GLOBAL BİLGİ GÜVENLİĞİ POLİTİKASI

aksa ELEKTRİK

İÇİNDEKİLER

GİRİŞ 2

1. AMAÇ 2

2. KAPSAM 2

3. TEMEL İLKELER 2

GİRİŞ

Kuruluş hedeflerimiz doğrultusunda küresel çapta başarıya ulaşmak için tutarlı, etkili ve şeffaf bir iletişim modelinin önemini biliyoruz. Bu nedenle tüm paydaşlarımızla açık, şeffaf ve güvenilir bir şekilde iletişim kurmak için kapsamlı bir Global Bilgi Güvenliği Politikası oluşturduk. Bu sayede günümüzde hızla bir devinim içerisinde olan teknolojik gelişimleri takip edip uluslararası standartlara uygun, ölçülebilir, şeffaf bir şekilde raporlanabilir ve denetlenebilir bir bilgi güvenliği sistemi ile süreçlerimize yön veriyoruz.

1. AMAÇ

Bu politika ile tüm bilgi varlıklarımızın gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda korunmasını sağlar; BT ve OT/SCADA ortamları dahil kritik sistemlerde ortaya çıkabilecek fiziksel ve siber güvenlik risklerini etkin biçimde yönetir, uyulması gereken asgari bilgi güvenliği esaslarını tanımlarız.

2. KAPSAM

Bu politika, faaliyet gösterdiğimiz ülkelerdeki tüm çalışanlar, taşeron personel, geçici çalışanlar, stajyerler, danışmanlar, ziyaretçiler ve bilgi sistemlerine erişimi olan üçüncü taraflar için geçerlidir.

3. TEMEL İLKELER

- Ulusal ve uluslararası düzenlemelere ve standartlara uygun risk ve süreç odaklı ISO/IEC 27001:2022 ve enerji sektörüne özgü ISO/IEC 27019 standartlarına uyumlu, ölçülebilir, raporlanabilir ve denetlenebilir global bir bilgi güvenliği sistemi kurar, işletir, periyodik olarak gözden geçirir ve sürekli iyileştiririz.
- Bilgi güvenliği alanında tabi olduğumuz tüm hukuki düzenlemelere ve sözleşmelerden kaynaklanan gereksinimlere uyarız, bu gereksinimleri düzenli olarak takip eder ve uyum süreçlerini sürekli geliştiririz.

- Teknolojideki sürekli değişim ve gelişmelere ayak uydurarak; organizasyon, süreç, teknoloji ve denetim yetkinliklerini geliştiririz, PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) yaklaşımını uygularız.
- Tüm karar ve iş süreçlerimizde bilgi güvenliği ilkelerini esas alırız, bilgi güvenliği hedeflerimizi iş hedeflerimiz ile uyumlu şekilde belirler ve kurumsal stratejimizin ayrılmaz bir parçası olarak ele alırız.
- Bilgi güvenliği kapsamı çerçevesinde görev, rol ve sorumluluklar ile gerekli kaynakları belirleriz.
- Şirket olarak her türlü kurumsal ve kişisel verinin;
  - Sadece yetkili personel tarafından erişilebilmesi için gizliliğini,
  - Doğru ve tam olmasını, değişikliklerin kontrol altında tutulmasını sağlamak için bütünlüğünü,
  - Yetkili kişiler tarafından ihtiyaç duyulduğunda erişilebilir olmasını sağlamak için erişilebilirliğini

    temin ederiz ve korunmasını sağlarız.
- Bilgi varlıklarını tanımlarız; bu varlıkların gizlilik, bütünlük, erişilebilirlik ve diğer güvenlik kriterlerine ilişkin risklerini değerlendiririz. Risk temelli yaklaşımımız doğrultusunda olasılık-etki analizleri gerçekleştirir, risklerimizi kabul edilebilir seviyeye indirir ve gerekli kontrol noktalarını oluştururuz.
- En az yetki prensibi ve Sıfır Güven yaklaşımımız doğrultusunda erişim yönetimini sağlarız; kimlik, yetki ve cihaz doğrulamalarını sürekli olarak gerçekleştiririz.
- Bilgi varlıklarımızın korunmasına yönelik olarak loglama, erişim kontrolü, veri saklama, maskeleme, şifreleme ve imha gibi teknik ve idari tedbirleri uygularız.
- Müşterilerimizin bilgileri başta olmak üzere tüm kritik bilgi varlıklarımızı güvenli, izlenebilir ve yönetilebilir şekilde koruruz; iç ve dış paydaşlarımızın bilgi güvenliği beklentilerini dikkate alırız.
- İş sürekliliği, acil durum ve kriz yönetimine yönelik süreç ve senaryoları tanımlarız; kritik süreç ve sistemlerimizin kesintisiz faaliyet göstermesini sağlamak amacıyla bu planları geliştirir, uygular ve düzenli olarak test ederiz.
- Bilgi güvenliği ihlallerini ve zafiyetlerini etkin şekilde yönetmek için gerekli sistemleri kurarız; ihlallerin etkisini en aza indirmek ve tekrarını önlemek amacıyla düzeltici ve önleyici faaliyetler uygularız. Olay müdahale süreçlerini iş sürekliliği ve acil durum yönetimi ile entegre şekilde yürütürüz.
- Endüstriyel kontrol sistemleri ve kurumsal bilişim sistemlerimizin güvenliğini ve sürekliliğini sağlamak amacıyla tehdit ve zafiyetleri belirler, analiz eder, önceliklendirir ve ilgili mevzuat ve standartlara uygun şekilde yönetiriz.

- Siber güvenlik süreçlerinde güvenilir ulusal ve uluslararası tehdit istihbaratı kaynaklarını kullanarak proaktif aksiyon alırız.
- Bu politikanın duyurulmasını, erişilebilir olmasını, anlaşılmasını ve etkin şekilde uygulanmasını sağlarız.
- Bilgi güvenliği farkındalığını artırmak ve kurumsal kültürün bir parçası haline getirmek amacıyla çalışanlarımıza, iş ortaklarımıza ve diğer paydaşlarımıza yönelik düzenli eğitimler planlar ve uygularız.
- Tüm iş ortaklarımızdan faaliyet gösterdikleri ülkelerdeki bilgi güvenliği mevzuatlarına uyum sağlamalarını ve bu politika doğrultusunda hareket etmelerini bekler ve denetleriz.

Yayın Tarihi: 09.01.2026 Revizyon Tarihi: - Rev:00

Kurumsal Yönetişim Politikalarımız, stratejimizin temel taşlarından biridir ve iş kültürümüzün ayrılmaz bir parçasıdır.

aksa
ELEKTRİK