Doküman Adı

Bilgi Güvenliği Politikası

Doküman Kodu	Yayın Tarihi	Revizyon Numarası	Revizyon Tarihi
BG-POL-01	**25.02.2021**	**01**	**25.02.2021**

Hazırlayanlar

İsim Soyisim	Unvan	İmza
Reyyan Aksoy Akkaranfil	Bilgi Güvenliği Yöneticisi	

Onaylar

İsim Soyisim	Unvan	İmza
Özkan Demir	Genel Müdür	

İÇİNDEKİLER

1 AMAÇ

Bu politikanın amacı, hukuka, yasal, düzenleyici, ya da sözleşmeye tabi yükümlülüklere, iç ve dış tarafların her türlü Bilgi Güvenliği Yönetim Sistemi gereksinimlerine ilişkin, Üst Yönetim'in bilgi güvenliği yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri duyurmaktır.

Bilgi Güvenliği Politikası kurumsal bilgi güvenliği ilkelerini ana hatlarıyla belirler. Bilgi Güvenliği Politikası, kurumda bilginin ve işlenme yöntemlerinin güvenli olarak gerçekleştirilmesi amacıyla düzenlemeler yapar.

Bu politika Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında bulunan tüm çalışanları ve bilgi varlıklarını kapsamaktadır.

2 KAPSAM

Bu politika, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında bulunan tüm çalışanları ve bilgi varlıklarını kapsamaktadır.

3 SORUMLULUK

Pisano Üst Yönetimi, Bilgi Güvenliği Politikasının tüm çalışanlara ve ilgili üçüncü taraflara duyurulmasını sağlar.

3.1 Gözden Geçirme

Bu politika periyodik olarak senede bir defa veya gerekli görülen hallerde Bilgi Güvenliği Komitesi tarafından gözden geçirilir.

4 TANIMLAR VE KISALTMALAR

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

Bilgi Varlığı: Kuruluşun sahip olduğu, işlerini aksatmadan yürütebilmesi için gerekli olan dolayısıyla korumakla yükümlü olduğu varlıklardır.

5 REFERANSLAR

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı Madde 5.2 : Politika

6 UYGULAMA

6.1 Üst Yönetim Taahhüdü

Kuruluş Üst Yönetimi bilgi güvenliğinin gerçekleştirilmesi, işletimi, izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi, bilgi güvenliğiyle ilgili uygulanabilir yasal şartların ve ISO/IEC 27001 standardı şartlarının yerine getirilmesi için gerekenin yapılacağını taahhüt eder.

Kuruluş bilgi güvenliği yönetimi ile ilgili olarak aşağıdaki ilkeleri benimsemektedir;

- Müşterilerine ve paydaşlarına sunduğu ürün ve hizmetlere ilişkin faaliyetlerinin güvenliğinin sağlanmasına önem vermektedir.
- Tüm iş süreçlerinin birbiri ile entegre, uyumlu ve dengeli olması hedeflenmektedir. Entegre ve dinamik iş stratejisi bilgi varlıklarının güvenliğini ve sürekliliğini gerekli kılmaktadır.
- Müşteri ve paydaşlarına değer sağlayan ürün ve hizmetlerinin gizlilik, bütünlük ve erişilebilirliğini tehdit edebilecek risklere karşı tedbir almayı ilke edinir.

- Bu politika ve organizasyonun amacı ile uyumlu bilgi güvenliği hedefleri belirlenir ve düzenli aralıklarla uyumluluk ölçülerek, sürekli iyileştirme fırsatları değerlendirilir.

6.2 Bilgi Güvenliği Politikası

Bilgi güvenliği, bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ile mümkündür.

Bilginin;

- Gizlilik gerekliliği, bilginin sadece yetkili kişiler tarafından erişilebilir olmasını,
- Bütünlük gerekliliği, bilgi varlıklarının tam ve doğruluğunun sağlanmasını, yetkisiz değişimlerden korunmasını,
- Erişilebilirlik gerekliliği, bilgi varlıklarının ihtiyaç duyulduğu anda yetkili kullanıcılar tarafından kullanılabilir olmasını ifade eder.

Pisano bilgi güvenliğini sağlamak amacıyla kendi kurumsal işleyişini düzenleyici prensipler oluşturur. Bilgi Güvenliği Politikasının belirlenmesi, güvenlik rollerinin tanımlanması ve ilgili tüm güncellemelerin yapılması Üst Yönetim'in desteği ve tüm birimlerin koordinasyonuyla gerçekleştirilir. Pisano gerekli durumlarda iç ve dış uzmanların görüşüne başvurabilir.

Pisano'da bilgi varlıkları uygun şekilde sınıflandırılır. Varlıkların değerlemesi yapılır ve uygun seviyede kontrol geliştirmek için varlıkların değeri hesaplanır.

6.3 Bilgi Güvenliği Amaçları

Kuruluş yukarıda belirtilen ilkelerden taviz vermeden bilgi güvenliği çalışmalarını aşağıda belirtilen amaçlarla gerçekleştirmeyi hedefler;

- Bilgi Güvenliği Yönetim Sistemi (BGYS), uluslararası olarak kabul edilmiş olan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı şartları doğrultusunda planlanır, gerçekleştirilir ve geliştirilir,
- İlgili kanun ve yönetmeliklere uyumlu hale gelinmesi için gereken çalışmalar yapılır,
- BGYS'nin sürekli iyileştirilmesi için gerekli iç denetim, yönetimin gözden geçirmesi, düzeltici faaliyetler ile risklerin ve fırsatların belirlenmesi için gerekli aksiyonlar yönetim ve yönetimin bilgi güvenliği sorumluluğu verdiği ekipler tarafından sağlanır,
- Bilgi güvenliği ile ilgili tüm rol ve sorumluluklar belirlenir ve yönetim tarafından yetkilendirmeler yapılır,
- Bilgi güvenliği yönetim sistemi çerçevesinde gerekli çalışmaların gerçekleştirilmesi için kaynaklar yönetim tarafından sağlanır,
- Paydaşları ile birlikte kuruluşun rekabet avantajını olumsuz yönde etkileyebilecek maddi ve manevi kayıplar engellenir,
- Bilgi Güvenliği Yönetim Sistemi kapsamı bilgi varlıkları belirlenerek, müşteriler, tedarikçiler ve iş ortakları gibi ilgili tarafların bilgi güvenliği beklentileri değerlendirilerek, varsa yasal ve sözleşmeler yükümlülükler analiz edilerek yönetim tarafından iş stratejileri doğrultusunda belirlenir,
- Bilgi varlıklarının sınıflandırılması ve bu varlıkların gizlilik, bütünlük ve erişilebilirlik değerlendirmesinin yapılabilmesi için varlık envanteri oluşturulur,
- Bilgi güvenliği risklerini yönetmek için risklerini değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirilerek, gerekli tedbirler geliştirilir ve olası riskleri önlemek için çalışmalar gerçekleştirilir,
- Bu politika ve organizasyonun amacı ile uyumlu bilgi güvenliği hedefleri belirlenir ve düzenli aralıklarla uyumluluk ölçülerek, sürekli iyileştirme fırsatları değerlendirilir,
- Çalışan özlük bilgilerinin mahremiyeti sağlanır,
- Müşteri bilgilerinin yetkisiz kişilerin eline geçmesi engellenir,

- Veri bütünlüğü sağlanır,
- Tedarikçi nezdinde bilgi güvenliği sağlanır,
- Operasyonel Know-How'ın sürekli geliştirilmesi ve korunması sağlanır,
- Son kullanıcı bilgi güvenliği farkındalığını ve bu farkındalığın sürekli arttırılması sağlanır,
- Bilgi güvenliğini etkin biçimde yöneterek bilgi güvenliği kaynaklı yaşanabilecek zararlar asgariye indirilir,
- Bilgi güvenliği ihlal olayı yaşama ihtimalini düşürmek için gerekli çalışmalar yapılır, yaşanması durumunda koordineli şekilde yanıt verilir,
- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçilmesi için gerekli düzenlemeler yapılır, geçilemediği durumda hedeflenen kurtarma süresi içerisinde tekrar çalışabilir hale gelmesi sağlanır,
- Bilgi Güvenliği Yönetim Sistemi kapsamında müşterilerimizin bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliği sağlanır. Müşteri ile ilgili kritik iş süreçlerinin devamlılığı sağlanır,
- Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesi sağlanır,
- İnsan kaynakları yönetiminde istihdam öncesi, sırası ve sonrasında güvenliği sağlama açısından kuralların belirlendiği süreçler oluşturulur,
- Güvenli çalışma alanları, ofis alanı, depo gibi kurum içi çalışma bölgelerinde ve kurum çevresinde güvenliğin sağlanması için gerekli önlemlerin alınması sağlanır,
- Tedarikçi ilişkilerinin güvenli bir şekilde yürütülmesi amacıyla; tedarik hizmetlerinin gözden geçirilmesi, meydana gelen değişikliklerin yönetilmesi için prosedür oluşturulur, özellikle bilgi teknolojileri tedarikçileri ile yapılan/yapılacak olan ve bilgi güvenliği risklerinin ifade edildiği anlaşmalarda güvenlik gereksinimleri belirlenir.

6.4 Bilgi Güvenliği Hedefleri

BGYS amaçları kapsamında belirlenen ölçülebilir hedefler, Bilgi Güvenliği Performans Değerlendirme Formu aracılığı ile belirlenir, Performans Değerlendirme ve Sürekli İyileştirme Prosedüründe anlatıldığı gibi değerlendirilir ve izlenir.

7 İLGİLİ KAYITLAR

- Performans Değerlendirme ve Sürekli İyileştirme Prosedürü
- Bilgi Güvenliği Performans Değerlendirme Formu
- BGYS Kapsam Analizi Dokümanı
- BGYS İlgili Taraf Analizi
- Dokümanların ve Kayıtların Kontrolü Prosedürü
- Yönetim Sistemleri Roller ve Sorumluluklar Dokümanı
- Varlık Yönetim Prosedürü
- Risk ve Fırsat Yönetim Prosedürü
- İç Denetim Prosedürü
- Düzeltici Faaliyet Prosedürü
- İnsan Kaynakları Güvenliği Prosedürü
- BGYS Fiziksel ve Çevresel Güvenlik Prosedürü
- Üçüncü Taraf Bilgi Güvenliği Prosedürü
- BT Güvenlik Prosedürü

8 REVİZYON TAKİP ÇİZELGESİ

Revizyon No	Revizyon Tarihi	Güncelleme Yapan	Açıklamalar

01	25.02.2021	Reyyan Aksoy Akkaranfil	İlk yayın
02	02.01.2023	Reyyan Aksoy	Onaycı ismi değiştirilmiştir