik kaybı, uygun olmayan kullanım veya bütünlük kaybından).  Dokümante edilmiş bilgilerin kontrolü için kuruluş, uygulanabilir olduğu şekilde aşağıdaki faaliyetleri ele almalıdır:  c) Dağıtım, erişim, getirme ve kullanım,  d) Okunabilirliğin korunması da dahil olmak üzere depolama ve muhafaza,  e) Değişikliklerin kontrolü (örneğin, sürüm kontrolü) ve  f) Muhafaza etme ve yok etme.  Bilgi güvenliği yönetim sisteminin planlanması ve işletilmesi için kuruluş tarafından gerekli olduğu belirlenen dış kaynaklı dokümante edilmiş bilgi, uygun şekilde tanımlanmış ve kontrol edilmekte midir?  *NOT Erişim, yalnızca dokümante edilmiş bilgileri görüntüleme izni veya dokümante edilmiş bilgileri görüntüleme ve değiştirme izni ve yetkisi vb. ile ilgili bir karar anlamına gelebilir.* |  |
| 8 8.1\* | 8 Operasyon  8.1 Operasyon ile ilgili planlama ve kontrol  Kuruluş, gereklilikleri karşılamak ve Madde 6'da belirlenen faaliyetleri uygulamak için gereken prosesleri aşağıdakileri yaparak planlamış, uygulamakta ve kontrol etmekte midir?  − Prosesler için kriterler oluşturulması,  − Kriterlere uygun olarak proseslerin kontrolünün uygulanması.  Dokümante edilmiş bilgi, proseslerin planlandığı gibi yürütüldüğünden emin olunması için gerekli olduğu ölçüde mevcut mudur?  Kuruluş, planlanan değişiklikleri kontrol etmekte ve istenmeyen değişikliklerin sonuçlarını gözden geçirmekte ve gerektiğinde herhangi bir olumsuz etkiyi azaltmak için önlem almakta mıdır?  Kuruluş, bilgi güvenliği yönetim sistemi ile ilgili, dışarıdan sağlanan proseslerin, ürünlerin veya hizmetlerin kontrol edilmesini sağlamakta mıdır? |  |
| 8.2 | 8.2 Bilgi güvenliği risk değerlendirmesi  Kuruluş, Madde 6.1.2 a)'da belirlenen kriterleri dikkate alarak, planlanan aralıklarla veya önemli değişiklikler önerildiğinde veya meydana geldiğinde bilgi güvenliği risk değerlendirmeleri gerçekleştirmekte midir?  Kuruluş, bilgi güvenliği risk değerlendirmelerinin sonuçlarına ilişkin dokümante edilmiş bilgileri muhafaza etmekte midir? |  |
| 8.3 | 8.3 Bilgi güvenliği risk işleme  Kuruluş, bilgi güvenliği risk işleme planını uygulamakta mıdır?  Kuruluş, bilgi güvenliği risk işlemenin sonuçlarına ilişkin dokümante edilmiş bilgileri muhafaza etmekte midir? |  |
| 9 9.1 | 9 Performans değerlendirmesi  9.1 İzleme, ölçme, analiz ve değerlendirme  Kuruluş aşağıdaki hususları belirlemiş midir?  a) Bilgi güvenliği prosesleri ve kontrolleri dahil olmak üzere neyin izlenmesi ve ölçülmesi gerektiğini,  b) Geçerli sonuçları sağlamak için, uygun olduğu şekilde, izleme, ölçme, analiz ve değerlendirme yöntemlerini. Seçilen yöntemlerin geçerli sayılabilmesi için karşılaştırılabilir ve tekrarlanabilir sonuçlar vermesi gerekir,  c) İzleme ve ölçümün ne zaman yapılacağını,  d) Kimin izleyeceği ve ölçeceğini,  e) İzleme ve ölçüm sonuçlarının ne zaman analiz edileceği ve değerlendirileceğini,  f) Bu sonuçları kimin analiz edeceği ve değerlendireceği.  Dokümante edilmiş bilgi, sonuçların kanıtı olarak mevcut mudur?  Kuruluş, bilgi güvenliği performansını ve bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmekte midir? |  |
| 9.2\* | 9.2 İç denetim  9.2.1 Genel  Kuruluş, bilgi güvenliği yönetim sisteminin, aşağıdaki hususları yerine getirip getirmediğine dair bilgi sağlamak amacıyla planlanan aralıklarda iç denetimini gerçekleştirmekte midir?  a) Aşağıdaki hususlara uyumlu olup olmadığı:  1) Kuruluşun bilgi güvenliği yönetim sistemi için kendi gerekliliklerine,  2) Bu dokümanın gerekliliklerine,  b) Etkin bir şekilde uygulanmakta ve sürdürülmekte olduğu.  9.2.2 İç denetim programı  Kuruluş; sıklık, yöntemler, sorumluluklar, planlama gereklilikleri ve raporlama dahil olmak üzere denetim programı/programları planlamış, oluşturmuş, uygulamakta ve sürdürmekte midir?  Kuruluş, iç denetim programını/programlarını oluştururken, ilgili proseslerin önemini ve önceki denetimlerin sonuçlarını dikkate almış mıdır?  Kuruluş aşağıdakileri gerçekleştirilmekte midir?  a) Her denetim için denetim kriterlerini ve kapsamını tanımlamalı,  b) Tetkik prosesinin objektifliğini ve tarafsızlığını sağlayan denetçileri seçmeli ve denetimler yapmalı,  c) Tetkik sonuçlarının ilgili yönetime rapor edilmesini sağlamış mıdır?  Tetkik programının/programlarının uygulanmasının ve denetim sonuçlarının kanıtı olarak dokümante edilmiş bilgi mevcut mudur? |  |
| 9.3\* 9.3.1 | 9.3 Yönetimin gözden geçirmesi  9.3.1 Genel  Üst yönetim, sürekli uygunluğunu, yeterliliğini ve etkinliğini sağlamak için kuruluşun bilgi güvenliği yönetim sistemini planlanan aralıklarla gözden geçirmekte midir?  9.3.2 Yönetim gözden geçirme girdileri  Yönetimin gözden geçirmesi, aşağıdaki hususların dikkate alınmasını içermekte midir?  a) Önceki yönetim gözden geçirmelerinde karar alınan faaliyetlerin durumu,  b) Bilgi güvenliği yönetim sistemi ile ilgili dış ve iç konulardaki değişiklikler,  c) Bilgi güvenliği yönetim sistemi ile ilgili olarak ilgili tarafların ihtiyaç ve beklentilerindeki değişiklikler,  d) Aşağıdaki hususlardaki eğilimler dahil olmak üzere bilgi güvenliği performansı hakkında geri bildirim:  1) Uygunsuzluklar ve düzeltici faaliyetler,  2) İzleme ve ölçme sonuçları,  3) Tetkik sonuçları,  4) Bilgi güvenliği hedeflerinin yerine getirilmesi,  e) İlgili taraflardan geri bildirim,  f) Risk değerlendirmesinin sonuçları ve risk işleme planının durumu,  g) Sürekli iyileştirme fırsatları.  9.3.3 Yönetim gözden geçirme sonuçları  Yönetimin gözden geçirmesinin sonuçları, sürekli iyileştirme fırsatlarıyla ilgili kararları ve bilgi güvenliği yönetim sistemindeki tüm değişiklik ihtiyaçlarını içermekte midir?  Dokümante edilmiş bilgiler, yönetimin gözden geçirmelerinin sonuçlarının kanıtı olarak mevcut mudur? |  |
| 10\* 10.1 | 10 İyileştirme  10.1 Sürekli iyileştirme  Kuruluş, bilgi güvenliği yönetim sisteminin uygunluğunu, yeterliliğini ve etkinliğini sürekli iyileştirmekte midir? |  |
| 10.2 | 10.2 Uygunsuzluk ve düzeltici faaliyet  Bir uygunsuzluk oluştuğunda, kuruluş:  a) Uygunsuzluğa tepki vermekte ve uygulanabilirse:  1) Kontrol altına almak ve düzeltmek için faaliyete geçmekte,  2) Sonuçlarıyla ilgilenmekte,  b) Uygunsuzluğun tekrar etmemesi veya başka bir yerde meydana gelmemesi için aşağıdaki hususları yaparak uygunsuzluğun nedenlerini ortadan kaldıracak faaliyet ihtiyacını değerlendirmekte:  1) Uygunsuzluğu gözden geçirerek,  2) Uygunsuzluğun nedenlerini belirleyerek ve  3) Benzer uygunsuzlukların mevcut olup olmadığının veya potansiyel olarak ortaya çıkıp çıkamayacağını belirleyerek,  c) Gereken herhangi bir faaliyeti uygulamakta,  d) Alınan herhangi bir düzeltici faaliyetin etkinliğini gözden geçirmekte ve  e) Gerektiğinde bilgi güvenliği yönetim sisteminde değişiklikler yapmakta mıdır?  Düzeltici faaliyetler karşılaşılan uygunsuzlukların etkilerine uygun olması sağlanmış mıdır?  Dokümante edilmiş bilgi, aşağıdakilerin kanıtı olarak mevcut mudur?  f) Uygunsuzlukların niteliği ve alınan müteakip önlemler,  g) Herhangi bir düzeltici faaliyetin sonuçları. |  |

| ISO/IEC 27001:2022 - Bilgi Güvenliği Kontrolleri | | | |
| --- | --- | --- | --- |
| Gereklilikler | | | Bulgular |
| 5 | Kurumsal kontroller | | |
| 5.1 | Bilgi güvenliği politikaları | Bilgi güvenliği politikası ve konuya özgü politikalar tanımlanmalı, yönetim tarafından onaylanmalı, yayımlanmalı, ilgili personele ve ilgili taraflara iletilmeli ve onlar tarafından onaylanmalı ve planlı aralıklarla ve önemli değişiklikler olması durumunda gözden geçirilmelidir. |  |
| 5.2 | Bilgi güvenliği rolleri ve sorumlulukları | Bilgi güvenliği rolleri ve sorumlulukları, kuruluşun ihtiyaçlarına göre tanımlanmalı ve dağıtılmalıdır. |  |
| 5.3 | Görevlerin ayrılığı | Çakışan görevler ve çatışan sorumluluk alanları birbirinden ayrılmalıdır. |  |
| 5.4 | Yönetim sorumlulukları | Yönetim, tüm personelinin bilgi güvenliğini kuruluşun oluşturulmuş bilgi güvenliği politikasına, konuya özgü politika ve prosedürlerine uygun olarak uygulamasını zorunlu tutmalıdır. |  |
| 5.5 | Yetkililerle iletişim | Kuruluş, ilgili makamlarla iletişim kurmalı ve sürdürmelidir. |  |
| 5.6 | Özel ilgi gruplarıyla iletişim | Kuruluş, özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel derneklerle iletişim kurmalı ve sürdürmelidir. |  |
| 5.7 | Tehdit istihbaratı | Bilgi güvenliği tehditlerine ilişkin bilgiler, tehdit istihbaratı oluşturmak için toplanmalı ve analiz edilmelidir. |  |
| 5.8 | Proje yönetiminde bilgi güvenliği | Bilgi güvenliği proje yönetimine entegre edilmelidir. |  |
| 5.9 | Bilgi envanteri ve diğer ilgili varlıklar | Sahipler de dahil olmak üzere bilgi ve diğer ilgili varlıkların bir envanteri geliştirilmeli ve sürdürülmelidir. |  |
| 5.10 | Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı | Bilgilerin ve diğer ilgili varlıkların işlenmesine yönelik kabul edilebilir kullanım kuralları ve prosedürler tanımlanmalı, dokümante edilmeli ve uygulanmalıdır. |  |
| 5.11 | Varlıkların iadesi | Personel ve diğer ilgili taraflar, istihdamlarının, sözleşmelerinin veya anlaşmalarının değiştirilmesi veya feshedilmesi üzerine ellerinde bulunan tüm kurumsal varlıkları uygun şekilde iade etmelidir. |  |
| 5.12 | Bilgilerin sınıflandırılması | Bilgiler; gizlilik, bütünlük, kullanılabilirlik ve bağıntılı ilgili taraf gerekliliklerine dayalı olarak kuruluşun bilgi güvenliği ihtiyaçlarına göre sınıflandırılmalıdır. |  |
| 5.13 | Bilgilerin etiketlenmesi | Bilgi etiketleme için uygun bir dizi prosedür geliştirilmeli ve kuruluş tarafından benimsenen bilgi sınıflandırma şemasına göre uygulanmalıdır. |  |
| 5.14 | Bilgi transferi | Kuruluş içindeki ve kuruluş ile diğer taraflar arasındaki her tip aktarım tesisi için bilgi aktarım kuralları, prosedürleri veya anlaşmaları yürürlükte olmalıdır. |  |
| 5.15 | Erişim kontrolu | Bilgiye ve diğer ilgili varlıklara fiziksel ve mantıksal erişimi kontrol etmeye yönelik kurallar, iş ve bilgi güvenliği gereksinimlerine dayalı olarak oluşturulmalı ve uygulanmalıdır. |  |
| 5.16 | Kimlik yönetimi | Kimliklerin tüm yaşam döngüsü yönetilmelidir. |  |
| 5.17 | Kimlik doğrulama bilgileri | Kimlik doğrulama bilgilerinin tahsisi ve yönetimi, personele kimlik doğrulama bilgilerinin uygun şekilde kullanılması konusunda tavsiye verilmesi de dahil olmak üzere bir yönetim prosesi tarafından kontrol edilmelidir. |  |
| 5.18 | Erişim hakları | Bilgiye ve diğer ilişkili varlıklara erişim hakları, kuruluşun erişim kontrolüne ilişkin konuya özgü politikasına ve kurallarına uygun olarak sağlanmalı, gözden geçirilmeli, değiştirilmeli ve kaldırılmalıdır. |  |
| 5.19 | Tedarikçi ilişkilerinde bilgi güvenliği | Tedarikçinin ürün veya hizmetlerinin kullanımıyla ilgili bilgi güvenliği risklerini yönetmek için prosesler ve prosedürler tanımlanmalı ve uygulanmalıdır. |  |
| 5.20 | Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması | İlgili bilgi güvenliği gereklilikleri, tedarikçi ilişkisinin tipine dayandırılarak her tedarikçi ile oluşturulmalı ve üzerinde anlaşmaya varılmalıdır. |  |
| 5.21 | Bilgi ve iletişim teknolojisi (BİT) tedarik zincirinde bilgi güvenliğini yönetme | BİT ürünleri ve hizmetleri tedarik zinciri ile ilişkili bilgi güvenliği risklerini yönetmek için prosesler ve prosedürler tanımlanmalı ve uygulanmalıdır. |  |
| 5.22 | Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişiklik yönetimi | Kuruluş, tedarikçi bilgi güvenliği uygulamaları ve hizmet sunumundaki değişiklikleri düzenli olarak izlemeli, gözden geçirmeli, değerlendirmeli ve yönetmelidir. |  |
| 5.23 | Bulut hizmetlerinin kullanımı için bilgi güvenliği | Bulut hizmetlerinin edinilmesi, kullanılması, yönetimi ve bulut hizmetlerinden çıkış prosesleri, kuruluşun bilgi güvenliği gerekliliklerine uygun olarak oluşturulmalıdır. |  |
| 5.24 | Bilgi güvenliği ihlal olayı yönetimi planlaması ve hazırlığı | Kuruluş, bilgi güvenliği ihlal olayı yönetimi proseslerini, rollerini ve sorumluluklarını tanımlayarak, oluşturarak ve ileterek bilgi güvenliği ihlal olaylarını yönetmeyi planlamalı ve hazırlamalıdır. |  |
| 5.25 | Bilgi güvenliği ihlal olaylarını değerlendirme ve karar verme | Kuruluş, bilgi güvenliği olaylarını değerlendirmeli ve bunların bilgi güvenliği ihlal olayları olarak kategorize edilip edilmeyeceğine karar vermelidir. |  |
| 5.26 | Bilgi güvenliği ihlal olaylarına yanıt verme | Bilgi güvenliği ihlal olaylarına, dokümante edilmiş prosedürlere uygun olarak yanıt verilmelidir. |  |
| 5.27 | Bilgi güvenliği ihlal olaylarından ders çıkarma | Bilgi güvenliği ihlal olaylarından elde edilen bilgiler, bilgi güvenliği kontrollerini güçlendirmek ve iyileştirmek amacıyla kullanılmalıdır. |  |
| 5.28 | Kanıt toplama | Kuruluş, bilgi güvenliği olaylarıyla ilgili kanıtların tanımlanması, toplanması, elde edilmesi ve korunması için prosedürler oluşturmalı ve uygulamakta mıdır? |  |
| 5.29 | Kesinti sırasında bilgi güvenliği | Kuruluş, kesinti sırasında bilgi güvenliğini uygun bir seviyede nasıl sürdüreceğini planlamalıdır. |  |
| 5.30 | İş sürekliliği için BİT hazırlığı | Kontrol  BİT hazırlığı, iş sürekliliği hedefleri ve BİT sürekliliği gereklilikleri temelinde planlanmalı, uygulanmalı, sürdürülmeli ve test edilmelidir. |  |
| 5.31 | Yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler | Bilgi güvenliği ile ilgili yasal, meşru, düzenleyici ve sözleşmeye tabi gereklilikler ve kuruluşun bu gereklilikleri karşılama yaklaşımı belirlenmeli, dokümante edilmeli ve güncel tutulmalıdır. |  |
| 5.32 | Fikri Mülkiyet Hakları | Kuruluş, fikri mülkiyet haklarını korumak için uygun prosedürleri uygulamakta mıdır? |  |
| 5.33 | Kayıtların korunması | Kayıtlar kayıp olma, tahrif edilme, sahtesini yapma, yetkisiz erişim ve yetkisiz yayıma karşı korunmalıdır. |  |
| 5.34 | Kişiyi tespit bilgisinin (PII) gizliliği ve korunması | Kuruluş, yürürlükteki yasalara ve düzenlemelere ve sözleşme Gerekliliklerine göre gizliliğin korunmasına ve PII'nin korunmasına ilişkin gereklilikleri belirlemeli ve karşılamalıdır. |  |
| 5.35 | Bilgi güvenliğinin bağımsız gözden geçirilmesi | İnsanlar, prosesler ve teknolojiler dahil olmak üzere Kuruluşun bilgi güvenliğini yönetme yaklaşımı ve uygulanması, planlanan aralıklarla veya önemli değişiklikler meydana geldiğinde bağımsız olarak gözden geçirilmelidir. |  |
| 5.36 | Bilgi güvenliğine yönelik politikalar, kurallar ve standartlara uygunluk | Kurumun bilgi güvenliği politikasına, konuya özgü politikalarına, kurallarına ve standartlarına uyum düzenli olarak gözden geçirilmelidir. |  |
| 5.37 | Dokümante edilmiş işletim prosedürleri | Bilgi işleme imkanları için işletim prosedürleri doküman haline getirilmeli ve bunlara ihtiyaç duyan personele sağlanmalıdır. |  |
| 6 | Kişi kontrolleri | | |
| 6.1 | Tarama | Tüm personel adaylarına dair geçmiş doğrulama kontrolleri, kuruluşa katılmadan önce ve sürekli olarak yürürlükteki kanunlar, yönetmelikler ve etik değerler dikkate alınarak yapılmalı ve işin gereklilikleri, erişilecek bilgilerin sınıflandırılmasına ve algılanan risklere orantılı olmalıdır. |  |
| 6.2 | İstihdam hüküm ve koşulları | İş akdi sözleşmelerinde, personelin ve kuruluşun bilgi güvenliğine ilişkin sorumlulukları belirtilmelidir. |  |
| 6.3 | Bilgi güvenliği farkındalığı, eğitim ve öğretim | Kuruluşun personeli ve bağıntılı ilgili taraflar, iş fonksiyonlarıyla ilgili olarak, uygun bilgi güvenliği farkındalığı, eğitim ve öğretim ve kuruluşun bilgi güvenliği politikası, konuya özgü politikalar ve prosedürler hakkında düzenli güncellemeler almalıdır. |  |
| 6.4 | Disiplin prosesi | Bilgi güvenliği politikası ihlali gerçekleştiren personele ve diğer bağıntılı ilgili taraflara karşı işlem yapılması için bir disiplin prosesi resmileştirilmeli ve iletilmelidir. |  |
| 6.5 | İstihdamın sona ermesinden veya değiştirilmesinden sonraki sorumluluklar | İstihdamın sona ermesinden veya değiştirilmesinden sonra geçerli olan bilgi güvenliği sorumlulukları ve görevleri tanımlanmalı, yürürlüğe konulmalı ve ilgili personele ve diğer ilgili taraflara iletilmelidir. |  |
| 6.6 | Gizlilik veya ifşa etmeme anlaşmaları | Kuruluşun bilgilerin korunmasına yönelik ihtiyaçlarını yansıtan gizlilik veya ifşa etmeme anlaşmaları personel ve diğer bağıntılı taraflarca tanımlanmalı, doküman haline getirilmeli, düzenli olarak gözden geçirilmeli ve imzalanmalıdır. |  |
| 6.7 | Uzaktan çalışma | Personel, uzaktan çalışırken kuruluşun tesisleri dışında erişilen, işlenen veya depolanan bilgileri korumak için güvenlik önlemleri uygulanmalıdır. |  |
| 6.8 | Bilgi güvenliği olayı raporlanması | Kuruluş, personelin gözlemlenen veya şüphelenilen bilgi güvenliği olaylarını uygun kanallar aracılığıyla zamanında raporlaması için bir mekanizma sağlamış mıdır? |  |
| 7 | Fiziksel kontroller | | |
| 7.1 | Fiziksel güvenlik sınırları | Bilgi ve diğer ilişkili varlıkları içeren alanları korumak için güvenlik sınırları tanımlanmalı ve kullanılmalıdır. |  |
| 7.2 | Fiziksel giriş | Güvenli alanlar, uygun giriş kontrolleri ve erişim noktaları ile korunmalıdır. |  |
| 7.3 | Ofislerin, odaların ve tesislerin güvenliğini sağlama | Ofisler, odalar ve tesisler için fiziksel güvenlik tasarımlanmalı ve uygulanmalıdır. |  |
| 7.4 | Fiziksel güvenlik izleme | Tesisler yetkisiz fiziksel erişime karşı sürekli olarak izlenmelidir. |  |
| 7.5 | Fiziksel ve çevresel tehditlere karşı koruma | Doğal afetler ve altyapıya yönelik diğer kasıtlı veya kasıtsız fiziksel tehditler gibi fiziksel ve çevresel tehditlere karşı koruma tasarımlanmalı ve uygulanmalıdır. |  |
| 7.6 | Güvenli alanlarda çalışma | Güvenli alanlarda çalışmaya yönelik güvenlik önlemleri tasarımlanmalı ve uygulanmalıdır. |  |
| 7.7 | Temiz masa ve temiz ekran | Kağıtlar ve çıkarılabilir depolama ortamları için temiz masa kuralları ve bilgi işleme tesisleri için temiz ekran kuralları tanımlanmalı ve uygun şekilde uygulanmalıdır. |  |
| 7.8 | Ekipman konumlandırma ve koruma | Ekipman güvenli bir şekilde yerleştirilmeli ve korunmalıdır. |  |
| 7.9 | Kuruluş dışındaki varlıkların güvenliği | Kuruluş dışındaki varlıklar korunmalıdır. |  |
| 7.10 | Depolama ortamı | Depolama ortamları, kuruluşun sınıflandırma şemasına ve taşıma gerekliliklerine uygun olarak edinme, kullanma, taşıma ve yok edilme yaşam döngüleri boyunca yönetilmelidir. |  |
| 7.11 | Destekleyici altyapı hizmetleri | Bilgi işleme tesisleri, destekleyici altyapı hizmetlerindeki arızalardan kaynaklanan elektrik kesintilerinden ve diğer kesintilerden korunmalıdır. |  |
| 7.12 | Kablo güvenliği | Güç, veri veya destekleyici bilgi servislerini taşıyan kablolar, dinleme, girişim veya hasara karşı korunmalıdır. |  |
| 7.13 | Ekipman bakımı | Bilginin kullanılabilirliğini (yararlanabilirliğini), bütünlüğünü ve gizliliğini sağlamak için ekipman bakımı doğru bir şekilde yapılmalıdır. |  |
| 7.14 | Ekipmanın güvenli bir şekilde yok edilmesi veya tekrar kullanılması | Depolama ortamı içeren ekipman öğeleri, tüm hassas verilerin ve lisanslı yazılımların yok edilmeden veya tekrar kullanılmadan önce kaldırıldığından veya güvenli bir şekilde üzerine yazıldığından emin olmak için doğrulanmalıdır. |  |
| 8 | Teknolojik kontroller | | |
| 8.1 | Kullanıcı uç nokta cihazları | Kullanıcı uç nokta cihazlarında depolanan, bunlar tarafından işlenen veya bunlar aracılığıyla erişilen bilgiler korunmalıdır. |  |
| 8.2 | Ayrıcalıklı erişim hakları | Ayrıcalıklı erişim haklarının tahsisi ve kullanımı sınırlandırılmalı ve yönetilmelidir. |  |
| 8.3 | Bilgi erişim kısıtlaması | Bilgilere ve diğer ilgili varlıklara erişim, erişim kontrolü konusunda oluşturulmuş konuya özgü politikaya uygun olarak kısıtlanmalıdır. |  |
| 8.4 | Kaynak koduna erişim | Kaynak koduna, geliştirme araçlarına ve yazılım kütüphanelerine okuma ve yazma erişimi uygun şekilde yönetilmelidir. |  |
| 8.5 | Güvenli kimlik doğrulama | Güvenli kimlik doğrulama teknolojileri ve prosedürleri, bilgi erişim kısıtlamalarına ve erişim kontrolüne ilişkin konuya özgü politikaya dayalı olarak uygulanmalıdır. |  |
| 8.6 | Kapasite yönetimi | Kaynakların kullanımı izlenmeli ve mevcut ve beklenen kapasite gereklilikleri doğrultusunda ayarlanmalıdır. |  |
| 8.7 | Kötü amaçlı yazılıma karşı koruma | Kötü amaçlı yazılıma karşı koruma uygulanmalı ve uygun kullanıcı farkındalığı ile desteklenmelidir. |  |
| 8.8 | Teknik açıklıkların yönetimi | Kullanımda olan bilgi sistemlerinin teknik açıklıkları hakkında bilgi edinilmeli, kuruluşun bu açıklara maruz kalma durumu değerlendirilmeli ve uygun önlemler alınmalıdır. |  |
| 8.9 | Konfigürasyon  (yapılandırma) yönetimi | Donanım, yazılım, hizmetler ve ağların güvenlik yapılandırmaları da dahil olmak üzere yapılandırmaları oluşturulmalı, doküman haline getirilmeli, uygulanmalı, izlenmeli ve gözden geçirilmelidir. |  |
| 8.10 | Bilgi silme | Bilgi sistemlerinde, cihazlarda veya diğer herhangi bir depolama ortamında saklanan bilgiler, artık gerekli olmadığında silinmelidir. |  |
| 8.11 | Veri maskeleme | Veri maskeleme, ilgili mevzuat dikkate alınarak, kuruluşun konuya özgü erişim kontrolü politikası ve ilgili diğer konuya özgü politikalara ve iş gerekliliklerine uygun olarak kullanılmalıdır. |  |
| 8.12 | Veri sızıntısı önleme | Hassas bilgileri işleyen, depolayan veya ileten sistemlere, ağlara ve diğer tüm cihazlara veri sızıntısı önleme önlemleri uygulanmalıdır. |  |
| 8.13 | Bilgi yedekleme | Bilgilerin, yazılımların ve sistemlerin yedek kopyaları muhafaza edilmeli ve üzerinde anlaşmaya varılan konuya özgü yedekleme politikasına uygun olarak düzenli bir şekilde test edilmelidir. |  |
| 8.14 | Bilgi işleme tesislerinin yedek fazlalığı | Bilgi işleme imkanlarında, kullanılabilirlik gerekliliklerini karşılamak için yeterli miktarda yedekleme sağlanmalıdır. |  |
| 8.15 | Kaydetme (Log tutma) | Faaliyetleri, istisnaları, hataları ve diğer ilgili olayları kaydeden kayıtlar (loglar) üretilmeli, depolanmalı, korunmalı ve analiz edilmelidir. |  |
| 8.16 | İzleme faaliyetleri | Ağlar, sistemler ve uygulamalar anomali içeren davranışlara karşı izlenmeli ve potansiyel bilgi güvenliği ihlal olaylarını değerlendirmek için uygun önlemler alınmalıdır. |  |
| 8.17 | Saat senkronizasyonu | Kuruluş tarafından kullanılan bilgi işlem sistemlerinin saatleri, onaylanmış zaman kaynaklarına senkronize edilmelidir. |  |
| 8.18 | Ayrıcalıklı destek programların kullanımı | Sistem ve uygulama kontrollerini geçersiz kılabilecek destek programların kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir. |  |
| 8.19 | Operasyon sistemlerine yazılım kurulumu | Operasyon sistemlerinde yazılım kurulumunu güvenli bir şekilde yönetmek için prosedürler ve önlemler uygulanmalıdır. |  |
| 8.20 | Ağ güvenliği | Sistemlerdeki ve uygulamalardaki bilgileri korumak için ağlar ve ağ cihazları güvenlik altına alınmalı, yönetilmeli ve kontrol edilmekte midir? |  |
| 8.21 | Ağ hizmetlerinin güvenliği | Ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve hizmet gereklilikleri belirlenmeli, uygulanmalı ve izlenmelidir. |  |
| 8.22 | Ağların ayrımı | Kuruluş ağlarında bilgi hizmetleri grupları, kullanıcılar ve bilgi sistemleri ayrılmalıdır. |  |
| 8.23 | Web filtreleme | Harici web sitelerine erişim, kötü amaçlı içeriğe maruz kalmayı azaltacak şekilde yönetilmelidir. |  |
| 8.24 | Kriptografi (şifreleme) kullanımı | Kriptografik anahtar yönetimi de dahil olmak üzere kriptografinin etkin kullanımına yönelik kurallar tanımlanmalı ve uygulanmalıdır. |  |
| 8.25 | Güvenli geliştirme yaşam döngüsü | Yazılım ve sistemlerin güvenli bir şekilde geliştirilmesi için kurallar oluşturulmalı ve uygulanmalıdır. |  |
| 8.26 | Uygulama güvenlik gereklilikleri | Uygulamalar geliştirilirken veya edinilirken bilgi güvenliği gereklilikleri; tanımlanmalı, belirtilmeli ve onaylanmalıdır. |  |
| 8.27 | Güvenli sistem mimarisi ve mühendislik ilkeleri | Güvenli sistemlerin mühendisliğine yönelik ilkeler oluşturulmalı, dokümante edilmeli, sürdürülmeli ve herhangi bir bilgi sistemi geliştirme faaliyetine uygulanmalıdır. |  |
| 8.28 | Güvenli kodlama | Güvenli kodlama ilkeleri yazılım geliştirmeye uygulanmalıdır. |  |
| 8.29 | Geliştirme ve kabul aşamasında güvenlik testleri | Güvenlik test prosesleri, geliştirme yaşam döngüsünde tanımlanmalı ve uygulanmalıdır. |  |
| 8.30 | Dış kaynak yoluyla geliştirme | Kuruluş, dış kaynak yoluyla sistem geliştirme ile ilgili faaliyetleri yönetmeli, izlemeli ve gözden geçirmelidir. |  |
| 8.31 | Geliştirme, test ve canlı (gerçek) ortamlarının ayrılması | Geliştirme, test ve canlı ortamlar birbirinden ayrılmalı ve güvenlik altına alınmalıdır. |  |
| 8.32 | Değişiklik yönetimi | Bilgi işleme tesisleri ve bilgi sistemlerindeki değişiklikler, değişiklik yönetimi prosedürlerine tabi olmalıdır. |  |
| 8.33 | Test bilgisi | Test bilgileri uygun şekilde seçilmeli, korunmalı ve yönetilmelidir. |  |
| 8.34 | Tetkik testi sırasında bilgi istemlerinin korunması | Operasyon sistemlerin değerlendirilmesini içeren denetim testleri ve diğer güvence faaliyetleri, test uzmanı ve uygun yönetim arasında planlanmalı ve kararlaştırılmalıdır. |  |