

**BİLGİ GÜVENLİĞİ POLİTİKASI**

|  |  |
| --- | --- |
| DOKÜMAN NO | PO.BG.01 |
| REVİZYON NO | 04 |
| YAYIN TARİHİ | 10.05.2018 |
| REVİZYON TARİHİ | 13.03.2025 |

# AMAÇ

Bu politika bilgi güvenliğini yönetim sisteminin nasıl kurulacağını, yönetileceğini, ölçüleceğini ve raporlanacağını açıklar.

Bilgi güvenliği yönetimi için izlenen uluslararası standart TS ISO/IEC 27001’dir ve sistem dokümantasyonunda bundan böyle kısaca ISO/IEC 27001 olarak adlandırılacaktır.

Platin Bilişim Teknoloji Hizmetleri A.Ş. (bundan sonra “Platin Bilişim” olarak anılacaktır), ISO/IEC 27001 sertifikasına sahiptir. Bu sertifikasyon sayesinde, kurumun bilgi güvenliği yönetimi kapsamında yürüttüğü uygulamalar, bağımsız bir kuruluş tarafından doğrulanarak güvence altına alınmıştır.

# KAPSAM

Platin Bilişim bünyesinde kurulan ISO / IEC 27001 Bilgi Güvenliği Yönetim Sisteminin kapsamı **“PR.GN.04 Yönetim Faaliyetleri Prosedürü”** dokümanı içerisinde detaylandırılmıştır.

BGYS Politikası kapsam içerisinde kalan tüm sistem için oluşturulmuştur.

# BİLGİ GÜVENLİĞİ GEREKSİNİMLERİ

Bilgi güvenliği gereksinimlerinin iş fonksiyonlarıyla mutabakata varılması gereklidir, BGYS bu şekilde bu gereksinimleri karşılayabilir. Kanun, yönetmelik ve kontrat gereksinimleri de belirlenip dokümante edilmeli ve planlama aşamasında girdi olarak kullanılmalıdır. Yeni veya değişmiş sistem ve servislerin bilgi güvenliği gereksinimleri tasarım ve planlama aşamasında belirlenmelidir.

BGYS’nin kontrollerinin iş ihtiyaçlarına göre belirlenmesi ve uygulanması, bu kontrollerin düzenli olarak tüm ilgili personele takım toplantıları gibi araçlarla duyurulması temel prensiplerdendir.

# YÖNETİMİ TAAHHÜDÜ

Kurum yönetimi olarak, “Kurum Bilgi Güvenliği Politikası” ‘nın uygulanmasının sağlanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.

Genel Müdür

Ayhan Bamyacı

# HEDEF VE POLİTİKALARI OLUŞTURURKEN KULLANILAN ÇERÇEVE

Bilgi güvenliği hedefleri yıllık olarak, bütçe planlarıyla paralel olarak planlanır. Bu sayede iyileşme aktiviteleri için gerekli kaynağın ayrılması sağlanmış olur. Bilgi güvenliği hedefleri iş hedefleri doğrultusunda, ilgili paydaşların katılımıyla belirlenir.

BGYS hedefleri bir sonraki finansal yıl için, hedeflere nasıl ulaşılacağının ayrıntılarıyla birlikte dokümante edilir. Bu hedefler periyodik olarak gözden geçirilir, bu sayede güncelliği sağlanır. Değişikliklerin gerekmesi durumunda değişiklik yönetim süreciyle bu değişiklikler sağlanır.

# ROLLER VE SORUMLULUKLAR

Bilgi güvenliği alanında, yukarıda sayılan alanlar için bir dizi yönetim rolleri bulunmaktadır. Büyük bir organizasyonda bu roller her alan için ayrı kişiler tarafından yürütülebilir, küçük bir organizasyonda ise bu roller bir takım içinde paylaştırılmalıdır.

Ekibin rollerini anlamalarının ve gerekli beceri ve yetkinliğe sahip olmalarının sağlanması bilgi güvenliği yöneticisi sorumluluğundadır

# RİSK YÖNETİMİ YAKLAŞIMI

Kurumun risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk değerlendirmesi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Bu planın yönetiminden ve gerçekleştirilmesinden Bilgi Güvenliği Yöneticisi ve Üst Yönetim Temsilcisi sorumludur.

BGYS’de risk yönetimi çeşitli seviyelerde gerçekleşir:

* Yönetim planlaması – hedeflerin gerçekleşmesine yönelik riskler
* Bilgi güvenliği risk değerlendirmesi
* Değişiklik yönetimi sürecindeki risklerin değerlendirilmesi

BGYS Risk değerlendirmeler senelik ya da iş ya da servis ortamında önemli değişiklikler olduğunda yeniden gerçekleştirilir.

Bu süreç, **“PR.BG.01 Risk Değerlendirme Prosedürü”** dokümanında ayrıntılandırılmıştır.

# SÜREKLİ İYİLEŞTİRME POLİTİKASI

Platin Bilişim ’in sürekli iyileşmeye ilişkin politikası aşağıda belirtildiği gibidir:

* BGYS’nin etkinliğini sürekli iyileştir
* Var olan süreçleri, ISO/IEC 27001’in gerekliliklerine göre iyileştir
* ISO/IEC 27001 sertifikanın gereklerini yerine getirerek sertifikayı devam ettir
* Bilgi güvenliği ile ilgili proaktif davran
* Servislerin sunulduğu iş birimlerini anla ve onlarla ilişki kur
* Bilgi güvenliği süreç ve kontrollerini ölçülebilir olarak tasarla, bu sayede daha sağlam kararlar almak
* İlgili metrikleri düzenli olarak gözden geçir ve toplanmış veriler ışığında bunları değiştirip değiştirmeyeceğine karar ver
* Paydaşlarla yapılacak toplantılarda, iyileşme için fikir topla ve bunları sürekli iyileştirme planında dokümante et
* Sürekli iyileştirme planını yönetim toplantılarında gözden geçir, zaman planı ve faydaları analiz et ve faaliyetleri önceliklendir.

Geliştirme için öneriler ve fikirler herhangi bir kaynaktan gelebilir. Bu kaynaklar arasında müşteriler, tedarikçiler, BT çalışanları, risk değerlendirmeler ve servis raporları olabilir. Geliştirme faaliyeti tanımlandığında, faaliyet “Sürekli iyileştirme planı” dokümanına eklenir ve sürekli iyileştirme süreci sorumluları tarafından değerlendirilir.

Değerlendirmede aşağıdaki kıstaslar kullanılır:

* Maliyet
* İş faydası
* Risk
* İyileştirmenin ne kadar zamanda tamamlanabileceği
* Kaynak ihtiyacı

Kabul edilmesi durumunda, iyileştirme önerisi önceliklendirilir.

# İNSAN KAYNAKLARI

Platin Bilişim bilgi güvenliği faaliyetlerine dahil olan tüm personelin uygun eğitim, bilgi, beceri ve tecrübe düzeyinde bulunmasını sağlar.

Gerekli olan beceriler ve var olan becerilerin durumu sürekli olarak gözden geçirilir. Eğitim ihtiyaçları belirlenir ve gerekli yeterliklerin sağlanması için bir plan oluşturulur.

Eğitim durumu, alınmış eğitimler ve diğer ilgili kayıtlar İnsan Kaynakları tarafından tutulur. Bilgi Güvenliğine dair periyodik eğitimlerin planlanması ve kayıtlarının tutulması İnsan Kaynakları tarafından gerçekleştirilir.

# DENETLEME VE GÖZDEN GEÇİRME

Bilgi güvenliği süreç, politika ve prosedürleri kurulduktan sonra, bunların düzenli olarak gözden geçirilmesi; sistemin işlerliğini ölçebilmek adına önemlidir. Bu gözden geçirme ve denetleme üç seviyede gerçekleşir:

1. Politikalara ve prosedürlere uygunluğun üst yönetim tarafından ihtiyaç duyulduğunda olağan dışı toplantılar ile ya da düzenli olarak her sene Yönetim Gözden Geçirme toplantıları ile
2. ISO/IEC 27001 standardına uygunluğun iç denetim sonuçlarının incelenmesi ile
3. ISO/IEC 27001 standardının dış denetimlerinin gerçekleşmesi, bu sayede sertifikanın devamının sağlanması

Gözden geçirilen ve güncellenen politika, üst yönetim tarafından onaylanır ve yayınlanır.

# DOKÜMANTASYON YAPISI

Tüm bilgi güvenliği politika ve planları dokümante edilmelidir. Bu kısımda her bir alanda bulunması gereken ana dokümanlar belirtilmiştir.

Dokümantasyonla ilgili kabul ve standartlar **“PR.İİ.01 Dokümante Bilginin Kontrolü Prosedürü”** prosedüründe verilmiştir.

BGYS kapsamında ana dokümanlar oluşturulmuştur. Bu dokümanlar dosya sunucusu içerisinde bulunmaktadır.

# KAYITLARIN KONTROLÜ

Kayıtların tutulması BGYS’nin temel bir kısmını oluşturur. Kayıtlar, süreçlerin etkin bir şekilde işletildiğine dair kanıtlar sunar.

Kayıtların yaşam döngüsü ilgili süreç **“PR.İİ.01 Dokümante Bilginin Kontrolü Prosedürü”** dokümanında belirtilmektedir.

# POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, Yönetim Personel İşyeri Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

* İhtar,
* Fesih,
  + Derhal (bildirimsiz) fesih,
  + Süreli (bildirimli) fesih

# DAĞITIM

Tüm Platin Bilişim çalışanları