BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ EL KİTABI

DOKÜMAN NO: BGYSEK

YAYIM TARİHİ: 11.04.2018

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ EL KİTABI

İÇİNDEKİLER

HAZIRLAYAN	ONAYLAYAN	ONAY TARİHİ
Bilgi İşlem Sorumlusu Mehmet YALÇIN	**Genel Müdür Yardımcısı Yusuf KAYA**	**11.04.2018**

HAZIRLAYAN	ONAYLAYAN	ONAY TARİHİ
Bilgi İşlem Sorumlusu Mehmet YALÇIN	Genel Müdür Yardımcısı Yusuf KAYA	11.04.2018

FİRMA TANITIMI

Firma Adı	:	Kayalar Pres Döküm San. Tic. Ltd. Şti.
Faaliyet Gösterdiği Sektör	:	Yapı Malzemeleri
Kuruluş Tarihi	:	1970
İletişim Adresi	:	Eyüpsultan Mah. Mezarlık Yolu Sok. No:4/2 PK: 34858 Sancaktepe İstanbul / Türkiye
Telefon No	:	+90 216 311 35 45
Faks No	:	+90 216 311 29 61
E-Mail Adresi	:	info@kas.com.tr
Web Site Adresi	:	www.kas.com.tr

TARİHÇE

Kayalar, üretim faaliyetlerine 1970 yılında başlamıştır. Daha sonra Kayalar Pres Döküm San. ve Tic. Ltd. Şti. adı altında pirinçten mamul parça ve fittings üretimine devam etmiş, 1994 yılında da KAS markasını tescil ettirmiştir. 1999 yılında İstanbul Sancaktepe'de bulunan 12.000 m² kapalı alana sahip üretim tesisine yerleşerek ürün çeşidini ve üretim kapasitesini artırmıştır. Firmamız halen bu tesiste hizmet vermeye devam etmektedir. Kayalar, büyüme stratejisi doğrultusunda; 2004 yılında esnek bağlantı hortumları, 2009 yılında plastik boru ve bağlantı parçaları ile 2010 yılında ise armatür üretimine başlayarak ürün gamını genişletmiştir.

1. KAPSAM

Bilgi Güvenliği Yönetim Sistemi El Kitabı'nda, TS ISO/IEC 27001:2013 kapsamındaki çalışmalar anlatılmaktadır. Bilgi Güvenliği Yönetim Sisteminin amacı; bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartların oluşturulmasıdır.

Kayalar, TS ISO/IEC 27001:2013 BGYS kapsamında hazırlanan Bilgi Güvenliği Yönetim Sistemi'ni tüm faaliyet alanları için uygulamaya koymuştur. Kayalar, TS ISO/IEC 27001:2013 Standardı'na uygun bir Bilgi Güvenliği Yönetim Sistemi kurmuştur. Kurulan Bilgi Güvenliği Yönetim Sistemi, el kitabında yer alan faaliyetleri kapsamakta ve bu faaliyetlere göre denetlenerek sertifikalandırılmaktadır.

Kayalar, bilgi güvenliği konularında birimlerinin gerçekleştireceği faaliyetler ve bunlara ilişkin izlenecek yöntemler ile detaylarını bu kitapta atıflarına yer verilen prosedür, talimat, form vb. dokümante edilmiş bilgilerle belirlemiştir.

2. ATIF YAPILAN STANDARD VE/VEYA DOKÜMANLAR

Kayalar, Bilgi Güvenliği Yönetim Sistemi El Kitabı'nın hazırlanmasında ve Bilgi Güvenliği Yönetim Sisteminin oluşturulmasında; TS EN ISO/IEC 27001:2013 standardını referans alınmıştır.

3. TERİMLER VE TARİFLER

Bu el kitabında ISO/IEC 27000 standardında verilen terimler ve tarifler uygulanmıştır.

HAZIRLAYAN	ONAYLAYAN	ONAY TARİHİ
Bilgi İşlem Sorumlusu Mehmet YALÇIN	Genel Müdür Yardımcısı Yusuf KAYA	11.04.2018

4. KURULUŞUN BAĞLAMI

4.1. Kuruluş ve bağlamının anlaşılması

Kayalar, amaçları ile ilgili olan ve bilgi güvenliği yönetim sisteminin hedeflenen sonucuna/sonuçlarına ulaşabilme yeteneğini etkileyen, iç ve dış hususları tayin etmiştir;

⇒ Ürünlere ilişkin teknik veriler, çalışanlar, yazılım/donanım altyapısı ve ihtiyaçları, fiziksel ortamlar vb. gibi iç hususlar ile

⇒ Tedarikçi firmalar, müşteriler, sistem güvenliğini tehlikeye sokabilecek saldırı, doğal afet gibi durumlar, kamu kurum ve kuruşları gibi dış hususlardan oluşmaktadır.

İlgili hususlara ilişkin bilgiler, Üst Yönetim tarafından organize edilen toplantılar doğrultusunda yıllık periyotlarda değerlendirilerek, gözden geçirilmektedir.

4.2. İlgili tarafların ihtiyaç ve beklentilerinin anlaşılması

Kayalar, Bilgi Güvenliği Yönetim Sistemi ile ilgili tarafları; çalışanlar, müşteriler, tedarikçi firmalar, kamu kurum ve kuruşları vb. olarak belirlemiştir. İlgili tarafların Bilgi Güvenliği Yönetim Sistemine yönelik ihtiyaç ve beklentileri, Risk Analizi, İç Denetim, İyileştirme faaliyetleri, Sözleşmeler vb. çalışmalar doğrultusunda tespit edilerek gerekli güncelleme çalışmaları yapılmaktadır. İlgili tarafların gereksinimleri genel olarak aşağıdaki gibidir;

İlgili Taraf	Beklentiler
Kayalar Tüzel Kişiliği	- Yasal yükümlülüklere uygun çalışma - Prestijinin korunması - Bilgi birikiminin korunması
Çalışanlar	- Kişisel bilgilerinin korunması - Bilişim suçlarına karşı koruma
Müşteriler	- Bilgilerinin korunması - Sözleşmeler doğrultusunda oluşacak yükümlülükler
Tedarikçi Firmalar	- Sözleşmeler doğrultusunda oluşacak yükümlülükler
Kamu Kurum ve Kuruluşları	- Yasal yükümlülüklerin yerine getirilmesi

4.3. Bilgi güvenliği yönetim sisteminin kapsamının belirlenmesi

Kayalar, Bilgi Güvenliği Yönetim Sisteminin kapsamı aşağıdaki gibidir;

"Vana, kollektör, yerden ısıtma grupları, su ve doğalgaz ürünleri, paslanmaz çelik esnek hortum ve bağlantı elemanları, armatür, ppr boru, plastik boru ve ek parçaları vb. yapı malzemelerinin; tasarım, üretim, montaj, satış ve pazarlaması ile gümrük ve dış ticaret işlemlerini ve bu işlemlerine ilişkin lojistik, depolama, muhasebe, finans ve bilgi işlem faaliyetlerinin bilgi varlıkları ile bu varlıkları korumak amacıyla kullandığı güvenlik önlemlerini"

Standart doğrultusunda kapsam dışı bırakılmış madde bulunmamaktadır.

HAZIRLAYAN	ONAYLAYAN	ONAY TARİHİ
Bilgi İşlem Sorumlusu Mehmet YALÇIN	Genel Müdür Yardımcısı Yusuf KAYA	11.04.2018

4.4. Bilgi güvenliği yönetim sistemi

Kayalar, bu standardın şartları çerçevesinde bir bilgi güvenliği yönetim sistemini kurmuş, uygulamakta ve sürekli iyileştirmektedir. Oluşturulan bu yapının sürekliliğini sağlamak amacıyla;

- ⇒ Bu standardın şartlarına uygun olarak, ihtiyaç duyulan prosesler ve bunların birbiri ile etkileşimi doğrultusunda; Bilgi Güvenliği Politikası, Bilgi Güvenliği Yönetim Sistemi El Kitabı, Talimatlar, Formlar vb. dokümanları baz alarak bir yapı oluşturmuştur.
- ⇒ Sistemin etkili işletimi ve kontrolünü güvence altına almak için ihtiyaç duyulan ilgili performans kriterleri tayin edilmiş,
- ⇒ İhtiyaç duyulan kaynaklar tayin edilmiş,
- ⇒ Yetki ve sorumlulukları belirlenmiş,
- ⇒ Madde 6.1'in şartlarına göre tayin edilmiş risk ve fırsatlar belirlenmiştir.

Dokümantasyon genel olarak elektronik ortamda oluşturulmaktadır. Dokümanların oluşturulmasına yönelik kurallar P.01 Dokümante Edilmiş Bilginin Sağlanması Prosedüründe, arşivlenmesi ise P.02 Dokümante Edilmiş Bilginin Muhafazası Prosedüründe yer almaktadır.

5. LİDERLİK

5.1. Liderlik ve bağlılık

Kayalar, Üst yönetimi tanımlanan Bilgi Güvenliği Yönetim Sisteminin uygulanması, geliştirilmesi, etkinliğinin ve sürekliliğinin sağlanması için aşağıda yer alan konuları yerine getirerek bağlılık göstermiştir;

- ⇒ Firmamızın stratejik yönü ve Bilgi Güvenliği Yönetim Sistemi amaçlarımız baz alınarak bir Bilgi Güvenliği Politikası belirlenmiş,
- ⇒ Bilgi güvenliği yönetim sisteminin sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan kaynakları tayin etmiş,
- ⇒ Etkin Bilgi Güvenliği Yönetimi ve Bilgi Güvenliği Yönetim Sistem şartlarına uygunluğun öneminin paylaşılması kapsamında ilgililer eğitim, sözleşme, iç denetim vb. çalışmalar yoluyla bilgilendirilmekte,
- ⇒ Bilgi güvenliği yönetim sisteminin hedeflenen çıktılarının başarılması ile ilgili olarak performans hedefleri belirlenmiş ve izlenmekte
- ⇒ Bilgi güvenliği yönetim sisteminin etkinliğine katkı sağlamaları için kişilerin yönlendirilmesi ve desteklenmesi amacıyla gerekli eğitimler verilmiş,

⇒ Bilgi Güvenliği Yönetim Sistemi ile ilgili kendi sorumluluk alanlarında liderliklerini sergileyebilmeleri için diğer ilgili yönetim rolleri belirlenerek Görev Tanımları aracılığıyla desteklenmiştir.

5.2. Politika

Bilgi Güvenliği Politikası

Kayalar üst yönetimi tarafından, firma ve bilgi güvenliği amaçlarımızla uyumlu şekilde aşağıda yer alan Bilgi Güvenliği Politikası oluşturulmuştur;

Şirketimiz bünyesinde yürütülen tüm faaliyetlere ilişkin bilgi, kayıt ve sistemlerin Gizliliği, Bütünlüğü ve Kullanılabilirliğini korumak ve bunlara ilişkin izlenebilirliği sağlamak amacıyla;

- ⇒ **Bilgi varlıklarına ilişkin olası riskleri, sistematik olarak değerlendirme ve yönetmeyi,**
- ⇒ **Bilgi güvenliği ile ilgili standart ve yasal şartların gereklerini yerine getirmeyi,**
- ⇒ **Bilgi güvenliği yönetim sisteminin sürekli olarak iyileştirilmesi için gerekli çalışmaları gerçekleştirmeyi taahhüt etmekteyiz.**

Bilgi Güvenliği Politikamız; şirket personelleri, tedarikçi firmalar, yasalar ve diğer yükümlülükler gereği sorumlu olduğumuz kamu kurum ve kuruluşları ile hizmet verdiğimiz müşteriler gibi tüm ve iç dış paydaşlarımızı kapsamaktadır.

Bilgi Güvenliği Politikası, tüm çalışanların bilgilendirilmesi amacıyla oryantasyon eğitimlerinde anlatılmakta, işletmenin çeşitli noktalarına asılarak çalışanlara duyurulmaktadır. Ayrıca tüm paydaşların bilgisine sunulmak amacıyla www.kas.com.tr web adresinde yayımlanmaktadır.

5.3. Kurumsal görev, yetki ve sorumluluklar

Üst yönetim, Bilgi Güvenliği Yönetim Sistemi ile ilgili olarak gerçekleştirilecek faaliyetler ve rollere ilişkin organizasyonel yapılanmayı kurmuş, gerekli görev tanımlarını oluşturarak yetki ve sorumlulukları tanımlamıştır. Bu dokümanları elektronik ortamda sürekli erişime açık halde tutmaktadır. Bu doğrultuda aşağıdaki çalışmalar gerçekleştirilmiştir;

Ayrıca Bilgi Güvenliği Yönetim Sisteminin performansı, iyileştirilmesi ve ilgili raporların oluşturulması amacıyla Bilgi Güvenliği Yönetim Sistemi Temsilcisi görevlendirilmiştir.

6. PLANLAMA

6.1. Risk ve fırsatları ele alan faaliyetler

6.1.1. Genel

Kayalar, Bilgi Yönetim Sistemini planlarken kuruluşun bağlamı ve kapsamını göz önüne alarak risk ve fırsatlarını belirlemiştir. İlgili çalışmada bu hususlardan etkilenecekler ve ne şekilde etkilenebilecekleri göz önünde bulundurulmuştur. Risk ve fırsatların belirlenme çalışmaları Bilgi İşlem Bölümü öncülüğünde ilgili bölümlerle görüşmeler, bölümlerden gelen iyileştirme talepleri, iç denetimler vb. sonucunda ortaya çıkmıştır. Risk ve fırsatlar, Bilgi Güvenliği Yönetim Sisteminin amaçlanan çıktılarına ulaşabilmesi için istenen etkileri geliştirmek, istenmeyen etkileri önlemek veya azaltmak, iyileşmeye erişimi amaçlamaktadır. Bu doğrultuda **FR.358 Risk Değerlendirme - Fırsat Tablosu** hazırlanmıştır.

6.1.2. Bilgi güvenliği risk değerlendirmesi

Bilgi güvenliği yönetim sistemi kapsamı dâhilindeki bilginin gizlilik, bütünlük ve erişilebilirlik kayıpları ile ilgili risklerin tespit edilmesi için risk değerlendirme çalışmalarını gerçekleştirmektedir. Bu doğrultuda riskler; tehlikelerin ortaya çıkma olasılık puanı, gerçekleşmeleri durumunda oluşacak sonucun şiddet düzeyleri ve varlık değeri puanlarının çarpılmasıyla hesaplanır ve Risk Değerlendirme Tablosu ilgili sütununa işlenir. Bu hesaplamalarda kullanılacak puanlar Risk Puanı Hesaplama ve Değerlendirme Tablolarından yararlanılarak belirlenmektedir. Riskin azaltılması ya da kabul edilebilir seviyeye indirgenmesi için sorumlular tanımlanarak aksiyonlar belirtilmektedir. Aksiyonların gerçekleştirilmesi çalışmaları için en yüksek risk seviyesinden başlanarak en düşük risk seviyesine kadar tüm risklere ilişkin zaman planlaması yapılmaktadır. Aksiyon çalışmaları tamamlandıktan sonra kalıntı risk değerlendirmesi yapılmaktadır. Risk seviyesi kabul edilebilir düzeye indirilemediyse tehlike ile ilgili ilave aksiyonlar belirtilerek tablo güncellenmektedir. Seviye kabul edilebilir düzeye indirilene kadar bu işlem tekrarlanmaktadır. Aksiyonlar, Bilgi İşlem Bölümü tarafından ilgili termin tarihleri baz alınarak takip edilerek **FR.358 Risk Değerlendirme - Fırsat Tablosu'**na işlenmektedir. BGYS Temsilcisi, risk işleme sonrası kalan risklere ilişkin üst yönetim onayını alarak artık riske ilişkin durumu bir tutanak ile kayıt altına alır.

HAZIRLAYAN	ONAYLAYAN	ONAY TARİHİ
Bilgi İşlem Sorumlusu Mehmet YALÇIN	Genel Müdür Yardımcısı Yusuf KAYA	11.04.2018

6.1.3. Bilgi güvenliği risk işleme

Kayalar, TS ISO/IEC 27001:2013 standardı Ek A da belirtilen kontrolleri baz alarak bir Uygulanabilirlik Bildirgesi hazırlamıştır. Bu bildirge ile standardın kontrol edilmesini istediği tüm kriterler gözden geçirilmektedir. Kontrollerde dışarıda bırakılan kısımlar Kapsam Dışı olarak belirtilmekte ve gerekli açıklamalar bildirgeye yazılmaktadır.

6.2. Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama

Kayalar, Bilgi Yönetim Sistemi için ihtiyaç duyulan seviyelerde bilgi güvenliği politikası ile uyumlu, standartlar ve yasal şartları kapsayacak şekilde amaç ve hedeflerini oluşturmaktadır. Oluşturulan amaç ve hedefler, yıllık periyotlarda yayımlanarak, ilgililere duyurulmaktadır. Oluşturulan amaç ve hedeflere; kod, performans göstergesi, hedef değeri, ölçü birimi, ölçüm periyodu, önceki yıllara ilişkin gerçekleşme bilgileri, tamamlanma tarihi ve kaynak ihtiyacı gibi bilgiler yer almaktadır. Listede yer alan tüm hedef/göstergeler sayısal ifadelerle tanımlanmış olup ölçülebilir durumdadır. Hedefler, tamamlanma tarihleri baz alınarak BGYS Temsilcisi tarafından izlenerek Üst Yönetim'e raporlanmaktadır. Ayrıca, Yönetimin Gözden Geçirme Toplantılarında hedeflerin ulaşılma durumları değerlendirilmekte ve bir sonraki dönemin hedefleri belirlenmektedir. Amaçlara ulaşmak için tanımlamalar oluşturulmuş olup; neler yapılacağı, ilgili kaynaklar ve sorumluların kimler/neler olduğu ve faaliyetlerin ne zaman tamamlanacağı ile sonuçların nasıl değerlendirileceği bu tanımlamalarda belirtilmiştir.

7. DESTEK

7.1. Kaynaklar

Kayalar, Bilgi Güvenliği Yönetim Sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan kaynakları; insan kaynakları, altyapı kaynakları (binalar ve ilgili müştemilat, donanım, taşıma kaynakları, bilgi ve iletişim teknolojileri vb.) şeklinde tanımlamıştır.

Kayalar bu doğrultuda Bilgi Güvenliği Yönetim Sisteminin etkili şekilde işletilmesi ve kontrolü için gerekli personeli belirleyerek tedarik etmektedir. İnsan kaynağının sürekliliğinin sağlanması amacıyla; **P.08 İnsan Kaynakları Prosedürü** oluşturulmuş ve uygulanmaktadır.

Altyapı kaynakları ile ilgili olarak **FR.383 Varlık Envanteri Formu** oluşturulmuş olup BGYS Temsilcisi tarafından takip edilmektedir. Fiziksel Alanlar ve Çevresel Güvenlik ile ilgili gerekli bakım işlemleri için **FR.25 Makine Koruyucu Bakım Fiş**leri oluşturulmuş ve BGYS Temsilcisi tarafından izlenmektedir. Ayrıca, **T.559 Bilgi İşlem Talimatı** doğrultusunda da bilgi işlem altyapısı, donanım, bakım onarım vb. ihtiyaçlar karşılanmaktadır.

7.2. Yeterlilik

Kayalar, Bilgi Güvenliği Yönetim Sisteminin performansını ve etkinliğini etkileyen kendi kontrolü altında çalışan kişi/kişilere yönelik rolleri belirlemiştir. Bu rollere ilişkin gerekli nitelik ve yetkinlikleri Görev Tanımlarında belirtmektedir. Çalışanların eğitim ihtiyaçlarının belirlenmesi, giderilmesi ve eğitim etkinliklerinin değerlendirilmesi amacıyla **YS.02 Eğitim Sürecini** uygulamaktadır. Ayrıca, BGYS Temsilcisi tarafından bilgi güvenliği konularını kapsayan yıllık **FR.18 Eğitim Planları** hazırlanarak Üst Yönetim onayına sunulmakta ve uygulanmaktadır. Eğitim faaliyetleri sonucunda oluşan kayıtlar İnsan Kaynakları Bölümü tarafından kişilerin özlük kayıtlarına eklenerek arşivlenmekte/izlenmektedir.

7.3. Farkındalık

Kayalar, kontrolü altında çalışan kişilere aşağıda yer alan konularda eğitici uygulamaları planlamakta ve gerçekleştirmektedir;

⇒ Bilgi güvenliği politikası
⇒ Bilgi Güvenliği Yönetim Sistemi açısından yapacağı çalışma ve katkılar

HAZIRLAYAN	ONAYLAYAN	ONAY TARİHİ
Bilgi İşlem Sorumlusu Mehmet YALÇIN	Genel Müdür Yardımcısı Yusuf KAYA	11.04.2018

⇒ Bilgi Güvenliği Yönetim Sistemi şartlarını yerine getirmeme durumunda sorumluluk

Bu eğitici uygulamalar işe giriş aşamasında **FR.78 Oryantasyon ve İşbaşı Eğitim Takip Formu** ile olabileceği gibi gerekli görüldüğü durumlarda bilgilendirme şeklinde de yapılabilmektedir.

7.4. İletişim

Kayalarda iletişim aşağıdaki gibi gerçekleştirilmektedir;

⇒ Kurum içi iletişim; duyuru panoları, toplantılar, e-mail, telefon vb. ile
⇒ Bilgi Güvenliği ile ilgili acil durumlarda **T.559 Bilgi İşlem Talimatı** doğrultusunda ilgili kişiler ile
⇒ Otoriteler ve Özel İlgi Grupları ile iletişim; Her bölüm kendi sorumluluk alanına giren konularda üst yönetimin bilgisi dahilinde **FR.385 Otoriteler ve Özel İlgi Grupları İle İletişim Formu** doğrultusunda iletişim kurulmaktadır.

İç ve dış iletişime geçilecek kişi/kurum bilgileri ERP programında kayıt altına alınmakta olup güncelliği sağlanmaktadır.

7.5. Yazılı bilgiler

7.5.1. Genel

Kayalar, Bilgi Güvenliği Yönetim Sisteminin genel işleyişi ve bilgileri, kapsamı, Bilgi Güvenliği Yönetim Sistemi için oluşturulan prosedür, talimat ve formlara atıfta bulunan Bilgi Güvenliği Yönetim Sistemi El Kitabını hazırlamıştır.

7.5.2. Oluşturma ve güncelleme

Bilgi Güvenliği Yönetim Sistemi dahilinde uygulamadaki tüm dokümante edilmiş bilgilerin hazırlanması, yayımlanması, dağıtımı, revizyonu ve yürürlükten kaldırılması işlemleri **P.01 Dokümante Edilmiş Bilginin Sağlanması Prosedürü** doğrultusunda gerçekleştirilmektedir. Ağlar üzerinde yazılı bilgi oluşturup, güncelleme işlemlerine ilişkin **T.784 Erişim Kontrolü Talimatı** oluşturulmuş ve uygulanmaktadır.

7.5.3. Yazılı bilgilerin kontrolü

Dokümante edilmiş bilgi; evrak üzerinde tutulabildiği gibi elektronik ortamda da saklanabilmekte/tutulabilmektedir. Sanal ortamda tutulan bilgiler belirli aralıklarla **T.03 Yedek Alma Talimatı** doğrultusunda yedekleme işlemine tabi tutulmaktadır.

Kayalar, dokümante edilmiş bilginin muhafazası amacıyla **P.02 Dokümante Edilmiş Bilginin Muhafazası Prosedürü** uygulamaktadır. Bu prosedür doğrultusunda bilginin saklanması, korunması, elden çıkarılması ve muhafaza edilme sürelerinin belirlenmesi ile ilgili bir sistem kurulmuştur.

8. İşletim

8.1. İşletimsel planlama ve kontrol

Kayalar bilgi güvenliği şartlarını karşılamak, risk ve fırsatlar doğrultusunda yapılacak olan faaliyetleri gerçekleştirmek için gerekli olan dokümantasyonlar, insan ve fiziki altyapı kaynaklarını sağlamakta, bunlara ilişkin uygulamaları yürütmekte ve düzenli periyotlarda kontrollerini gerçekleştirmektedir. Bunların yanı sıra Bilgi Güvenliği Amaçlarına ulaşmak için gerekli planlamaları yaparak uygulamaktadır.

Firmamız, planlanan değişiklikleri kontrol etmekte, istenmeyen durumların sonuçları ile olumsuz etkilerini azaltıcı faaliyetler uygulanmaktadır. Bu vb. durumlarda risk analizi çalışmaları güncellenmektedir.

Firmamızda, dış kaynaklı proses olarak ERP, E-mail, Web Hosting, PDKS ve Firewall ürünleri ile ilgili tedarikçi firmalardan destek alınmaktadır. Tüm tedarikçiler ile gizlilik sözleşmeleri yapılarak kayıt altına alınmaktadır.

8.2. Bilgi güvenliği risk değerlendirme

Firmamız, bölümlerden gelen iyileştirme talepleri, iç denetimler, kaynak ihtiyaçları, doğal afetler, dış tehditler vb. sonucunda yeni risklerin ortaya çıkması durumlarında **FR.358 Risk Değerlendirme - Fırsat Tablosu** güncellenmektedir. Ayrıca bu tablo, yıllık periyotlarda Yönetim Gözden Geçirme Toplantısında ele alınmakta ve gözden geçirilmektedir. Risk değerlendirme çalışmalarına ilişkin kayıtlar **P.02 Dokümante Edilmiş Bilginin Muhafazası Prosedürü**'ne uygun şekilde arşivlenmektedir. Ayrıca **FR.387 Uygulanabilirlik Bildirgesi Formu** yılık periyotlarda gözden geçirilerek standarda uygunluk durumu değerlendirilmektedir.

8.3. Bilgi güvenliği risk işleme

Kayalar, bilgi güvenliğine ilişkin riskleri **FR.358 Risk Değerlendirme - Fırsat Tablosu'**na işlemekte olup bu çalışmalara ilişkin kayıtları **P.02 Dokümante Edilmiş Bilginin Muhafazası Prosedürü**'ne uygun şekilde arşivlenmektedir. Artık risklerin oluşması durumunda Üst Yönetim onayı alınarak (tutanak, antetli kağıt vb.) bu risk ile çalışmaya devam edilebilmektedir.

9. Performans değerlendirme

9.1. İzleme, ölçme, analiz ve değerlendirme

9.1.1. Genel

Kayalar, Bilgi Güvenliği Yönetim Sisteminin performansı ve etkinliğini izlemek, ölçmek ve iyileştirmek amacıyla aşağıda belirtilen uygulamaları gerçekleştirmektedir;

- ⇒ İç tetkikler,
- ⇒ Paydaş analizleri,
- ⇒ Risk değerlendirmeleri,
- ⇒ Amaçlara ulaşma dereceleri,
- ⇒ Düzeltici/önleyici faaliyetler.

Bu uygulamalar çeşitli periyotlarda (günlük, haftalık, aylık, yıllık vb.) tekrarlanmakta olup bunlar sonucunda oluşan uygunsuzluklar aksiyon planları doğrultusunda hızlı bir şekilde giderilmektedir. Tüm bu çalışmalara ilişkin ortaya çıkan kayıtlar **P.02 Dokümante Edilmiş Bilginin Muhafazası Prosedürü**'ne uygun şekilde arşivlenmektedir.

9.2. İç tetkik

Kayalar, Bilgi Güvenliği Yönetim Sisteminin planlanmış düzenlemelere ve TS ISO/IEC 27001:2013 Standardına uygunluğunu ve etkinliğini periyodik olarak doğrulanmak, uygunsuzluklar için düzeltici faaliyetleri belirlenmek ve iyileştirme alanlarını tespit etmek amacıyla **P.03 İç Denetim Prosedürü'**nü hazırlanmış ve uygulamaktadır. İlgili prosedür; sorumlulukları, tetkiklerin planlanarak yerine getirilme gereklilikleri ile sonuçlarının raporlanmasını ve dokümante edilmiş bilgilerin muhafaza edilmesi konularını tarif etmektedir.

İç Tetkikler yılda 1 defa yapılmaktadır. Bilgi Güvenliği Yönetim Sistemi Sorumlusu her yıl iç tetkik planını hazırlayarak, yıl içinde tetkiklerin gerçekleştirilmesini sağlamaktadır. Tetkiklerde tespit edilen uygunsuzluklar ile ilgili faaliyetler ve uygunsuzlukların kapatılmasına ilişkin esaslar; **P.05 Düzeltici Faaliyetler Prosedürü'**nde açıklanmaktadır.

9.3. Yönetimin gözden geçirmesi

Kayalar üst yönetimi, Bilgi Güvenliği Yönetim Sistemi'nin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için yılda 1 defa **YP.01 Yönetim Süreci**'ne uygun olarak gözden geçirme toplantısını gerçekleştirmektedir.

Toplantıların gündemi önceden belirlenmekte olup gündem maddeleri aşağıdaki gibidir;

- ⇒ Önceki YGG toplantı sonuçları
- ⇒ BGYS sistemini etkileyebilecek iç ve dış konulardaki değişiklikler
- ⇒ BGYS performans ve etkinliği
  - Uygunsuzluklar ve düzeltici faaliyetler
  - İzleme ve ölçme sonuçları
  - Denetim sonuçları
  - Bilgi güvenliği amaçlarına ulaşma durumu
- ⇒ İlgili taraflardan geri bildirim
- ⇒ Risk değerlendirme sonuçları
- ⇒ İyileştirme için öneriler

Gözden geçirme toplantı sonuçları ve alınan kararlar, Bilgi Güvenliği Yönetim Sistemi Sorumlusu ve/veya yönetimin atayacağı kişi tarafından alınan kararlar ve ilgili eylemleri içeren bir toplantı tutanağı ile toplantıya katılanlara ve gerek görülen kişilere duyurulmaktadır. Toplantı tutanakları **P.02 Dokümante Edilmiş Bilginin Muhafazası Prosedürü**'ne göre muhafaza edilmektedir. Toplantı çıktıları; İyileştirme için fırsatlar ile Bilgi Güvenliği Yönetim Sistemi ile ilgili değişiklik ihtiyacı gibi konuları içermektedir.

HAZIRLAYAN	ONAYLAYAN	ONAY TARİHİ
Bilgi İşlem Sorumlusu Mehmet YALÇIN	Genel Müdür Yardımcısı Yusuf KAYA	11.04.2018

10. İyileştirme

10.1. Genel

Kayalar, Bilgi Güvenliği Yönetim Sistemi'nde, mevcut uygunsuzlukları gözden geçirerek sebeplerinin ortadan kaldırılması amacıyla düzeltici faaliyetlerin planlanması, uygulanması, sonuçların izlenmesi ve tekrarlarının önlenmesi amacıyla **P.05 Düzeltici Faaliyetler Prosedürü**'nü uygulamaktadır. Düzeltici Faaliyetlerin hangi durumlarda kimler tarafından kimlere açılacağı aynı prosedürde anlatılmaktadır. Bu konular şu ana başlıklar altında toplanmıştır;

- ⇒ İç ve dış tetkikler,
- ⇒ Faaliyetler sonucunda saptanan/yaşanan uygunsuzluklar.

Uygunsuzluklar niteliklerine göre; FR.58 İç Denetim Uygunsuzluk Formu veya FR.389 BGYS Olay Kayıt Bildirim Formu doğrultusunda takip edilmektedir. Gerçekleştirilen düzeltici faaliyetlerin etkinliği Bilgi İşlem Bölümü tarafından denetlenmekte, uygunsuzluk giderildiyse kapatılmaktadır. Yapılan işlemlerle ilgili dokümante edilmiş bilgiler **P.02 Dokümante Edilmiş Bilgilerin Kontrolü Prosedürü** doğrultusunda muhafaza edilmektedir.

10.2. Sürekli iyileştirme

Kayalar, Bilgi Güvenliği Yönetim Sisteminin uygunluğunu, doğruluğunu ve etkinliğini sürekli iyileştirmektedir. Bu doğrultuda **P.09 Sürekli İyileştirme Prosedürü** oluşturulmuş ve uygulanmaktadır. Prosedür kapsamında; analiz ve değerlendirme sonuçları ile yönetimin gözden geçirme toplantısı çıktıları ihtiyaç ve fırsatların belirlenmesi için değerlendirilmektedir.