InfoSteer

Bilgi Güvenliği Politikası

Yayın tarihi: 01.01.2026

Kuruluş: İNFOSTEER BİLİŞİM TEKNOLOJİLERİ SANAYİ ANONİM ŞİRKETİ

Amaç ve kapsam

InfoSteer olarak bilgi güvenliğini, müşterilerimizin güvenini ve hizmetlerimizin sürekliliğini korumanın temel unsurlarından biri olarak kabul ederiz. Bu politika ile sahip olduğumuz veya sorumluluğumuz altında işlediğimiz bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı; Bilgi Güvenliği Yönetim Sistemimizi (BGYS) ISO/IEC 27001 şartları doğrultusunda kurmayı, uygulamayı, sürdürmeyi ve sürekli iyileştirmeyi taahhüt ederiz.

Politika; yazılım, yapay zekâ, veri analitiği ve üretim zekâsı faaliyetlerimizle ilişkili bilgi varlıklarını, iş süreçlerini ve destek hizmetlerini kapsar. Çalışanlarımıza ve görevleri veya sözleşmeleri ölçüsünde bilgi varlıklarımıza erişen tedarikçi, danışman ve iş ortaklarına uygulanır. Yönetim sisteminin organizasyonel, fiziksel ve teknolojik sınırları ayrı BGYS kapsam dokümanında tanımlanır.

Bilgi güvenliği taahhütlerimiz

1. Bilginin korunması Bilgilerin yalnızca yetkili kişiler tarafından erişilebilir olmasını, doğruluğunun ve bütünlüğünün korunmasını ve yetkili kullanıcıların ihtiyaç duyduğu zamanda kullanılabilirliğini sağlamaya yönelik tedbirleri uygularız. Dijital, fiziksel ve sözlü bilgileri yaşam döngüleri boyunca koruruz.

2. Risklerin yönetilmesi Bilgi güvenliği risklerini belirlenmiş ölçütlerle değerlendirir, risk sahiplerini ve uygun risk işleme yöntemlerini belirleriz. Kontrollerimizi iş ihtiyaçları, olası etkiler ve ilgili tarafların gereklilikleri doğrultusunda seçer; kalan riskleri yetkili yönetim seviyesinde değerlendiririz.

3. Uygulanabilir şartlara uyum Bilgi güvenliğiyle ilgili yasal, düzenleyici ve sözleşmesel yükümlülükleri ve kabul ettiğimiz diğer gereklilikleri karşılamayı taahhüt ederiz. Kişisel verileri, ticari sırları, fikri mülkiyeti ve müşterilerimizin bize emanet ettiği bilgileri bu yükümlülükler doğrultusunda koruruz.

4. Erişim ve varlık güvenliği Bilgi varlıklarının sahipliğini ve sınıflandırmasını belirler, erişimleri iş gereği ve en az yetki ilkesiyle yönetiriz. İşe giriş, görev değişikliği ve işten ayrılma süreçlerinde erişim haklarını gözden geçirir; fiziksel alanları, cihazları ve uzak çalışma ortamlarını risklerine uygun şekilde koruruz.

5. Güvenli ürün ve hizmet geliştirme Güvenliği yazılım ve sistemlerin tasarım, geliştirme, test, devreye alma ve bakım süreçlerine dahil ederiz. Kaynak kodları, yapay zekâ modelleri, veri setleri ve erişim bilgilerini korur; değişiklikleri, güvenlik açıklarını ve üçüncü taraf bileşenleri kontrollü biçimde yönetiriz. Gizli bilgilerin yetkisiz yapay zekâ araçlarına veya platformlara aktarılmasını önleriz.

6. Tedarikçi ve bulut güvenliği Tedarikçilerin ve bulut hizmetlerinin bilgi güvenliği risklerini hizmetin niteliğine göre değerlendiririz. Erişim, gizlilik, veri işleme, olay bildirimi ve hizmetin sona ermesiyle ilgili sorumlulukları sözleşmelerde belirler; ilgili hizmetleri ve değişiklikleri izleriz.

7. Güvenlik olaylarının yönetilmesi Çalışanların ve ilgili tarafların şüpheli durumları ve güvenlik olaylarını gecikmeden bildirebileceği kanalları belirler ve duyururuz. Olayları kaydeder, değerlendirir, etkilerini sınırlandırır ve tekrarını önlemek için gerekli faaliyetleri yürütürüz. Gerekli bildirimleri uygulanabilir yükümlülüklere göre gerçekleştiririz.

8. Süreklilik ve dayanıklılık Kritik hizmetlerin bilgi güvenliği ihtiyaçlarını iş sürekliliği planlamasına dahil ederiz. Yedekleme, geri yükleme ve kesinti sonrası toparlanma önlemlerini risklere ve iş ihtiyaçlarına göre belirler; etkinliklerini planlı olarak test ederiz.

9. Yetkinlik ve farkındalık Bilgi güvenliği rollerini, sorumluluklarını ve yetkilerini tanımlarız. Çalışanların görevleri için gerekli yetkinlikleri geliştirmesini sağlar; eğitim, farkındalık ve gizlilik çalışmalarını sürdürürüz. İlgili dış taraflara kendilerinden beklenen güvenlik kurallarını bildiririz.

10. Performans ve sürekli iyileştirme BGYS'nin etkinliğini izleme, ölçme, iç tetkik ve yönetimin gözden geçirmesi yoluyla değerlendiririz. Uygunsuzlukların nedenlerini giderir, düzeltici faaliyetleri izler ve bilgi güvenliği yönetim sistemimizi sürekli iyileştirmeyi taahhüt ederiz.

Hedefler ve yönetimin sorumluluğu

Bu politika, bilgi güvenliği hedeflerinin belirlenmesi ve gözden geçirilmesi için çerçeve oluşturur. Hedefler; riskler, iş öncelikleri ve uygulanabilir gereklilikler dikkate alınarak, uygulanabildiği ölçüde ölçülebilir biçimde belirlenir. Her hedef için sorumlu, gerekli kaynaklar, tamamlanma zamanı ve değerlendirme yöntemi tanımlanır. Olay yönetimi, erişimlerin gözden geçirilmesi, güvenlik açıklarının giderilmesi, geri yükleme testleri ve çalışan farkındalığı hedeflerin belirlenmesinde dikkate alınır.

Üst yönetim, BGYS'nin iş süreçlerine dahil edilmesini, sorumlulukların atanmasını ve gerekli insan kaynağı, teknoloji ve bütçenin sağlanmasını destekler. Çalışanlar ve ilgili dış taraflar, kendilerine bildirilen politika ve güvenlik kurallarına görev ve yetkileri kapsamında uymakla sorumludur.

İletişim ve gözden geçirme

Bu politika üst yönetim onayıyla yürürlüğe girer; kuruluş içinde duyurulur ve ilgili tarafların erişimine uygun şekilde sunulur. Kamuya açık sürümü InfoSteer web sitesinde yayımlanır. Politika en az yılda bir ve faaliyetlerde, risklerde veya uygulanabilir gerekliliklerde önemli değişiklik olduğunda gözden geçirilir. Değişiklikler üst yönetim onayıyla yürürlüğe alınır ve güncel sürüm ilgili taraflara iletilir.

Onaylayan: FIRAT AKINCILAR

Onay tarihi: 01.01.2026

Fırat Akıncılar