Bilgi Güvenliği Yönetimi Politikamız

ParaQR Elektronik Para ve Ödeme Hizmetleri A.Ş. olarak, sunduğumuz ödeme hizmetlerinin güvenli, kesintisiz ve güvenilir şekilde yürütülmesini sağlamak amacıyla bilgi güvenliğini kurumsal yönetimimizin ayrılmaz bir parçası olarak ele alırız. Bu kapsamda, bilgi varlıklarımızı korumaya yönelik süreç ve kontrollerimizi **ISO/IEC 27001** standardı yaklaşımı doğrultusunda yönetir ve düzenli olarak gözden geçiririz.

Bilgi Güvenliği Yaklaşımımız

Bilgi güvenliği yönetimimizin temelinde, bilgi varlıklarının:

- **Gizliliğinin** (yetkisiz erişimin önlenmesi),
- **Bütünlüğünün** (bilginin doğruluğu ve değiştirilmemesi),
- **Erişilebilirliğinin** (yetkili kişilerin ihtiyaç duyduğu anda erişebilmesi)

sağlanması yer alır.

Bilgi güvenliği yönetimi; yalnızca elektronik sistemleri değil, aynı zamanda yazılı/basılı dokümanlar ile sözlü olarak paylaşılan bilgiler dahil olmak üzere, iş süreçlerimiz kapsamında oluşan tüm bilgi varlıklarını kapsar. Kuruluşumuz adına hizmet sunan ve bilgi varlıklarımıza erişebilen hizmet sağlayıcılarımızın da belirlenen güvenlik kurallarına uyması beklenir. Aşağıdaki yaklaşımı benimseriz;

- İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı kuruluşumuza ait bilgi varlıklarını korumak; bilgiye erişilebilirliği iş süreçlerinin gerektirdiği ölçüde sağlamak, yasal ve düzenleyici gereksinimleri karşılamak ve sürekli iyileştirme faaliyetlerini yürütmek,
- Bilgi güvenliğinin temel unsurları olan **gizlilik, bütünlük ve erişilebilirlik** ilkeleri doğrultusunda; bilgi varlıklarının izinsiz veya yetkisiz erişim, kullanım, değiştirme, ifşa, silme, kaybetme, el değiştirme veya zarar görme risklerine karşı korunmasını sağlamak,
- Bilgi güvenliği kapsamında yalnızca elektronik ortamda tutulan verileri değil; yazılı, basılı, sözlü ve benzeri tüm ortamlarda bulunan bilgi varlıklarını kapsayan bütüncül bir güvenlik yaklaşımı benimsemek,

- Ödeme hizmetleri ve elektronik para faaliyetlerine ilişkin yürürlükteki mevzuat, ikincil düzenlemeler ve ilgili otoritelerin gereklilikleri doğrultusunda gerekli idari ve teknik tedbirleri almak, uygulamak ve sürekli iyileştirmek,
- Müşterilerimize, kullanıcılarımıza ve iş ortaklarımıza ait verilerin gizliliğinin ve mahremiyetinin korunmasına yönelik gerekli önlemleri almak ve bu yaklaşımı kurumsal bir taahhüt olarak sürdürmek,
- Bilgi güvenliği farkındalığını artırmak amacıyla tüm çalışanlara yönelik düzenli eğitimler ve bilgilendirme faaliyetleri gerçekleştirmek,
- Çalışanlarımızın bilgi güvenliğine bilinçli yaklaşmasını, görev ve sorumluluklarını yerine getirmesini ve yayımlanan politika, prosedür ve talimatlara uygun hareket etmesini sağlamak,
- Bilgi güvenliğini etkileyebilecek mevcut veya potansiyel açıklıkların ve olayların bilgi güvenliği olay yönetimi süreçleri kapsamında değerlendirilmesini; değerlendirme sonuçlarına göre mevcut kontrollerin güncellenmesini veya yeni kontrollerin devreye alınmasını sağlamak,
- İş sürekliliği ve hizmet devamlılığını sağlamak amacıyla iş sürekliliği planlarını hazırlamak, sürdürmek ve periyodik olarak test etmek,
- Bilgi güvenliği risklerini düzenli olarak değerlendirmek, risklere yönelik aksiyon planlarını oluşturmak, uygulamak ve takibini yapmak,
- Bilgi Güvenliği Politikası kapsamında belirlenen amaçların, yıllık olarak oluşturulan bilgi güvenliği hedefleri ile desteklenmesini; bu hedeflere ilişkin ilerleme durumlarının izlenmesini ve raporlanmasını sağlamak,
- Bilgi Güvenliği Yönetim Sistemi'nin etkinliğini sürekli iyileştirmek ve bu kapsamda yapılan çalışmaların üst yönetim tarafından düzenli olarak gözden geçirilmesini sağlamak.

Temel Uygulamalarımız

Bilgi güvenliğini sağlamak amacıyla genel olarak;

- Bilgi varlıklarımızı tanımlar, sınıflandırır ve sahipliklerini belirleriz.
- Bilgi güvenliği risklerini düzenli olarak değerlendirir; gerekli kontrol ve iyileştirmeleri planlar ve uygularız.
- Erişim yetkilerini "**asgari yetki**" prensibiyle yönetir; kimlik doğrulama ve yetkilendirme mekanizmaları uygularız.

- Sistemlerimizin sürekliliğini desteklemek için iş sürekliliği ve yedekleme yaklaşımlarını işletir, düzenli testler yaparız.
- Güvenlik olaylarını tespit etmek, yönetmek ve tekrarını önlemek için süreçler yürütür; gerekli durumlarda kontrol altyapımızı güncelleriz.
- Çalışanlarımızın bilgi güvenliği farkındalığını artırmak için eğitim ve bilgilendirme faaliyetleri gerçekleştiririz.

Sürekli İyileştirme ve Gözden Geçirme

Bilgi güvenliği uygulamalarımızın etkinliğini düzenli olarak izler; gerekli gördüğümüzde süreç ve kontrollerimizi güncelleriz. Bilgi güvenliği hedeflerimizi belirler, gerçekleşmelerini takip eder ve üst yönetim seviyesinde gözden geçiririz.