BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Baia Hotels Üst Yönetimi olarak temel amacımız; sunduğumuz konaklama ve otelcilik hizmetlerinde; insan, altyapı, yazılım, donanım, misafir bilgileri, kurumsal bilgiler, üçüncü şahıslara ait bilgiler ve finansal kaynaklarımızı kapsayan tüm bilgi varlıklarımızın güvenliğini sağlamaktır.

Bu politika, TS EN ISO 27001:2022 standardını referans alarak;

- Bilgi güvenliği risklerimizi tanımlamayı, değerlendirmeyi ve yönetmeyi,
- Bilgi varlıklarımızı içeriden veya dışarıdan gelebilecek kasıtlı veya kasıtsız tüm tehditlere karşı korumayı,
- Başta KVKK (Kişisel Verilerin Korunması Kanunu) olmak üzere, tüm yasal mevzuatlara ve regülasyonlara (PCI-DSS vb.) tam uyum sağlamayı,
- İş süreçlerimizin kesintisiz devamlılığını güvence altına almayı,
- Tüm paydaşlarımızın (misafirlerimiz, çalışanlarımız, tedarikçilerimiz) bilgi güvenliği farkındalığını artırmayı hedeflemektedir.

2. Kapsam

Bu politika, Baia Hotels'in tüm lokasyonlarındaki (Baia Lara, Baia Salima Kemer, Baia Bodrum, Monte Baia Uludağ, Baia Bursa ve merkez ofis) tüm tam zamanlı/yarı zamanlı çalışanlarını, stajyerlerini, danışmanlarını ve dış hizmet sağlayıcılarını kapsar.

Politika; elektronik, yazılı, basılı, sözlü veya benzeri ortamlarda bulunan ve aşağıdakileri içeren ancak bunlarla sınırlı olmayan tüm bilgi varlıkları için geçerlidir:

- Misafir Verileri: Kimlik/Pasaport bilgileri, rezervasyon detayları, ödeme bilgileri, konaklama tercihleri.
- Kurumsal Veriler: Finansal kayıtlar, stratejik planlar, operasyonel veriler, pazarlama bilgileri.
- Sistem Altyapısı: Mülk Yönetim Sistemleri (PMS), Satış Noktası (POS) sistemleri, Misafir Wi-Fi ağları, CCTV kayıtları, kartlı geçiş sistemleri, sunucular ve veri tabanları.
- Çalışan Verileri: Personel özlük dosyaları ve iletişim bilgileri.

3. Bilgi Güvenliğinin Temel İlkeleri

Yürüttüğümüz tüm faaliyetlerde Bilgi Güvenliği Yönetim Sisteminin üç temel öğesinin sürekliliği sağlanacaktır:

- Gizlilik (Confidentiality): Kritik öneme sahip misafir ve kurum bilgilerine (özellikle KVKK kapsamındaki kişisel ve özel nitelikli verilere) yetkisiz erişimlerin kesin olarak önlenmesi.
- Bütünlük (Integrity): Misafir rezervasyonları, finansal kayıtlar ve operasyonel veriler başta olmak üzere tüm bilginin doğruluğunun, tutarlılığının ve yetkisiz değiştirmelere karşı korunmasının sağlanması.
- Erişebilirlik (Availability): Yetkili kullanıcıların (personel, yönetim), görevlerini yerine getirebilmeleri için ihtiyaç duydukları bilgi ve iş sistemlerine (PMS, e-posta vb.) kesintisiz ve hızlı bir şekilde erişebilmesinin garanti edilmesi.

4. Taahhütler ve Sorumluluklar

- Üst Yönetim: BGYS'nin kurulması, işletilmesi ve sürekli iyileştirilmesi için gerekli liderliği göstermeyi, kaynakları (insan, bütçe, teknoloji) sağlamayı ve politikanın tüm kurumda benimsenmesini desteklemeyi taahhüt eder.
- BGYS Ekibi (Kalite Koordinatörü/Bilgi Güvenliği Yöneticisi): BGYS'nin operasyonel yönetiminden, risk analizlerinin yapılmasından, güvenlik olaylarının soruşturulmasından ve politikaların güncel tutulmasından sorumludur.
- Tüm Çalışanlar: Görev tanımları ne olursa olsun tüm çalışanlar, bu politikayı ve ilgili prosedürleri bilmekle, uymakla ve bilgi güvenliği eğitimlerine katılmakla yükümlüdür. Gerçekleşen veya şüphelenilen tüm güvenlik açıklarını ve olaylarını derhal ilgili birime rapor etmek zorundadır.

5. Politika Alanları

- Risk Yönetimi: Bilgi varlıklarımıza yönelik riskler periyodik olarak değerlendirilecek, kabul edilebilir seviyeye indirmek için gerekli teknik ve idari kontroller (erişim kontrolü, şifreleme, güvenlik duvarı vb.) uygulanacaktır.
- Yasal Uyum ve Standartlar: Başta 6698 sayılı KVKK ve ilgili kurul kararları olmak üzere, kredi kartı güvenliği için PCI-DSS (Ödeme Kartı Sektörü Veri Güvenliği Standardı) ve diğer tüm yasal gerekliliklere tam uyum sağlanacaktır.
- Ağ Güvenliği: Misafirlerimize sunulan internet (Guest Wi-Fi) ağı ile Baia Hotels kurumsal iç ağı (personel ağı, PMS ve POS sistemleri) birbirinden tamamen izole (ayrı) tutulacaktır.
- İş Sürekliliği: Kritik otelcilik süreçlerimizin (rezervasyon alma, check-in/check-out, ödeme sistemleri) olası bir kesinti, kriz veya felaket anında dahi devamlılığını sağlamak için İş Sürekliliği Yönetim Sistemi (ISYS) kurulacak, test edilecek ve güncel tutulacaktır. Gerekli aksiyonların hızla alınması taahhüt edilmektedir.
- Üçüncü Taraf İlişkileri: Dışarıdan alınan yazılım (PMS, CRM vb.), donanım veya destek hizmetleri için tedarikçilerle yapılan sözleşmelerde bilgi güvenliği ve KVKK şartları net olarak tanımlanacak ve denetlenecektir.
- Farkındalık ve Eğitim: Tüm personelin bilgi güvenliği tehditlerini (örn: oltalama/phishing saldırıları, sosyal mühendislik) tanıması ve önlem alabilmesi için düzenli olarak farkındalık eğitimleri verilecektir.

6. Sürekli İyileştirme ve Gözden Geçirme

Bu politika, BGYS süreç performansı, denetim sonuçları, güvenlik olayları ve değişen iş/teknoloji koşullarına bağlı olarak Üst Yönetim tarafından yılda en az bir kez veya gerekli görüldüğünde gözden geçirilecek ve güncellenecektir.