



ROYAL
GROUP HOTELS

BİLGİ GÜVENLİĞİ POLİTİKASI

Royal Group Hotels olarak; yenilikçi, güvenilir, sürdürülebilir ve misafir odaklı hizmet anlayışımız doğrultusunda, faaliyetlerimizin tüm aşamalarında bilgi varlıklarımızın korunmasını kurumsal yönetim anlayışımızın temel unsurlarından biri olarak kabul etmekteyiz.

Misafirlerimizin, çalışanlarımızın, iş ortaklarımızın, tedarikçilerimizin ve diğer tüm paydaşlarımızın bilgilerini korumak, bilgi güvenliğini kurumsal kültürümüzün ayrılmaz bir parçası haline getirmek ve bilgi güvenliği uygulamalarımızı sürekli geliştirmek amacıyla;

- Bilgi Güvenliği Yönetimi: ISO/IEC 27001 standardının temel prensiplerini esas alarak bilgi güvenliği süreçlerimizi geliştirmeyi, bilgi varlıklarımızı korumaya yönelik teknik, fiziksel ve idari kontrolleri oluşturmayı, uygulamayı ve sürekli iyileştirmeyi,
- Gizlilik, Bütünlük ve Erişilebilirlik: Kurumsal bilgi varlıklarımızın gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı; yetkisiz erişim, değiştirme, kayıp, ifşa ve kötüye kullanım risklerine karşı gerekli güvenlik önlemlerini almayı,
- Risk Yönetimi: Bilgi güvenliği risklerini sistematik olarak tanımlamayı, analiz etmeyi ve değerlendirmeyi; risk kabul kriterlerini ve risk sahiplerini belirleyerek uygun kontrolleri geliştirmeyi, uygulamayı ve etkinliğini düzenli olarak izlemeyi,
- Kişisel Verilerin Korunması: Misafirlerimizin, çalışanlarımızın ve iş ortaklarımızın kişisel verilerini başta 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) olmak üzere yürürlükteki ilgili mevzuata uygun şekilde işlemeyi, saklamayı, korumayı ve yasal saklama sürelerinin sonunda mevzuata uygun yöntemlerle imha etmeyi,
- Yasal ve Sözleşmesel Uyum: Bilgi güvenliği ile ilgili yürürlükteki ulusal ve uygulanabilir uluslararası düzenlemelere, ilgili mevzuata, sözleşmesel yükümlülöklere ve paydaşlarımızın bilgi güvenliği gereksinimlerine uymayı,
- Dijital Güvenlik: Otel yönetim sistemleri, rezervasyon altyapıları, misafir ilişkileri uygulamaları, ödeme sistemleri, kurumsal iletişim ağıları ve diğer dijital platformlarda bilgi güvenliğini sağlamaya yönelik gerekli önlemleri almayı,
- Erişim Yetkilendirmesi: Bilgi varlıklarına erişimi görev, yetki ve sorumluluklar doğrultusunda sınırlandırmayı; yetkisiz erişimleri önlemeyi, erişim yetkilerini düzenli olarak gözden geçirmeyi ve bilgiye yalnızca yetkili kişilerin erişimini sağlamayı,
- Bilgi Varlıklarının Korunması: Elektronik ve fiziksel ortamlarda bulunan bilgi varlıklarını hassasiyet seviyelerine göre sınıflandırmayı; uygun saklama, paylaşım, aktarım, yedekleme ve güvenli imha kurallarını belirlemeyi ve uygulamayı,
- İş Sürekliliği: Bilgi güvenliği tehditlerinin operasyonel süreçlerimiz ve hizmet sürekliliğimiz üzerindeki olası etkilerini azaltmayı; kritik bilgi sistemlerinin sürekliliğini destekleyecek önlemleri geliştirmeyi,
- Bilgi Güvenliği Olay Yönetimi: Olası bilgi güvenliği ihlallerini ve siber güvenlik olaylarını zamanında tespit etmeyi, raporlamayı, olaylara etkin şekilde müdahale etmeyi ve tekrarını önlemeye yönelik düzeltici faaliyetleri gerçekleştirmeyi,
- Çalışan Farkındalığı: Tüm çalışanlarımızın bilgi güvenliği sorumluluklarını benimsemelerini sağlamayı; eğitim ve farkındalık faaliyetleriyle güvenli bilgi kullanım kültürünü geliştirmeyi,

- Tedarikçi ve İş Ortağı Güvenliği: Dış kaynaklı hizmet sağlayıcılarımızın, tedarikçilerimizin ve iş ortaklarımızın bilgi güvenliği yükümlülüklerini tanımlamayı ve ilgili güvenlik gereksinimlerine uyumlarını takip etmeyi,
- Teknolojik Gelişim ve Sürekli İyileştirme: Gelişen teknolojileri, dijital dönüşüm süreçlerini ve değişen siber güvenlik tehditlerini takip ederek bilgi güvenliği uygulamalarımızı güncel tutmayı, performanslarını değerlendirmeyi ve sürekli iyileştirmeyi,
- Kurumsal İtibar ve Güven: Bilgi güvenliği uygulamalarımızla misafirlerimizin ve tüm paydaşlarımızın güvenliğini korumayı, kurumsal itibarımızı güçlendirmeyi ve güvenilir hizmet anlayışımızın sürdürülebilirliğini sağlamayı,

taahhüt ederiz.

Royal Group Hotels Üst Yönetimi olarak; bu politikanın grup bünyesindeki tüm tesislerde, departmanlarda ve ilgili faaliyet alanlarında uygulanmasını, çalışanlarımıza ve ilgili paydaşlarımıza duyurulmasını, gerekli kaynakların sağlanmasını ve bilgi güvenliği uygulamalarımızın düzenli olarak gözden geçirilerek sürekli iyileştirilmesini desteklemekteyiz.