



İSTANBUL
GELİŞİM
ÜNİVERSİTESİ

İSTANBUL GELİŞİM ÜNİVERSİTESİ
İSTANBUL GELİŞİM MESLEK YÜKSEKOKULU
BİLGİSAYAR TEKNOLOJİLERİ BÖLÜMÜ
BİLİŞİM GÜVENLİĞİ TEKNOLOJİSİ PROGRAMI

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi

FİNAL PROJE ÖDEVİ

HAZIRLAYANLAR

220175109-MERT CAN KIZILDAĞ

220175059- EMİRHAN KAYA

ÖDEV DANIŞMANI

ÖĞR. GÖR. TUĞBA SARAY ÇETİNKAYA

İSTANBUL - 2024

ÖDEV TANITIM FORMU

HAZIRLAYANLAR- EMİRHAN KAYA, MERT CAN KIZILDAĞ

ÖDEV DİLİ- TÜRKÇE

ÖDEV ADI- ISO/IEC 27001 Bilgi güvenliği yönetim sistemi

BÖLÜM- BİLGİSAYAR TEKNOLOJİLERİ

PROGRAM- BİLİŞİM GÜVENLİĞİ TEKNOLOJİSİ

PROJE TÜRÜ- FİNAL PROJESİ

PROJE TESLİM TARİHİ- 10.05.2024

SAYFA SAYISI-30

ÖDEV DANIŞMANI- ÖĞR. GÖR. TUĞBA SARAY ÇETİNKAYA

BEYAN

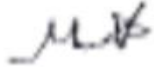
Bu ödevin/projenin hazırlanmasında bilimsel ahlak kurallarına uyulduğu, başkalarının ederlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğu, kullanılan verilerde herhangi tahrifat yapılmadığını, ödevin/projenin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir ödev/proje olarak sunulmadığını beyan eder, aksi durumda karşılaşacağım cezai ve/veya hukuki durumu kabul eder; ayrıca üniversitenin ilgili yasa, yönerge ve metinlerini okuduğumu beyan ederim.

Tarih
10.05.2024

Adı Soyadı

İmza

Mert Can Kızıldağ



Emirhan Kaya



KABUL VE ONAY SAYFASI

220175059 numaralı Emirhan KAYA'nın , 220175109 numaralı Mert Can KIZILDAĞ'ın BİLGİ VE AĞ GÜVENLİĞİ PROJESİ adlı çalışması benim tarafımdan Vize/Ders içi/Final ödevi olarak kabul edilmiştir.

TUĞBA SARAY ÇETİNKAYA

ÖĞRETİM GÖREVLİSİ

ÖZET

Ödevimizin hazırlanması sürecinde karşılaştığımız zorluklarla birlikte, bu projenin hayata geçirilmesine katkı sağlayan Mert Can KIZILDAĞ'a ve Emirhan KAYA'ya teşekkürlerimizi sunarız.

Yazarlar

Mert Can KIZILDAĞ

Emirhan KAYA

İçindekiler

Ödev Tanıtım Formu.....	2
Beyan.....	3
Kabul ve Onay Sayfası.....	4
Özet.....	5
İçindekiler.....	6
Ön Söz.....	7

Birinci Bölüm

1.1 ISO 27001 belgesi nedir? Bu belgeyi almak için neler gerekir?.....	9
1.2.Peki neden bilgi güvenliğinde ISO 27001 belgesini bu kadar önemli?.....	10-12

İkinci Bölüm

2.1 Proje Senaryo	13
2.2. Varlık Envanteri.....	14-15
2.3 Risk Kütüğü.....	16-19
2.3.1 Risk Kütüğü Görselleri.....	20-21
2.4 ISO 27001 Uygulanabilirlik Bildirgesi Göstergesi.....	22-29
Kaynakça.....	30

ÖN SÖZ

Ödev boyunca yardımını esirgemeyen. ÖĞR. GÖR. TUĞBA SARAY ÇETİNKAYA'ya minnet ve şükranlarımızı sunarız.

Grup arkadaşlarımızla beraber yaptığımız çalışma boyunca birlikteliğimiz için de teşekkür ederim

GİRİŞ : TANITIM

Bu rapor, Gelişim Üniversite Hastanesi için ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin kurulumunu belgelemektedir. Kurum yönetimi tarafından belirlenen amaç, kapsam ve politika doğrultusunda, Bilgi Güvenliği Yöneticisi tarafından gerçekleştirilen adımlar ve alınan kararlar bu raporda detaylandırılmıştır.

BİRİNCİ BÖLÜM

1.1 İSO 27001 BELGESİ NEDİR? BU BELGEYİ ALMAK İÇİN NELER GEREKİR?

ISO 27001 belgesi, bilgi güvenliği yönetim sistemlerini belirlemek ve uygulamak için uluslararası bir standarttır. Bu belge, bir kuruluşun bilgi varlıklarını nasıl yönettiğini, koruduğunu ve sürekli olarak geliştirdiğini gösteren bir kanıt sağlar. İşletmelerin müşteri güvenini artırmak, yasal gerekliliklere uygunluğu sağlamak ve risk yönetimini güçlendirmek için ISO 27001'e uyum sağlamaları yaygın bir uygulamadır.



ISO 27001 belgesi almak için bir kuruluşun aşağıdaki adımları izlemesi gerekmektedir:

- 1)Kapsamın Belirlenmesi: Kuruluş, ISO 27001 standardının kapsamını belirler. Hangi bilgi varlıklarını içereceği, hangi süreçleri ve bölümleri kapsayacağı gibi konular belirlenir.
- 2)Risk Değerlendirmesi ve Risk Yönetimi: Bilgi güvenliği risklerini belirlemek için kapsamlı bir risk değerlendirmesi yapılır. Bu, olası tehditleri, zayıf noktaları ve bunların olası etkilerini içerir. Daha sonra, bu risklerin nasıl ele alınacağına dair bir plan yapılır.
- 3)Politika ve Süreçlerin Oluşturulması: Bilgi güvenliği politikası ve süreçleri oluşturulur ve belgelendirilir. Bu politika ve süreçler, ISO 27001 standardının gereksinimlerine uygun olarak kuruluşun bilgi güvenliğini nasıl sağlayacağını belirtir.
- 4)Uygulama ve Operasyonel Kontrollerin Kurulması: Belirlenen politika ve süreçlerin uygulanması için gerekli kontroller hayata geçirilir. Bunlar, fiziksel güvenlik önlemleri, erişim kontrolü, eğitim ve farkındalık programları gibi çeşitli alanları kapsar.
- 5)İzleme ve İyileştirme: ISO 27001 belgesine uygunluğun sürekli olarak izlenmesi ve iyileştirilmesi sağlanır. Bunun için periyodik iç denetimler ve yönetim incelemeleri yapılır. Ayrıca, geribildirimler ve olaylar üzerinden sürekli olarak bilgi güvenliği performansı değerlendirilir ve iyileştirme fırsatları belirlenir.

ISO 27001 belgesi, bir kuruluşun bilgi güvenliği yönetim sistemini uluslararası kabul görmüş bir çerçeve içinde değerlendirmesine ve belgelendirmesine olanak tanır. Bu da hem kuruluş içinde hem de dışında güvenilirlik ve rekabet avantajı sağlar.

1.2 PEKİ NEDEN BİLGİ GÜVENLİĞİNDE ISO 27001 BELGESİNİ BU KADAR ÖNEMLİ?

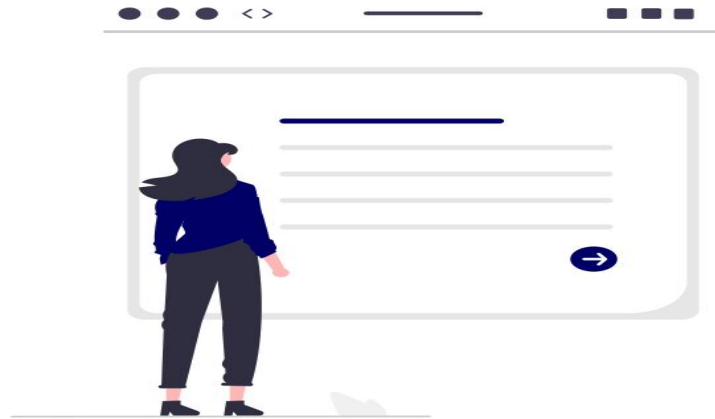
Bilgi güvenliği, günümüzde işletmeler için giderek artan bir öneme sahiptir. Veri ihlalleri, siber saldırılar ve diğer bilgi güvenliği tehditleri, hem finansal hem de itibari kayıplara yol açabilir. İşte bu noktada, ISO 27001 belgesi gibi uluslararası kabul görmüş bir standart, işletmelere önemli faydalar sağlar. İşte bu faydaların ana hatları:

1)Müşteri Güveni ve Rekabet Avantajı:



ISO 27001 belgesi, müşterilere güvenilirlik ve bilgi güvenliği konusunda sağlam bir kanıt sunar. Bir şirket, bu belgeyi elde ettiğinde, müşterilerine bilgi varlıklarını koruma konusundaki taahhütlerini kanıtlamış olur. Bu da müşteri güvenini artırır ve rekabet avantajı sağlar.

2)Yasal ve Düzenleyici Uyumluluk:



İşletmeler, çoğu zaman belirli yasal ve düzenleyici gereksinimlere uyumlu olmak zorundadır. ISO 27001 belgesi, bu gereksinimleri karşılamak için güçlü bir çerçeve sunar. Bir kuruluş, bu standarta uyumlu hale geldiğinde, ilgili yasal ve düzenleyici gereksinimlere uyum konusunda daha güçlü bir konuma gelir.

3)Risk Yönetimi ve Verimlilik:



ISO 27001 belgesi, bir işletmenin bilgi güvenliği risklerini etkin bir şekilde yönetmesine olanak tanır. Risk değerlendirmesi ve risk yönetimi süreçleri sayesinde, potansiyel tehditler belirlenir ve önlem alınır. Bu da işletmelerin daha güvenli ve verimli bir şekilde faaliyet göstermelerini sağlar.

4)Maliyet Tasarrufu:



Bilgi güvenliği ihlalleri ve siber saldırılar, işletmeler için ciddi maliyetlere yol açabilir. Veri kaybı, itibar kaybı, yasal cezalar ve müşteri kaybı gibi maliyetler, uzun vadede önemli olabilir. ISO 27001 belgesi, bu tür maliyetleri azaltmaya yardımcı olabilir. Daha güçlü bir bilgi güvenliği yönetim sistemi, potansiyel riskleri azaltır ve böylece maliyetleri düşürür.

5)Sürekli İyileştirme ve İnovasyon:



ISO 27001 belgesi, sürekli iyileştirme ve yenilik kültürünü teşvik eder. Belgenin gerektirdiği periyodik iç denetimler ve yönetim incelemeleri, işletmelerin sürekli olarak bilgi güvenliği performansını değerlendirmesini sağlar. Bu da işletmelerin sürekli olarak iyileştirme fırsatları bulmalarını ve bilgi güvenliği alanında yenilik yapmalarını sağlar.

Sonuç olarak, ISO 27001 belgesi, işletmeler için bilgi güvenliği yönetiminde uluslararası bir referans noktası sağlar. Bu belgeyi elde etmek, müşteri güvenini artırır, yasal uyumluluğu sağlar, risk yönetimini güçlendirir, maliyetleri azaltır ve sürekli iyileştirmeyi teşvik eder. Bu nedenle, birçok işletme için önemli bir rekabet avantajı ve operasyonel gereklilik haline gelmiştir.

İKİNCİ BÖLÜM

2.1 PROJE SENARYO

1. Amaç :

Hastanede belirtilen bölümlerin varlıklarını belirlemek ve bu varlıkları karşı karşıya gelebilecek her türlü tehdit , tehlike ve riskten korumaktır.

2. Kapsam :

Maaş Mutematığı , Arşiv Birimi ve Bilgi İşlem Birimini kapsamı alanına almaktadır.

3. Politika :

Hastane verilerinin saklanması, erişimi, güvenliği ve yok edilmesi , hastane içindeki bilgi teknolojileri (BT) altyapısı, veri güvenliği, yazılım kullanımı ve ağ yönetimi , çalışanlar maaş verilerini , kişisel ve kurumsal verilerini korumak gibi konuları düzenler.

2.2 VARLIK ENVANTERİ

Varlık envanteri, bir kuruluşun veya birimin sahip olduğu fiziksel varlıkların tam bir listesini ve bunların detaylı bilgilerini içeren kayıt sistemidir. Bu envanter, kuruluşun varlık yönetimi süreçlerinin bir parçası olarak kullanılır ve genellikle bilgisayar programları veya özel yazılımlar aracılığıyla tutulur.

Bu kısımda, hastanede belirlenen üç birim ve bu birimlerde bulunan değerli varlıklar listelenmiştir;

Maaş mutematiği birimi

- Personel bilgi birimi
- Maaş hesaplama tabloları ve formülleri
- Zaman takip sistemi
- Muhasebe yazılım
- İç kontrol ve denetim prosedürleri
- Personel dosyaları ve bilgileri
- Yasal düzenlemeler ve ilgili belgeler
- Maaş mutematiği politika ve ve prosedürleri

Arşiv birimi

- Arşiv dolapları
- Dijital arşiv sistemi
- Güvenlik sistemleri
- Yedekleme cihazları
- Arşiv güvenlik politikaları
- Personel eğitim belgeleri

Bilgi işlem birimi

- Ofis uygulamaları
- İşletim sistemi ve yedekleme yazılımları
- Veri merkezi sunucuları
- Router, switch, hub
- SAN ve NAS cihazları
- Firewall cihazları
- KasperSky, Avast
- Teknik destek iş akışı dokümanları

Görsel 1.0

Varlık Adı
Personel Bilgi Sistemi
Maaş Hesaplama Tabloları ve Formülleri
Zaman Takip Sistemi
Muhasebe Yazılımı
İç Kontrol ve Denetim Prosedürleri
Personel Dosyaları ve Belgeleri
Yasal Düzenlemeler ve İlgili Belgeler
Maaş Mutemetigi Politika ve Prosedürleri
Arşiv Dolapları
Dijital Arşiv Sistemi
Güvenlik Sistemleri
Yedekleme Cihazları
Arşiv Güvenlik Politikaları
Personel Eğitim Belgeleri
Ofis Uygulamaları
İşletim sistemi ve yedekleme yazılımları
Veri Merkezi Sunucuları
Router ,Switch ,Hub
SAN ve NAS Cihazları
Firewall Cihazları
Kaspersky ,Avast , vb
Teknik Destek İş Akışı Dokümanları

Görsel 1.1

Varlık Sahibi
Maaş Mutematığı
Maaş Mutematığı
Maaş Mutematığı
Maaş Mutematığı
Maaş Mutematığı
Maaş Mutematığı
Maaş Mutematığı
Maaş Mutematığı
Arşiv Birimi
Arşiv Birimi
Arşiv Birimi
Arşiv Birimi
Arşiv Birimi
Arşiv Birimi
Bilgi İşlem Birimi
Bilgi İşlem Birimi
Bilgi İşlem Birimi
Bilgi İşlem Birimi
Bilgi İşlem Birimi
Bilgi İşlem Birimi
Bilgi İşlem Birimi
Bilgi İşlem Birimi

2.3 RİSK KÜTÜĞÜ

Risk kütüğü, bir organizasyonun veya işletmenin faaliyetleri sırasında karşılaşılabileceği potansiyel risklerin sistematik bir şekilde belirlendiği, kaydedildiği ve yönetildiği bir doküman veya veri tabanıdır. Bu kütük, belirlenen risklerin önceliklendirilmesine, değerlendirilmesine ve uygun önlemlerin alınmasına olanak sağlar. Ayrıca, risklerin izlenmesi ve yönetim süreçlerinin etkinliğinin değerlendirilmesi için de kullanılır.

Bu bölümde her bir varlık ve varlık için belirlenen potansiyel riskler/tehditler açıklanmıştır;

Personel bilgi sistemi

- I. Veri sızıntısı ve ihlalleri
- II. Yetersiz veri yedekleme
- III. Kötü amaçlı yazılımlar

Maaş hesaplama tabloları ve formülleri

- I. Hatalı veri girişi
- II. Güvenlik açıkları
- III. Yasal ve düzenleyici riskler

Zaman takip sistemi

- I. Sahte veri girişi
- II. Kimlik hırsızlığı
- III. Donanım sorunları
- IV. Güvenlik eğitimi eksikleri
- V. Yetkisiz erişim

Muhasebe yazılımı

- I. Veri güvenliği tehditleri
- II. Phishing saldırıları
- III. İç tehditleri
- IV. Yazılım güncellemeleri

İç kontrol ve denetim prosedürleri

- I. İşletme sürecindeki hatalar
- II. İşletme personeli
- III. Yetersiz iç kontrol politikaları
- IV. Teknolojik tehditler
- V. Hatalı veri analizi

VI. İç denetim zafiyetleri

Personel dosyaları ve belgeleri

- I. Veri hırsızlığı
- II. Phishing
- III. Fiziksel güvenlik tehditleri
- IV. Kötü amaçlı yazılımlar
- V. Yetersiz veri koruma ilkeleri

Yasal düzenlemeler ve ilgili belgeler

- I. Bilgi güvenliğinin ihlalleri
- II. Uyumsuzluk ve ceza
- III. Yetkisiz erişim
- IV. Fiziksel güvenlik tehditleri
- V. Yetersiz saklama ve imha yöntemleri

Maaş mutematiği politikaları ve prosedürleri

- I. Yetki ihlalleri
- II. İç tehditleri
- III. Veri güvenliği tehditleri
- IV. Yetersiz iç kontrol politikaları

Arşiv dolapları

- I. Yangın ve su baskını
- II. İç tehditler
- III. Yetkisiz erişim
- IV. Veri hırsızlığı

Dijital arşiv sistemi

- I. Siber saldırılar
- II. Kötü amaçlı yazılımlar
- III. Zayıf şifreleme
- IV. Yetersiz yedekleme
- V. Phishing

Güvenlik sistemleri

- I. Crackli programlar
- II. Kullanıcı fazlalığı
- III. Zayıf ve aynı şifreler
- IV. Yetersiz personel eğitimi

Yedekleme cihazları

- I. Yetersiz güvenlik ayarları
- II. Dış tehditleri
- III. Teknolojik sorunlar
- IV. Yetersiz yedekleme planları

Arşiv güvenlik politikaları

- I. Erişim kontrolü zafiyetleri
- II. Yetersiz veri saklama ve imha politikaları
- III. İç tehditler

Personel eğitim belgeleri

- I. Belgede sahtecilik
- II. Bilinçsizlik
- III. Bilgiyi kötüye kullanım
- IV. Yedekleme ve kurtarma sorunları

Ofis uygulamaları

- I. Crack yazılımlar
- II. Zayıf şifreleme
- III. Yetkisiz kullanıcılar
- IV. Güvenlik güncellemeleri
- V. Denetim ve izleme yapılamaması

İşletim sistemi ve yedekleme yazılımları

- I. Exploitler
- II. Güvenlik zafiyetleri
- III. Zayıf şifreleme
- IV. Yetersiz yedekleme planları
- V. Sosyal mühendislik saldırıları

Veri merkezi sunucuları

- I. Denial of services (DoS) saldırılar
- II. Uzaktan erişimler
- III. Kötü amaçlı yazılımlar
- IV. Fiziksel güvenlik tehditleri

Router/switch/hub

- I. Fiziksel tehdit
- II. Ağ trafiği yönlendirme hataları
- III. Yazılım güncellemesi yapmama
- IV. DDoS saldırıları

SAN ve NAS cihazları

- I. Veri güvenliği
- II. Veri sızıntıları
- III. DoS/DDoS saldırıları
- IV. Yetersiz güvenlik politikaları
- V. Exploitler

Firewall cihazları

- I. Firewall bypass
- II. DoS saldırıları
- III. Kötü amaçlı yazılımlar

Kasper Sky/Avast

- I. Crack yazılımlar
- II. Yanlış pozitif yanılmalar
- III. Fiziksel güvenliği sağlama
- IV. Gizlilik ve verileri koruma politikaları

Teknik destek ve iş akışı dokümanları

- I. Gizlilik riskleri
- II. Yetkisiz erişim
- III. Güvenlik politikalarının yetersizliği
- IV. Düzenli denetimlerin olmaması
- V. Doğruluk ve güncellik sorunları

2.3.1 RİSK KÜTÜĞÜ GÖRSELLERİ

Görsel 1.2

Gelişim A.Ş Risk Kütüğü				Doküman Kodu:								
				Yayın Tarihi:								
				Revizyon Tarihi:								
				Revizyon No:								
Varlık sıra no	Varlık	Varlık sahibi	Tehdit	Açıklık	Varlığın güzelliliğine etkisi	Varlığın bütünlüğüne etkisi	Varlığın erişilebilirliğine ne etkisi	Tehdit olasılık değeri	Risk Değeri			
1	personel bilgi sistemi	Maaş mutematiği	Veri sızıntısı ve ihalleri Yetersiz Veri Yedekleme kötü amaçlı yazılımlar	Donanımsız personel Veri kaybı Virüsler,fidyeye yazılımları	2 1 2	2 1 2	2 1 2	1 1 2	7 5 8			
2	Maaş hesaplama tabloları ve formülleri	Maaş mütematiği	Hatalı veri girişi Güvenlik açıkları Yasal ve düzenli riskler	Çalışanların maaşının eksik ödenmesi Veri manipülasyonu , sisteme sızılması Cezai yaptırımlar,yasal sorunları	0 2 1	0 1 1	0 2 1	1 1 4	1 6 4			
3	Zaman takip sistemi	Maaş mutematiği	sahte veri girişi Kimlik hırsızlığı Donanım sorunları Güvenlik eğitimi eksikleri Yetkisiz erişim	Çalışma saatlerinin karışması Kullanıcı kimliklerinin çalınması Veri kaybı,verilerin doğrulunun etkilenmesi Sistemlerin savunmasız kalması Veri manipülasyonu	0 2 2 2 2	0 2 2 1 1	0 1 1 2 1	1 2 1 2 1	1 7 6 7 5			
4	Muhasebe yazılımı	Maaş mutematiği	Veri güvenliği tehditleri Phishing saldırıları İç tehditler Yazılım güncellemeleri	Veri hırsızlığı,verilere yetkisiz erişim Kullanıcıların kimliklerine izinsiz erişim Personellerin verileri dışarı sızdırması Güvenlik zafiyetleri	2 1 1 2	2 1 1 2	1 1 1 2	2 2 1 2	7 5 5 8			
5	İç kontrol ve denetim prosedürleri	Maaş mutematiği	İşletme sürecindeki hatalar İletişim sorunu	Yanlış/eksik bilgi girişi İletim kısıtlılığı,etkileşimsiz yönetim süreçleri	0 1	2 1	1 2	1 4	4 5			

Görsel 1.3

6	Personel dosyaları ve belgeleri	Maas mutemetiği	Veri hrsrzlığı	Verilerin 3 kşilerin ellne gemesi	2	2	2	2	8
			Phishing	Kullanıcı kimliklerinin alınması	2	1	1	2	6
			Fiziksel güvenlik tehditleri	Dosyaların kaybolması veya alınması	2	2	1	1	6
			Kötü amaçlı yazılımlar	Virüsler,kötü amaçlı yazılımlar	2	2	2	2	8
			Yetersiz veri koruma ilkeleri	personel bilgilerine kolay ulaşılması	1	1	1	1	4
7	Yasal düzenlemeler ve ilgili belgeler	Maas mutemetiği	Bilgi güvenliğinin ihlalleri	Müşteri verileri,finans bilgilerinin sızdırılması	2	2	1	1	6
			Uyumsuzluk ve ceza	İşletmenin yasal yaptırımlara çarptırılması	1	1	1	1	4
			Yetkisiz erişim	Bilgilerin değiştirilmesi,hukuki yaptırımlar	2	1	1	1	5
			Fiziksel güvenlik tehditleri	Belgelerin alınması,zarar görmesi	2	1	1	1	5
			Yetersiz saklama ve imha yöntemleri	İşletmenin gereksiz bilgileri saklaması imha etmesi	2	1	1	1	5
8	Maas mutemetiği politikaları ve prosedürü	Maas mutemetiği	Yetki ihlalleri	Verilerin alınması,sızdırılması	2	1	2	1	6
			İç tehditler	İhmalcilikler,kötü niyetli çalışan	1	2	2	1	6
			Veri güvenliği tehditleri	Maas,finansal verilerin alınması	1	1	1	1	4
			Yetersiz iç kontrol politikaları	Çalışanların denetlenmemesi	0	2	1	1	4
			Fiziksel güvenlik tehditleri	Belgelerin imha edilmemesi,açıkta tutulması	2	1	1	1	5
9	Arşiv dolapları	Arşiv birimi	Yangın ve su baskını	Arşiv dosyalarının zarar görmesi, tamamen yok olması	2	2	1	2	7
			İç tehditler	Çalışanların kötü niyetli eylemleri	2	1	1	1	5
			Yetkisiz erişim	3 kişilerin arşiv dosyalarını erişmesi	2	1	1	1	5
			Veri hrsrzlığı	Dosyaların alınması,çöğaltılıp sızdırılması	2	2	2	1	7
10	Dijital arşiv sistemi	Arşiv birimi	Siber saldırılar	Verilerin alınması,sistemin çökmesi	2	2	1	2	7
			Kötü amaçlı yazılımlar	Virüsler,fidye yazılımları,solucanlar	1	1	1	2	5
			Zayıf şifreleme	Bilgilerin yetkisiz erişime açık hale gelmesi	2	1	1	1	5
			Yetersiz yedekleme	Büyük veri kayıpları	2	2	2	2	8
			phishing	Kullanıcıların kimliklerinin alınması	0	2	1	1	4
11	Güvenlik sistemleri	Arşiv birimi	Crackli programlar	Bilgisayarların sağlığı	1	1	2	1	5
			Kullanıcı fazlalığı	Bilgilerin silinmesi,kopyalanması	1	1	1	1	4

Görsel 1.4

12	Yedekleme cihazları	Arşiv birimi	Yetersiz güvenlik ayarları	Veri kayıpları,yüksek para kayıpları	1	1	2	1	5
			Diş tehditler	yedekleme cihazlarının hacklenmesi	2	2	1	2	7
			Teknolojik sorunlar	elektronik cihazların bozulması,veri kayıpları	2	2	1	1	6
			Yetersiz yedekleme planları	geri dönüşü olmayan veri kayıpları	2	2	2	2	8
13	Arşiv güvenlik politikaları	Arşiv birimi	Erişim kontrolü zafiyetleri	Yetkisiz kişilerin belgelere erişmesi	2	2	1	1	6
			Yetersiz veri saklama ve imha politikaları	verilen düzgün saklanmaması ve imha edilmemesi	2	2	2	2	8
			İç tehditler	sistem yöneticilerinin ihlalleri	1	1	1	1	4
14	Personel eğitim belgeleri	Arşiv birimi	Belgede sahtecilik	Cezai yaptırımlar,işletmede aksaklıklar	1	1	1	1	4
			Bilinçsizlik	Riskelerin göz ardı edilmesi,önlem alınmaması	2	1	1	1	5
			Bilgiyi kötüye kullanım	Personellerin verileri çıkarılmasına göre işlemesi	2	1	1	1	5
			Yedekleme ve kurtarma sorunları	Veri kayıpları/silinmesi	2	1	1	1	5
15	Ofis uygulamaları	Bilgi işlem birimi	Crack yazılımlar	Dosyaların silinmesi,fidye yazılımla ele geçirilmesi	2	1	2	1	6
			Zayıf şifreleme	Verilerin çalınması,kopyalanması	1	2	2	1	6
			Yetkisiz kullanıcılar	Verilerin 3.kişilerin eline geçmesi	1	1	1	1	4
			Güvenlik güncellemeleri	siber saldırıları	0	2	1	1	4
			Denetim ve izleme yapılamaması	Anormal aktivitelerin verileri bozması	2	1	1	1	5
16	İşletim sistemi ve yedekleme yazılımları	Bilgi işlem birimi	Exploitler	Zafiyetleri kullanarak verilere erişme					
			Güvenlik zafiyetleri	Veri kayıpları	2	2	1	2	7
			Zayıf şifreleme	Sisteme yetkisiz erişim	2	1	1	1	5
			Yetersiz yedekleme planları	Veri sızıntıları,kayıpları	2	1	1	1	5
			Sosyal mühendislik saldırıları	Kullanıcı bilgilerine izinsiz erişim	2	2	2	1	7
17	Veri merkezi sunucuları	Bilgi işlem birimi	Denial of service (DoS) saldırıları	Hizmet kalitesinin düşmesi , işletmede aksaklık	2	2	2	2	8
			Uzaktan erişimler	Yetkisiz erişimler,bilgi sızıntısı,veri hırsızlığı	2	1	1	1	5
			Kötü amaçlı yazılımlar	Virüsler,fidye yazılımlar,solucanlar	2	2	2	1	7
			Fiziksel güvenlik tehditleri	Doğal afetler,yangın	2	1	1	1	5

Görsel 1.5

18	Router/switch/hub	Bilgi işlem birimi	Fiziksel tehditler	Elektrik dalgalanmaları,anı kesintileri,sel baskınları	1	2	2	2	7
			Ağ trafiği yönlendirme hataları	Ağ hizmetlerinin bozulması	2	1	1	1	5
			Yazılım güncellemesi yapmama	Cihazların işlevselliğinin kısıtlanması	2	2	2	1	7
			DDOS saldırıları	Cihazların aşırı yüklenerek bozulması	2	2	2	2	8
19	SAN ve NAS cihazları	Bilgi işlem birimi	Veri güvenliği	Kötü niyetli kişilerin verilere erişmesi	1	2	2	2	7
			Veri sızıntısı	Hassas bilgilerin ifşa edilmesi	2	1	1	1	5
			DoS/DDoS saldırıları	Cihazları aşırı yükleyerek bozma işlemi	2	2	2	1	7
			Yetersiz güvenlik politikaları	verili kaybının geri dönüşünün olmaması	2	2	2	2	8
			Exploitler	Cihazların zafiyetlerinden yararlanma	0	2	1	1	4
20	Firewall cihazları	Bilgi işlem birimi	Firewall Bypass	Yanlış trafik yönlendirmesi,güvenlik duvarlarının e	2	2	2	2	8
			DoS saldırıları	Cihazları aşırı yükleyerek korumayı etkisizleştirme	2	2	2	1	7
			Kötü amaçlı yazılımlar	Cihazlara yetkisiz erişim	2	2	2	2	8
21	Kasper sky / avast	Bilgi işlem birimi	Crack yazılımlar	Verileri virüs bulaştırma	2	2	2	1	7
			Yanlış pozitif algılamalar	yazılımların programları bozması	1	1	1	2	5
			Fiziksel güvenliği sağlama	Yazılımlara 3. kişilerin erişmesi	2	2	2	1	7
			Gizlilik ve verileri koruma politikaları	yazılımların gizliliğinin sağlanmaması	2	2	2	2	8
22	Teknik destek iş akışı dokümanları	Bilgi işlem birimi	Gizlilik riskleri	Bilgilerin ifşa edilmesi	2	2	2	2	7
			Yetkisiz erişim	Bilgilerin çalınması,sızdırılması	2	1	1	1	5
			Güvenlik politikalarının yetersizliği	Verilerin çalınmaya açık hale gelmesi	2	2	2	1	7
			Düzenli denetimlerin olmaması	Personellerin kendi çıkarına göre hareket etmesi	1	1	1	2	5
			Doğruluk ve güncellik sorunları	Yanlış bilgi aktarımı	1	2	1	1	5

2.4 ISO 27001 UYGULANABİLİRLİK BİLDİRGESİ GÖSTERGESİ

Görsel 1.6

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
13		5.1.1.	Bilgi güvenliği için politikalar	Bir bilgi güvenliği politika dokümanı, yönetim tarafından onaylanmalı, yayınlanmalı, ve tüm çalışanlar ve ilgili dış taraflara bildirilmelidir.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
14		5.1.2.	Bilgi güvenliği için politikaların gözden geçirilmesi	YGG toplantılarında gözden geçirme sağlanır. Gündem maddesidir.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
15		6.1.1.	Bilgi Güvenliği Roller ve Sorumlulukları	Çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların güvenlik rolleri ve sorumlulukları kuruluşun bilgi güvenliği politikasına uygun olarak tanımlanmalı ve dokümanite edilmiştir.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
16		6.1.2.	Görevlerin Ayrılığı	Kuruluşun varlıklarının yetkisiz veya farkında olmadan değiştirilme ya da kötüye kullanıma fırsatlarını azaltmak için, görevler ve sorumluluk alanları ayrılmaktadır.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
17		6.1.3.	Otoritelerle İletişim	İlgili otoritelerle uygun iletişim kurulmaktadır.	UYGULANMAYACAK	Olan taraflar yeterli olduğu için ilgili otoritelere gerek yoktur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
18		6.1.4.	Özel İlgili Grupları ile İletişim	Özel ilgi grupları ve diğer uzman güvenlik forumları ve profesyonel dernekler ile uygun iletişim kurulmaktadır.	UYGULANMAYACAK	Sistem yeterliliği ve düzeni oluşturma için gerekliliği yoktur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak

Görsel 1.7

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
18												
19		6.1.5.	Proje yönetiminde bilgi güvenliği	Proje yönetiminde, proje aşamalarına bakılmaksızın bilgi güvenliği ele alınmalıdır.	UYGULANMAYACAK	Bilgi güvenliği ele alınmıştır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
20		6.2.1.	Mobil Cihaz Politikası	Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.	UYGULANMAYACAK	Active Directory üzerinden politikalar oluşturulmuştur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
21		6.2.2.	Uzaktan Çalışma	Uzaktan çalışma için bir politika, operasyonel planlar ve prosedürler geliştirilmeli ve gerçekleştirilmektedir.	UYGULANMAYACAK	Uzaktan çalışma sistemine elverişli değildir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
22		7.1.1.	Tarama	Tüm işe alım adayları, yükleniciler ve üçüncü taraf kullanıcıları için ilgili yasa, düzenleme ve etişe göre ve iş gereksinimleri, erişilecek bilginin sınıflandırılması ve alınan risklerle orantılı olarak geçmiş doğrulama kontrolleri gerçekleştirilmektedir.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
23		7.1.2.	İstihdam Hükümleri ve Koşulları	Sözleşme yükümlülüklerinin parçası olarak çalışanlar, yükleniciler ve üçüncü taraf kullanıcıları, kendilerinin ve kuruluşun bilgi güvenliği sorumluluklarını belirten kendi işe alım sözleşmelerinin koşullarına katılmış ve bunu imzalamıştır.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
24		7.2.1.	Yönetimin Sorumlulukları	Yönetim, çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların, kuruluşun yerleşik politika ve prosedürlerine göre güvenliği uygulamaları istenmektedir.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı

Görsel 1.8

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
26		7.2.3.	Disiplin Prosesi	Bir güvenlik kınımına yol açan çalışanlar için resmi bir disiplin prosesi oluşturulmuştur.	UYGULANACAK	Güvenlik kınımına ilişkin yedek bir plan mevcut olmalıdır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
27		7.3.1.	İstihdam sorumluluklarının sonlandırılması ve değiştirilmesi	İstihdamın sonlandırılması veya değiştirilmesini gerçekleştirme sorumlulukları açıkça tanımlanmıştır.	UYGULANMAYACAK	Farklı sorumluluklar yoktur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
28		8.1.1.	Varlıkların Envanteri	Tüm varlıklar açıkça tanımlanmalı ve önemli varlıkların bir envanteri hazırlanmalı ve tutulmaktadır.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
29		8.1.2.	Varlıkların Sahipliği	Bilgi işleme olanakları ile ilişkili bilgi ve varlıkların kuruluşun belirlenmiş bir bölümü tarafından sahiplenmiştir.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
30		8.1.3.	Varlıkların kabul edilebilir kullanımı	Bilgi işleme olanakları ile ilişkili bilgi ve varlıkların kabul edilebilir kullanım kuralları tanımlanmalı, doküman ve gerçekleştirilmektedir.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
31		8.1.4.	Varlıkların İadesi	Tüm çalışanlar, yükleniciler, ve üçüncü taraf kullanıcılar, çalışmalar, sözleşmeleri veya anlaşmalarının sonlandırılmasıyla birlikte kendilerinde bulunan kuruluşun tüm varlıklarını iade etmektedirler.	UYGULANACAK	Tüm personellere verilen envanterler geri alınması kontrol edilmelidir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
32		8.2.1.	Bilgi Sınıflandırması	Bilgi, değeri, yasal gereksinimleri, hassaslığı ve kuruluş için kritikliğine göre sınıflandırılmıştır.	UYGULANMAYACAK	Böyle bir tabloya kurum için ihtiyaç yoktur.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak

Görsel 1.9

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
33												
34		8.2.3.	Varlıkların Kullanımı	Varlıkların kullanımı için Parolaların tahsis, resmi bir yönetim prosesi aracılığıyla kontrol edilmelidir.	UYGULANACAK	Parolalar 2 ayda bir değiştirilecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
35		8.3.1.	Taahhütlü Ortam Yönetimi	Taahhütlü ortam yönetimi için mevcut prosedürler bulunmaktadır.	UYGULANMAYACAK	Taahhütlü bir ortam olmayacaktır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
36		8.3.2.	Ortamın Yok Edilmesi	Ortam gereksinimi ortadan kalktığında, resmi prosedürler kullanılarak güvenli ve emniyetli bir biçimde yok edilmektedir.	UYGULANACAK	Gerekli evrakların uygun bir biçimde yok edilmesi için gerekli şartlar oluşturulacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
37		8.3.3.	Fiziksel Ortam Aktarımı	Bilgi içeren ortam, kuruluşun fiziksel sınırları ötesinde taşıma esnasında, yetkisiz erişime, kötüye kullanıma ya da bozulmaya karşı korunmaktadır.	UYGULANACAK	Her zaman yedek alınacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
38		9.1.1.	Erişim Kontrolü Politikası	Erişim için iş ve güvenlik gereksinimleri temel alan bir erişim kontrol politikası kurulmalı, doküman ve edilmiş ve gözden geçirilmektedir.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
39		9.1.2.	Ağlara ve Ağ Hizmetlerine Erişim	Kullanıcıların sadece, özellikle kullanıcılarına yetki verilen hizmetlere erişimine yetki verilen hizmetlere erişime sahip olmaları sağlanmaktadır.	UYGULANACAK	Kullanıcı bazlı erişim hizmetleri aktif olmuştur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
40		9.2.1.	Kullanıcı kaydetme ve kayıt silme	Tüm bilgi sistemlerine ve hizmetlerine erişim izni vermek ve bunu kaldırmak için resmi bir kullanıcı kaydetme ve kayıttan çıkarma prosedürü vardır.	UYGULANACAK	Eski ve yeni personellerinin kaydı 5 yıl sonra silinecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı

Görsel 1.10

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
42	9.2.3.	Ayrıcalıklı Erişim Haklarının yönetimi	Ayrıcalıkların tahsis ve kullanımı sınırlandırılmalı ve kontrol edilmelidir.	UYGULANACAK	Sınırlar 3 ay da bir kontrol edilecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak	
43	9.2.4.	Kullanıcılara Ait gizli kimlik doğrulama bilgilerinin yönetimi	Tüm kullanıcılar, kendi kişisel kullanımları için benzersiz bir kimliğe sahip olmalıdırlar ve bir kullanıcının öne sürdüğü kimliği ispatlamak için uygun bir kimlik doğrulama sistemi vardır.	UYGULANACAK	Kimlik doğrulama sistemi kullanılacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak	
44	9.2.5.	Kullanıcı Erişim Haklarının Gözden Geçirilmesi	Yönetim, kullanıcıların erişim haklarını resmi bir proses kullanarak düzenli aralıklarla gözden geçirmelidir.	UYGULANACAK	1 ay da bir yöneticiler gizlilikleri için gerekli prosedürleri izleyecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
45	9.2.6.	Erişim Haklarının Kaldırılması veya düzenlenmesi	Tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların bilgi ve bilgi işleme olanaklarına olan erişim hakları, istihdam, sözleşme veya anlaşmalarının sonlandırılmasıyla birlikte kaldırılmaktadır ya da	UYGULANMAYACAK	Erişim hakları kalmayacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
46	9.3.1.	Gizli Kimlik Doğrulama Bilgisinin Kullanımı	Kullanıcıların,gizli kimlik doğrulama bilgisinin kullanımında kurumsal uygulamalara uymaları şart koşulmalıdır.	UYGULANACAK	Kimlik doğrulama uygulanacak.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
47	9.4.1.	Bilgi Erişimin Kısıtlanması	Kullanıcılar ve destek personeli tarafından bilgi ve uygulama sistem işlevlerine erişim, tanımlanmış erişim kontrol politikasına uygun olarak kısıtlanmaktadır.	UYGULANACAK	Kontrol politikasına uygun kısıtlanmıştır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
48	9.4.2.	Güvenli Oturma Açma Prosedürleri	İşletim sistemine erişim güvenli bir oturma açma prosedürü ile kontrol edilmektedir.	UYGULANACAK	Yeni oturma açma prosedürü mevcuttur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	

Görsel 1.11

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
50		9.4.4.	Ayrıcalıklı Destek Programlarının Kullanımı	Sistemin üzerine yazabilme yeteneği olabilecek yardımcı sistem programlarının kullanımı kısıtlanmalı ve sıkıca kontrol edilmektedir.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
51		9.4.5.	Program Kaynak Koduna Erişim Kontrolü	Program kaynak kodlarına erişim kısıtlı olmalıdır.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
52		10.1.1.	Kriptografik Kontrollerin Kullanımına İlişkin Politika	Bilginin korunması için kriptografik kontrollerin kullanımına ilişkin bir politika geliştirilmeli ve gerçekleştirilmelidir.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
53		10.1.2.	Anahtar Yönetimi	Kriptografik anahtarların kullanımı, korunması ve yaşam süresine dair bir politika geliştirilmeli ve tüm yaşam çevrimleri süresince uygulanmalıdır.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
54		11.1.1.	Fiziksel Güvenlik Çevresi	Bilgi ve bilgi işleme olanaklarını içeren alanları korumak için güvenlik çevreleri kullanılmaktadır.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
55		11.1.2.	Fiziksel Giriş Kontrolleri	Güvenli alanların yalnız yetkili personelin erişimine izin vermesi için uygun giriş kontrolleri ile korunmaktadır.	UYGULANACAK	Kapı girişlerinde parmak izi tanımlama sistemi olacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
56		11.1.3.	Ofislerin odaların ve tesislerin güvenliğini sağlanması	Ofisler odalar ve olanaklar için fiziksel güvenlik tasarlanmış ve uygulanmaktadır.	UYGULANACAK	Odalara parmak izi ile giriş yapılacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı

Görsel 1.12

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
58		11.1.5.	Güvenli Alanlarda Çalışma	Güvenli alanlarda çalışma için fiziksel koruma tasarlanmış ve uygulanmaktadır.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
59		11.1.6.	Teslimat ve yükleme alanları	Dağıtım ve yükleme alanları gibi erişim noktaları ve yetkisiz kişilerin içeri girebileceği diğer noktalar kontrol edilmekte ve yetkisiz erişimden kaçınmak için bilgi işleme olanakları geliştirilmiştir.	UYGULANMAYACAK	Kameralar mevcut olduğu için gerekli değildir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
60		11.2.1.	Techizat Yerleştirme ve Koruma	Techizat çevresel tehditlerden ve tehlikelerden kaynaklanan riskleri ve yetkisiz erişim fırsatlarını azaltmak için yerleştirilmiş ve korunmuştur.	UYGULANACAK		Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
61		11.2.2.	Destekleyici Altyapı Hizmetleri	Techizat, elektrik kesintileri ve destek hizmetlerindeki arızalardan kaynaklanan diğer bozulmalara karşı korunmaktadır.	UYGULANACAK	Destekleyici altyapı mevcuttur.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
62		11.2.3.	Kablo Güvenliği	Veri taşıyan ya da bilgi hizmetlerini destekleyen elektrik ve haberleşme kabloları, kesilme ya da hasarlardan korunmaktadır.	UYGULANACAK	Fiber kablolar ile donatılmıştır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
63		11.2.4.	Techizat Bakımı	Techizatın sürekli kullanılabilirliğini ve bütünlüğünü sağlamak için doğru şekilde bakımı yapılmaktadır.	UYGULANACAK	Yatırım ve uzun vade bakımından yapılmıştır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
64		11.2.5.	Varlıkların Taşınması	Ön yetkilendirme olmaksızın techizat, bilgi veya yazılım bulunduğu yerden çıkarılmamaktadır.	UYGULANMAYACAK	Varlıklar taşınmayacaktır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak

Görsel 1.13

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
66		11.2.7.	Techizatın Güvenli Yok Edilmesi Veya Tekrar Kullanımı	Techizatın güvenli şekilde yok edilmesi için tüm parçaları, elden çıkarılmadan önce, herhangi bir hassas veri ve lisanslı yazılım varsa kaldırılmasını veya güvenli şekilde üzerine yazılmasını sağlamak için kontrol	UYGULANACAK	Techizatlar tekrar kullanılacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
67		11.2.8.	Gözetimsiz Kullanıcı Techizatı	Kullanıcılar, gözetimsiz techizatın uygun bir korumaya sahip olmasını sağlamalıdır.	UYGULANMAYACAK	Gözetimsiz kullanmaya uygundur.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
68		11.2.9.	Temiz Masa ve Temiz Ekran Politikası	Kağıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme olanakları için bir temiz ekran politikası benimsenmiştir.	UYGULANACAK	Temiz masa ve temiz çevre politikası vardır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
69		12.1.1.	Yazılı İşletim Prosedürleri	İşletim prosedürleri dokümanlar halinde edilmekte, sürdürülmekte ve ihtiyacı olan tüm kullanıcılara kullanılabilir yapılmaktadır.	UYGULANACAK	İşletim prosedürleri yazılacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
70		12.1.2.	Değişiklik Yönetimi	Bilgi işleme olanakları ve sistemde olan değişiklikler kontrol edilmektedir.	UYGULANACAK	Değişiklik sağlanmayacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
71		12.1.3.	Kapasite Yönetimi	Gerekli sistem performansını sağlamak için, kaynakların kullanımı izlenerek ayarlanmakta ve gelecekteki kapasite gereksinimleri için projeksiyonlar yapılmaktadır.	UYGULANACAK	Kapasite yöntemleri düzenli aralıklarla kontrol edilecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
72		12.1.4.	Geliştirme Test Ve İşletim Ortamlarının Birbirinden Ayrılması	Geliştirme, test ve işletim olanakları, işletilen sisteme yetkisiz erişim veya değişiklik risklerini azaltmak için ayrılmıştır.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı

Görsel 1.14

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
74		12.3.1.	Bilgi Yedekleme	Bilgi ve yazılımlara ait yedekleme kopyaları alınmalı ve anlaşılan yedekleme politikasına uygun şekilde düzenli olarak test edilmektedir.	UYGULANACAK	Yedekleme ve kopyalama işlemleri olacaktır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
75		12.4.1.	Olay Kaydetme	Kullanıcı faaliyetleri, ayrıcalıkları ve bilgi güvenliği olaylarını kaydeden denetim kayıtları üretilemeli ve ileride yapılabilecek soruşturmalara ve erişim kontrolü işlemeye yardımcı olmak için anlaşılmış bir süre tutulmalıdır.	UYGULANACAK	Kamera kayıtları sayesinde olayları kaydedeceğiz.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
76		12.4.2.	Kayıt Bilgisinin Korunması	Kayıt olanakları ve kayıt bilgisi kuralanma ve yetkisiz erişime karşı korunmalıdır.	UYGULANACAK	Yetkisiz erişimlere karşı önlemler alınacaktır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
77		12.4.3.	Yönetici ve Operatör Kayıtları	Yönetici ve Operatör Kayıtları	UYGULANMAYACAK	Yönetici ve operatör kayıtları alınmayacaktır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
78		12.4.4.	Saat Senkronizasyonu	Bir kuruluş ya da güvenlik etki alanındaki tüm ilgili bilgi işleme sistemlerinin saatleri, üzerinde uzlaşya varılmış doğru bir zaman kaynağı ile senkronize edilmektedir.	UYGULANMAYACAK	Saat senkronizasyonu değiştirilmeyecektir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
79		12.5.1.	İşletimsel Sistemler Üzerine Yazılım Kurulumu	İşletimsel Sistemler Üzerine yazılım kontrolü için prosedürler uygulanmalıdır.	UYGULANACAK	İşletim sistemi üzerine farklı yazılımlar kurulmayacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
80		12.6.1	Teknik Açıklıkların Yönetimi	Kullanılan bilgi sisteminin teknik açıklıkları hakkında zamanında bilgi elde edilmeli, kuruluşun bu tür açıklıklara maruz kalması değerlendirilmeli ve ilişkili riskleri hedef alan uygun önlemler	UYGULANMAYACAK	Teknik açıklar için gerekli personeller mevcuttur.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak

Görsel 1.15

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
81												
82		12.7.1.	Bilgi Sistemleri Tetkik Kontrolleri	İş proseslerindeki bozulma risklerini en aza indirmek için, operasyonel sistemlerde kontrolleri içeren denetim gereksinimleri ve faaliyetleri dikkatlice planlanmış ve üzerinde anlaşmaya varılmıştır.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
83		13.1.1.	Ağ Kontrolleri	Tehditlerden korunmak için ve iletilmekte olan bilgi dahil ağ kullanan sistemler ve uygulamalar için güvenliği sağlamak amacıyla ağlar uygun şekilde yönetilmekte ve kontrol edilmektedir.	UYGULANACAK	Ağ kontrolleri her ay sonunda kontrol edilecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
84		13.1.2.	Ağ Hizmetlerinin Güvenliği	Tüm ağ hizmetlerinin güvenlik özellikleri, hizmet seviyeleri ve yönetim gereksinimleri tanımlanmalı ve hizmetler kuruluş içinden ya da dışından sağlanmaktadır.	UYGULANACAK	Ağ hizmet politikaları gözden geçirilecektir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
85		13.1.3.	Ağlarda Ayırım	Ağlarda, bilgi hizmetleri, kullanıcıları ve bilgi sistemleri grupları ayrılmalıdır.	UYGULANACAK	Bilişim hizmetleri ve ağlar gruplandırılacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
86		13.2.1.	Bilgi Transfer Politikası	Tüm iletişim olanağı türlerinin kullanımıyla bilgi değişimini korumak için resmi değişim politikaları, prosedürleri ve kontrolleri mevcuttur.	UYGULANACAK	Bilgi transfer politikası oluşturulacak.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
87		13.2.2.	Bilgi Transferindeki Anlaşmalar	Kuruluş ve dış taraflar arasında bilgi ve yazılımın değişimi için anlaşmalar yapılmaktadır.	UYGULANMAYACAK	Bilgi transfer anlaşmaları sağlanmayacak.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
88		13.2.3.	Elektronik Mesajlaşma	Elektronik mesajlaşmadaki bilgi uygun olarak korunmalıdır.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı

Görsel 1.16

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü					
11													
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz	
90		14.1.1.	Güvenlik Gereksinimleri Analizi ve Belirtimi	gereksinimleri bildiregeleri ya da mevcut bilgi sistemlerine yapılan iyileştirmeler güvenlik kontrolleri için gereksinimleri belirlenmiştir.	UYGULANACAK	Gereksinimler analiz edilmiştir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak	
91		14.1.2.	Halka Açık Ağlardaki Uygulama Hizmetlerinin Güvenliğinin Sağlanması	Açık ağlardan geçen elektronik ticaretteki bilgi, hileli faaliyet, anlaşma uyumsuzluğu ve yetkisiz ifşa ve değiştirmeden korunmalıdır.	UYGULANACAK	Halka açık ağlar kullanılmayacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
92		14.1.3.	Uygulama Hizmet İşlemlerinin Korunması	Çevrimiçi işlemlerdeki bilgi, eksik iletimi, yanlış yönlendirmeyi, yetkisiz mesaj değiştirmeyi, yetkisiz ifşa ve yetkisiz mesaj çoğaltmayı ya da yeniden yürütmeyi önlemek için korunmalıdır.	UYGULANACAK	Bilgi ve iletişim korunaklı olacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
93		14.2.1.	Güvenli Geliştirme Politikası	Yazılım ve Sistemlerin Geliştirme Kuralları belirlenmeli ve kuruluş içerisinde ki geliştirmelere uygulanmalıdır.	UYGULANACAK	Güvenli geliştirmeler düzenli olarak yapılmalıdır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak	
94		14.2.2.	Sistem Değişiklik Kontrolü Prosedürleri	Değişikliklerin gerçekleştirilmesi, resmi değişim kontrol prosedürlerinin kullanımı ile kontrol edilmektedir.	UYGULANMAYACAK	Sistem değişiklik kontrol prosedürü hazırdr.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak	
95		14.2.3.	İşletim Platformu Değişikliklerden Sonra Uygulamaların Teknik Gözden Geçirilmesi	İşletim sistemleri değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmasını sağlamak amacıyla iş için kritik uygulamalar gözden geçirmekte ve test edilmektedir.	UYGULANACAK	İşletim sistemleri değiştirildiğinde gerekli kontrollerden geçirilecek.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
96		14.2.4.	Yazılım Paketlerindeki Değişikliklerdeki Kısıtlamalar	Yazılım paketlerine yapılacak değişiklikler, gereksinimlere haric önlenmeli ve tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.	UYGULANACAK	Yazılım paketleri tekrar tekrar incelenip hazır hale getirilecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	

Görsel 1.17

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü					
11													
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz	
98		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.	UYGULANACAK	Güvenli geliştirme ortamı mevcuttur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
99		14.2.7.	Dışarıdan Sağlanan Geliştirme	Dışarıdan sağlanan yazılım geliştirme kuruluşlarından denetlenmeli ve izlenmelidir.	UYGULANACAK	Dışarıdan sağlanan yazılım geliştirme tarafımızca denetlenecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
100		14.2.8.	Sistem Güvenlik Testi	Güvenlik işlevselliğinin test edilmesi, geliştirme süresince gerçekleştirilmelidir.	UYGULANACAK	3 ayda bir sistem denetlenmesi yapılacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak	
101		14.2.9.	Sistem Kabul Testi	Kabul test programları ve ilgili kriterler, yeni bilgi sistemleri, yükseltmeleri ve yeni versiyonları için belirlenmelidir.	UYGULANACAK	Yeni versiyon güncellemeleri kontrol edilecektir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
102		14.3.1.	Test Verisinin Korunması	Test verisi dikkatlice seçilmeli, korunmakta ve kontrol edilmektedir.	UYGULANACAK	Test verileri korunmayacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	
103		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.	UYGULANACAK	Bilgi güvenliği politikası oluşturulmuştur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak	
104		15.1.2.	Tedarikçi anlaşmalarında güvenliği ifade etme	Üçüncü tarafların kuruluşun bilgi veya bilgi işleme olanaklarına erişimini, bunlarla iletişimini veya bunları yönetmelerini içeren ya da bilgi işleme olanaklarına ürün veya hizmetler ekleyen anlaşmalar tüm	UYGULANACAK	Anlaşmalarda güvenliği ifade edilecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı	

Görsel 1.18

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
106		15.2.1.	Tedarikçi Hizmetlerini İzleme ve Gözden Geçirme	Kuruluşlar düzenli aralıklarla tedarikçi hizmet sunumunu izlemeli, gözden geçirmeli ve tetkik etmelidir.	UYGULANMAYACAK	Tedarikçiler tekrar edilen hizmetlerden yararlanmayacaktır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
107		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	UYGULANACAK	Tedarikçi hizmetlerindeki değişiklikler sözleşmelere tabii olacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
108		16.1.1.	Sorumluluklar ve Prosedürler	Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için yönetim sorumlulukları ve prosedürleri oluşturulmuştur.	UYGULANACAK	Sorumlu kişiler belirlenmiş ve prosedürler oluşturulmuştur.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
109		16.1.2.	Bilgi Güvenliği Olaylarının Raporlanması	Bilgi güvenliği olayları uygun yönetim kanalları aracılığıyla mümkün olduğu kadar hızlı biçimde rapor edilmektedir.	UYGULANACAK	Raporlama faaliyetleri en kısa sürede üst birimlere ulaştırılmaktadır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
110		16.1.3.	Bilgi Güvenliği Açıklıklarının Raporlanması	Bilgi sistemleri ve hizmetlerinin tüm çalışanları, yüklenicileri ve üçüncü taraf kullanıcılarından, sistemler ve hizmetlerdeki gözlenen veya şüphelenilen herhangi bir güvenlik zayıflığını dikkat etmeleri ve rapor	UYGULANACAK	Tüm açıklıklar güvenlik personelleri tarafından raporlanacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
111		16.1.4.	Bilgi güvenliği olaylarında değerlendirme ve karar verme	Bilgi güvenliği olayları değerlendirilmeli ve bilgi güvenliği ihlal olayı olarak sınıflandırılıp sınıflandırılmayacağına karar verilmelidir	UYGULANACAK	Sınıflandırma olmayacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
112		16.1.5.	Bilgi Güvenliği ihlal olaylarına yanıt verme	Bilgi Güvenliği ihlal olaylarına yazılı prosedürlere uygun olarak yanıt verilmelidir.	UYGULANACAK	İhwal olaylarında en kısa sürede cevap verilecek ve sorunların çözümleri için aksiyonlar alınacaktır.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak

Görsel 1.19

10					UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü				
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
114		16.1.7.	Kanıt Toplama	Bir bilgi güvenliği ihlal olayından sonra bir kişi veya kuruluşa karşı alınan takip önlemi yasal eylem (ya sivil hukuk ya da ceza hukuku) içerdiğinde, ilgili yargılama kurallarında belirlenmiş olan kanıt	UYGULANACAK	Tüm kanıtlar gerekli mercilere ulaştırılacaktır.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
115		17.1.1.	Bilgi Güvenliğini Sürekliliğinin Planlanması	Önemli iş süreçlerinde yaşanan kesintileri ya da beşerîsizlikleri takiben iş operasyonlarını sürdürmek ya da onarmak ve bilginin gerekli seviyede ve gerekli zaman ölçeklerinde kullanılabilirliğini	UYGULANACAK	Bilgi güvenliğinin sürekliliği için yedeller her zaman alınacak ve prosedürler takip edilecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
116		17.1.2.	Bilgi Güvenliğini Sürekliliğinin Uygulanması	Kuruluş genelinde iş sürekliliği için, bu amaçla ihtiyaç duyulan bilgi güvenliği gereksinimlerini ifade eden bir yönetilen proses geliştirilmeli ve sürdürülmektedir.	UYGULANACAK	Bilgi güvenliği ihtiyacı duyulan personellere yardım edilecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
117		17.1.3.	Bilgi Güvenliğini Sürekliliğinin Doğrulanması, Gözden Geçirilmesi Ve Değerlendirilmesi	İş sürekliliği planları, güncel ve etkili olmalarını sağlamak için, düzenli olarak test edilmiş ve güncelleştirilmiştir.	UYGULANACAK	Sürekli güncelleme ve etkili testler gerçekleştirilecektir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
118		17.2.1.	Bilgi İşleme Olanaklarının Erişilebilirliği	Bilgi işleme olanaklarının kullanımını izlemek için prosedürler oluşturulmalı ve izleme faaliyetlerinin sonuçları düzenli şekilde gözden geçirilmelidir.	UYGULANACAK	Gerekli prosedürler mevcut olup revizyonlar edilecektir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
119		18.1.1.	Uygulanabilir Yasaları Ve Sözleşmeye Tabii Gereksinimleri Tanımlama	İlgili tüm yasal, düzenleyici ve sözleşmeden doğan gereksinimleri ve kuruluşun bu gereksinimleri karşılama yaklaşımı her bilgi sistemi ve kuruluş için açıkça tanımlanmış dokümanla edilmiş ve güncel tutulmaktadır.	UYGULANACAK	Avukatlar ile beraber tüm sözleşmeler yazılmış olup sorun teşkil etmemektedir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
120		18.1.2.	Fikri Mülkiyet Hakları	Fikri mülkiyet haklarına göre materyallerin kullanımı ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalarla doğan gereksinimlere uyum sağlamak için uygun	UYGULANACAK	Fikri mülkiyet hakları mevcut değildir.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı

Görsel 1.20

10				UYGULANACAK/ UYGULANMAYACAK	Açıklamalar (Uygulanmayacaksa Nedeni)	Kontrollerin Etkinliği	Etkinlik Ölçümü					
11												
12	Başlık	Bölüm	Kontrol Başlığı	Kontrol		İşletme İçerisinde Gerçekleştirilen Uygulamalar	Etkinliği Ölçülmesi	2024 Temmuz	2024 Ekim	2024 Ocak	2024 Nisan	2024 Temmuz
122		18.1.4.	Kişi Tespit Bilgisinin Gizliliği Ve Korunması	Uygun yasa, düzenlemeler ve varsa anlaşma maddelerinde belirtildiği gibi veri koruma ve gizlilik sağlanmaktadır.	UYGULANACAK	Uygun yasa ve düzenlemeleri takibe konu avukatlar takip edecektir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
123		18.1.5.	Kriptografik Kontrollerin Düzenlenmesi	İlgili tüm sözleşmeler, yasalar ve düzenlemelerle uyum için kriptografik kontroller kullanılmalıdır.	UYGULANACAK		Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
124		18.2.1.	Bilgi Güvenliğinin Bağımsız Gözden Geçirilmesi	Kuruluşun bilgi güvenliği yönetimi ve yaklaşımı ve gerçekleştirilmesi, belirli aralıklarla veya güvenlik gerçekleştirilmesinde önemli değişiklikler olduğunda bağımsız şekilde gözden geçirilmektedir.	UYGULANMAYACAK	Bilgi güvenliği elemanları bağımsız bir şekilde gözden geçirecek tüm prosedürleri.	Yeterli	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapıldı
125		18.2.2.	Güvenlik Politikaları ve Standartları ile Uyum	Yöneticiler, güvenlik politikaları ve standartlarla uyumu sağlamak için sorumluluk alanlarındaki tüm güvenlik prosedürlerinin doğru olarak gerçekleştirilmesi sağlanmaktadır.	UYGULANACAK	Güvenlik politikaları ile standartları uygun bir şekilde uyumlu hale getirilmiştir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak
126		18.2.3.	Teknik Uyum gözden geçirilmesi	Bilgi sistemleri, güvenlik gerçekleştirme standartlarıyla uyumlu olması için düzenli aralıklarla kontrol edilmektedir.	UYGULANACAK	Uyumluluk söz konusu olduğundan gerekli kontroller emir gelinceye kadar kontrolü gerek görülmemiştir.	Yetersiz	Yapılacak	Yapılacak	Yapıldı	Yapıldı	Yapılacak

Uygulama bildirgesi amacına uygun bir şekilde düzenlendi ve dolduruldu. Kontroller düzenli olarak denetimi sağlandı ve işlenmiştir.

KAYNAKÇA

Projede Örnek Oluşturması İçin Verilen Dosyalar

-Tehdit Olasılık Listesi

-Açıklık Listesi

-Risk Kütüğü

-Amaç Kapsam Ve Politika

<https://www.certby.com/iso-iec-27001e-gecis-kemerlerinizi-baglayin-ucusa-basliyoruz/>

<https://www.sezginkoyun.com/rekabet-avantaji-turleri/>

<https://www.adlbelge.com/iso-27001-belgesi-nedir-nasil-alinir>

<https://www.bsigroup.com/tr-TR/ISO-27001-Bilgi-Guvenligi-Yonetimi/iso-27001-nedir/>