Doküman No: OJT.PO.01 Yayın Tarihi: 01.09.2026 Rev No: 00 Revizyon Tarihi: -

BİLGİ GÜVENLİĞİ POLİTİKASI

Otojet Enerji Sanayi ve Ticaret A.Ş. olarak; elektrikli araç şarj ağı işletmeciliği, e-mobilite çözümleri ve dijital platformlarımızda sunduğumuz hizmetlerin güvenilirliği ve kesintisizliği için, kurumsal ve kullanıcılarımıza ait tüm bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde korunmasının temel önceliğimiz olduğunun bilincindeyiz.

Üst Yönetimimiz; bilgi varlıklarımızın ve dijital hizmet altyapımızın korunması amacıyla TS EN ISO/IEC 27001 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmayı, işletmeyi, gerekli kaynakları tahsis etmeyi, sistemi düzenli olarak gözden geçirmeyi ve sürekli iyileştirmeyi taahhüt eder.

Bu doğrultuda Şirketimizde;

- Başta EPDK Şarj Hizmeti Yönetmeliği, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve 5651 sayılı Kanun olmak üzere tabi olduğumuz tüm yasal düzenlemelere, sektörel standartlara ve kullanıcı/tedarikçi sözleşmelerinden doğan şartlara eksiksiz uyum sağlamayı,
- Teknoloji odaklı büyüme stratejimizle uyumlu, ölçülebilir bilgi güvenliği amaç ve hedefleri belirlemeyi ve bu hedeflerin gerçekleşme performansını düzenli olarak izlemeyi,
- Şarj ağı yönetim platformlarımıza, kurumsal süreçlerimize ve bilgi varlıklarımıza yönelik siber ve operasyonel riskleri kabul görmüş metodolojilerle değerlendirmeyi ve etkin güvenlik kontrolleriyle yönetmeyi,
- Kullanıcılarımıza, çalışanlarımıza ve iş ortaklarımıza ait kişisel ve kurumsal verilerin gizliliğini ve bütünlüğünü en üst düzeyde korumayı,
- Grup içi paylaşımlı hizmetler kapsamında alınan merkezi bilgi teknolojileri, siber güvenlik ve destek süreçleri ile dış tedarikçi operasyonlarının, Hizmet Seviyesi Anlaşmaları (SLA) ve bilgi güvenliği kurallarımız doğrultusunda güvenli şekilde yürütülmesini sağlamayı,
- Hizmetlerimizin ve kritik iş süreçlerimizin kesintisizliğini güvence altına almak üzere iş sürekliliği planlarını hazırlamayı, uygulamayı ve periyodik olarak test etmeyi,
- Dijital platformlarımıza yönelik güncel siber tehditleri ve güvenlik açıklarını proaktif olarak izleyerek gerekli önleyici tedbirleri zamanında almayı,
- Bilgi güvenliği bilincini tüm çalışanlarımızda kurum kültürü haline getirecek düzenli eğitim ve farkındalık programları yürütmeyi,

tüm paydaşlarımıza taahhüt ediyoruz.