MURAT ÖZ - LG TEKNOLOJİ

BİLGİ GÜVENLİĞİ VE SİBER GÜVENLİK POLİTİKASI (ISO/IEC 27001 UYUM POLİTİKASI)

1. AMAÇ VE KAPSAM

Bu Bilgi Güvenliği Politikası, Murat Öz - LG Teknoloji ("Şirket") tarafından işlenen, üretilen, aktarılan veya saklanan her türlü bilgi varlığının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak amacıyla hazırlanmıştır. Şirketimiz, uluslararası kabul görmüş ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standartlarına tam uyum sağlamayı taahhüt eder.

Bu politika; şirket yönetimi, tüm çalışanlar, stajyerler, tedarikçiler, alt yükleniciler ve bilgi varlıklarımıza erişim sağlayan üçüncü tarafları kapsar. Bilgi işlem altyapısı, ağ sistemleri, veri depolama üniteleri ve fiziki belgelerin tamamı bu politika çerçevesinde korunur.

2. BİLGİ GÜVENLİĞİNİN ÜÇ TEMEL UNSURU (CIA TRIAD)

Şirketimizin bilgi güvenliği yaklaşımı aşağıdaki üç temel ilkeye dayanmaktadır:

- **Gizlilik (Confidentiality):** Bilginin yetkisiz kişilerin eline geçmesinin veya açıklanmasının engellenmesi.
- **Bütünlük (Integrity):** Bilginin yetkisiz kişilerce değiştirilmesinin, silinmesinin veya tahrif edilmesinin önlenmesi; doğruluğunun ve tamlığının korunması.
- **Erişilebilirlik (Availability):** Bilginin ve ilişkili sistemlerin yetkili kullanıcılar tarafından ihtiyaç duyulduğunda erişilebilir ve kullanılabilir olması.

3. TEKNİK VE OPERASYONEL BİLGİ GÜVENLİĞİ TEDBİRLERİ

3.1. Ağ ve Sistem Güvenliği

- Şirket ağı, güncel Güvenlik Duvarı (Firewall) ve Saldırı Önleme Sistemleri (IPS/IDS) ile 7/24 koruma altındadır.
- Tüm sunucularda ve uç nokta cihazlarında (bilgisayarlar, mobil cihazlar) lisanslı ve merkezi olarak yönetilen Antivirüs / EDR çözümleri kullanılır.

3.2. Erişim Yönetimi ve Parola Politikası

- Erişim yetkileri, "Bilmesi Gereken Kadar" (Need-to-Know) ve "En Az Yetki" (Least Privilege) ilkelerine göre tanımlanır.
- Tüm sistem erişimlerinde güçlü karmaşık parola standartları (en az 8 karakter, harf, rakam ve özel karakter) zorunludur. Kritik sistemlerde Çok Faktörlü Kimlik Doğrulama (MFA) kullanılır.

3.3. Veri Yedekleme ve İş Sürekliliği (Disaster Recovery)

- Kritik veri ve sistemler günlük ve haftalık periyotlarla şifrelenmiş ortamlarda otomatik olarak yedeklenir.
- Olası bir sistem çökmesi veya siber saldırı durumunda iş sürekliliğini sağlamak için düzenli yedekten geri dönme (Restore) testleri gerçekleştirilir.

3.4. Temiz Masa ve Temiz Ekran Politikası

- Çalışanlar, hassas bilgi içeren belgeleri kilitli dolaplarda muhafaza etmek ve çalışma alanlarından ayrılırken bilgisayar ekranlarını kilitlemekle yükümlüdür.

4. İNSAN KAYNAKLARI VE FARKINDALIK EĞİTİMLERİ

Bilgi güvenliğinin en kritik halkası insan faktörüdür. Bu doğrultuda:

- Tüm çalışanlar işe alım sürecinde Bilgi Güvenliği ve Gizlilik Sözleşmesi imzalar.
- Çalışanlara oltalama (Phishing) saldırıları, sosyal mühendislik ve siber tehditlere karşı düzenli olarak farkındalık eğitimleri verilir.

5. BİLGİ GÜVENLİĞİ İHLAL OLAYLARI YÖNETİMİ

Gerçekleşen veya şüphelenilen tüm bilgi güvenliği ihlalleri (veri sızıntısı, virüs bulaşması, yetkisiz erişim denemesi vb.) vakit kaybetmeksizin Bilgi Teknolojileri / Yönetim Birimine bildirilir. İhlal olayları derhal izole edilir, kök neden analizi yapılır ve gerekli önleyici tedbirler hayata geçirilir.

6. DENETİM VE YAPTIRIMLAR

Bilgi güvenliği politikalarının uygulanması yönetim tarafından düzenli olarak denetlenir. Politikaya aykırı tutum ve davranışlar iş akdinin feshi de dâhil olmak üzere disiplin cezalarına ve gerekirse hukuki süreçlere konu edilir.

7. İLETİŞİM VE BİLGİ GÜVENLİĞİ SORUMLUSU

Bilgi güvenliği süreçleri veya ihlal bildirimleri ile ilgili şirketimizle aşağıdaki kanallardan iletişime geçebilirsiniz:

Firma Adı	Murat ÖZ - LG Teknoloji
Adres	Dr. Ömer Besim Paşa Cad. Kamer Sokak No:7/1 Yenimahalle Beykoz / İstanbul
Telefon	0216 599 01 37
E-posta	info@lgteknoloji.com | info@lazergozluk.net | info@lazergozluk.com.tr
Bilgi Güvenliği İhbar / Destek	info@lgteknoloji.com

Bu politika, Murat Öz - LG Teknoloji yönetiminin onayıyla yürürlüğe girmiştir.