İçindekiler

1. Amaç

Bu politika, kurumsal bilgilerin, bilgi sistemlerinin, süreçlerin ve uygulamaların gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek ve yönetmek amacıyla hazırlanmıştır. Ayrıca bilgi güvenliği risklerinin belirlenmesi, değerlendirilmesi ve işlenmesi yoluyla ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi gerekliliklerine uyum sağlanmasını hedefler.

2. Kapsam ve Dayanak

Anadolu ISUZU bilgi varlıklarını kullanmakta olan tüm çalışanlar ve iş paydaşları bu politikanın kapsamındadır. Bu kapsam; çalışanlar, taşeronlar, tedarikçiler, danışmanlar, ziyaretçiler ve bilgi sistemlerine erişimi bulunan tüm üçüncü tarafları içerir.

Bu politika;

- ISO/IEC 27001:2022 Standardı,
- İlgili ulusal ve uluslararası mevzuat,
- Sözleşmesel yükümlülükler,
- Kurumsal risk yönetimi çerçevesi
- esas alınarak hazırlanmıştır.

3. Tanımlar

- **BGYS:** Bilgi Güvenliği Yönetim Sistemi
- **BGY:** Bilgi Güvenliği Yöneticisi
- **Şirket:** Anadolu ISUZU Otomotiv Sanayi ve Ticaret A.Ş.

4. Rol ve Sorumluluklar

Tüm Çalışanlar: Anadolu Isuzu'ya ait bilgilerin yetkili ellerde kalması; bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması ve bilgilerin ve sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır. Bu nedenle tüm Anadolu Isuzu çalışanları, konumları veya görevleri ne olursa olsun işlerini, bilgilerin Anadolu Isuzu bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur. Çalışanlar ayrıca;

- Bilgileri sınıflandırma seviyelerine uygun şekilde kullanmakla,
- Yetkisiz erişim ve paylaşımlardan kaçınmakla,
- Gözlemledikleri veya şüphelendikleri bilgi güvenliği ihlallerini, belirlenmiş kanallar aracılığıyla derhal raporlamakla yükümlüdür.

Departman/Bölüm Yöneticileri: Her birimin yöneticisi kendi sorumluluk alanında, Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak, faaliyetleri gözlemlemek ve bilgi güvenliği risklerinin izlenmesi ile uygulanan kontrollerin etkinliğini gözetilmesinden birinci derece sorumludur.

Bilgi Güvenliği Yöneticisi: Bu politikaya bağlı diğer alt politikalar ilgili Bilgi Güvenliği Yöneticisi tarafından değerlendirilir ve onaylanır.

Üçüncü Taraflar: Bilgi sistemlerine erişimi olan tüm üçüncü taraflar;

- Bu politika ve ilgili bilgi güvenliği şartlarına uyması zorunludur,
- Sözleşmelerde bilgi güvenliği gereklilikleri açıkça tanımlanır,
- Uyum, izleme ve gerektiğinde yaptırım mekanizmaları işletilir.

5. Üst Yönetim Taahhüdü

Anadolu Isuzu üst yönetimi;

- Bilgi güvenliğini kurumsal risk yönetimi sürecinin bir parçası olarak ele almayı,
- BGYS'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli kaynakları sağlamayı,
- Bilgi güvenliği kontrollerinin etkinliğini izlemeyi ve gözetmeyi,
- Bilgi güvenliği gerekliliklerinin sözleşmelere ve üçüncü taraf ilişkilerine yansıtılmasını sağlamayı,
- Hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere uygun hareket ederek bilgi güvenliğini sağlamayı,
- Kurum'un güvenilirliğini ve imajını korumayı
- Bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanmasını
- Kurum'un temel ve destekleyici faaliyetlerinin en az kesinti ile devam etmesini sağlayacak ve İş sürekliliğini destekleyecek bilgi güvenliği tedbirlerini uygulamayı taahhüt eder.

6. Bilgi Güvenliği Politikası

Anadolu Isuzu, kurumsal bilgiyi değerli bir varlık olarak kabul eder. Bilgi güvenliği, kurumsal hedeflerin ve iş sürekliliğinin ayrılmaz bir parçasıdır. Faaliyetler sırasında kullanılan, Anadolu Isuzu'ya ve/veya iş paydaşlarımıza ait her türlü kurumsal bilgi ve bilginin bulunduğu ortam, işimiz ve sorumluluklarımız açısından kritik önem taşır ve uygun şekilde güvenliğinin sağlanması gerekir. Güvenlik kavramı, gizlilik (bilgilerin yetkisiz kişilerin eline geçmesinin engellenmesi), bütünlük (tam, doğru, yetkisiz olarak değiştirilmemiş) ve kullanılabilirlik (gerektiğinde kullanıma hazır olması) olarak 3 bileşenden oluşur ve bu ana bileşenlerden herhangi birinde oluşabilecek bir güvenlik zafiyeti Anadolu Isuzu'nun iş faaliyetlerinin bütünlüğü ve itibarı üzerinde ciddi bir etkiye neden olabilir.

Bu politika, kurumsal bilgilerin, bilgi sistemlerinin, süreçlerin ve uygulamaların gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek ve yönetmek amacıyla hazırlanmıştır. Anadolu Isuzu bilgi varlıklarını kullanmakta olan tüm çalışanlar ve iş paydaşları bu politikanın kapsamındadır. Görev ve pozisyonu ne olursa olsun, tüm Anadolu Isuzu çalışanları ve tedarikçileri, ilgili yasal düzenlemeler, politikalar, prosedürler, yönetmelikler, Anadolu Isuzu çalışma ilkeleri ve sözleşmelerde belirtilen güvenlik ilkelerine uymak, riskleri sınırlandırmak ve kabul görmüş iyi uygulamalar çerçevesinde çalışmak zorundadır. İlgili taraflar ile BGYS Politikası web sitesi üzerinden, kurum çalışanları ile eposta aracılığı ile, kurum ziyaretçileri ile fuaye alanında paylaşılmaktadır.

Bilgi güvenliği ile ilgili politikaların ihlali ve risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması Anadolu Isuzu'nun maddi ve manevi zarar görmesine sebep olabilir. Bu nedenle gözetim, denetim ve/veya ihbar sonucu tespit edilen bilgi güvenliği ve/veya ilgili politika ihlalleri adli ve cezai yasal işlemler başlatılmasına varıncaya kadar gidebilecek şirket içi disiplin cezalarının uygulanmasına yol açar. Kurum Personel Yönetmeliği gereğince uyarma, kınama, sözleşme feshi gibi yaptırımlar uygulanır. Anadolu Isuzu bilgi güvenliği ihlallerinin önlenmesi, tespiti, raporlanması ve etkilerinin azaltılması için gerekli organizasyonel ve teknik tedbirleri alır.

Her birimin yöneticisi kendi sorumluluk alanında, Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve faaliyetleri gözetlemekten birinci derece sorumludur. Anılan hususlar ile birlikte Bilgi Güvenliği Politikamız;

- Bilgi varlıklarımızın risklerini tanımlayarak uygun önlemlerin alınmasını sağlamak,
- Bilgi Güvenliğini etkileyen ulusal/uluslararası kanun, mevzuat, düzenleyici kurul/otorite kararlarına, talimat ve prosedürlerine uymak,
- Sözleşme şartlarına uymak,
- İş ve hizmetlerimizin sürekliliğini temin edecek çerçeveleri oluşturmak,

- Kurumsal ve müşteri bilgi varlıklarının gizlilik, bütünlük, erişilebilirlik haklarını korumak,
- Bilgi Güvenliği Yönetim Sisteminin şartlarına uymak ve etkinliğinin sürekli iyileştirilmesini sağlamak,
- Yönetimin yılda en az bir kez ve önemli değişiklikler veya ortaya çıkan bilgi güvenliği ihlalleri durumunda gerektiğinde bu politikayı gözden geçirmesini sağlamaktır.

Anadolu Isuzu, yukarıda sayılanlar ile birlikte Bilgi Güvenliği Yönetim Sistemi ile kendisinin ve paydaşlarının bilgi ve bilgi varlıklarını korumayı hedefler. Anadolu Isuzu Yönetimi, bu hedefine ulaşmak amacıyla Bilgi Güvenliği Yönetim Sistemi'nin kurulması, uygulanması, işletilmesi ve sürekli iyileştirilmesi için gerekli kaynakları sağlayacağını taahhüt eder. Anadolu Isuzu üst yönetmi;

7. Farkındalık ve Eğitim

Anadolu Isuzu, tüm çalışanlara periyodik Bilgi Güvenliği Farkındalık Eğitimlerini ve bilgi güvenliğini destekleyici eğitimlerin verilmesini sağlar ve bilgi güvenliği kültürünün kurumsal düzeyde yerleşmesini hedefler.

8. Denetim ve İyileştirme

Bilgi güvenliği uygulamaları iç ve dış denetimlerle periyodik olarak değerlendirilir. Denetim sonuçları üst yönetime raporlanır, tespit edilen uygunsuzluklar için aksiyon planları oluşturulur ve takip edilir. BGYS sürekli iyileştirme yaklaşımıyla yönetilir.

9. Gözden Geçirme

Yönetimin yılda en az bir kez bu politikayı gözden geçirmesi sağlanır. Ayrıca önemli organizasyonel, teknolojik veya uygulamakla yükümlü olunan mevzuat değişiklikler ile ciddi bilgi güvenliği ihlalleri sonrasında politika yeniden değerlendirilir ve güncellenir.

10. İlgili Dokümanlar veya Ekler

ISO 27001 Standardı

Bilgi Varlığı Yönetim Prosedürü

Bilgi Güvenliği Risk Yönetim Prosedürü