1. AMAÇ

Bu politika, **Arzum Elektrikli Ev Aletleri Sanayi ve Ticaret A.Ş.'nin** ("Arzum", "Şirket") bilgi güvenliği sistem ve uygulamalarını tanımlamaktadır. Arzum, bilgi güvenliğini yasal zorunluluklar ve mevzuatlar çerçevesinde mevcut ve oluşabilecek riskleri de yöneterek sağlamayı, sürekli olarak iyileştirmeyi, geliştirmeyi ve gözden geçirmeyi taahhüt eder.

Arzum'da bilgi sistemlerinin yönetimi, kurumsal yönetim uygulamalarının bir parçası olarak ele alınır. Arzum operasyonlarını istikrarlı, rekabetçi, gelişen ve güvenli bir çizgide sürdürebilmek için bilgi sistemlerine ilişkin stratejilerin iş hedefleri ile uyumlu olmasını sağlar. Arzum'da bilgi sistemleri yönetimine ilişkin olarak bilgi sistemlerinin güvenlik, performans, etkinlik, doğruluk ve sürekliliği hedeflenerek bu hususların doğru yönetimi için gerekli finansman ve insan kaynağı tahsis edilir.

2. KAPSAM

Bu politika, Arzum'un teknolojisini, bilgi birikimini, veri sorumlusu veya veri işleyen sıfatı ile işlediği kişisel verileri ve özel nitelikli kişisel verileri ve bu suretle itibarını koruyabilmek için "Kapsam, Sınırlar, Bağlam ve İlgili Taraflar" dokümanında tanımlanmış olan bilgi ve bilgi kaynaklarının gizliliğinin, erişilebilirliğinin ve bütünlüğünün sağlanmasını hedefler.

Bu politika, Arzum bilgisini ve iş sistemlerini kullanmakta olan tüm çalışanlar ve şirket adına çalışan danışmanları kapsamaktadır.

3. TANIMLAR VE KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi

BGYS Ekibi: BGYS ekibi yönetimi temsil eden, BGYS'nin başarılı biçimde sürdürülebilmesi için sorumluluğu üstlenen ve gözetimini sağlayan organizasyondur.

BGYS İç Denetçisi: BGYS'nin uygulanmasından ve işletiminden bağımsız, BGYS denetimini yerine getirebilecek deneyim, eğitim ve sertifikasyonlara sahip kişi olup BGYS'nin iç denetimini gerçekleştiren kişidir. İç denetçi kurum personeli olabileceği gibi kurum dışından da sağlanabilir.

KVKK: 6698 sayılı Kişisel Verilerin Korunması Kanunu

4. SORUMLULUKLAR

Üst Yönetim: Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya kurum politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur. Üst yönetimi temsilen bu görevi BGYS Temsilcisi yapar ve Genel Müdür Yardımcısına tasdik ettirir.

BGYS Temsilcisi: Bilgi Güvenliği Yönetim sisteminin kurulmasından işletilmesi ve yönetilmesine dek her aşamada üst yönetime karşı sorumluluk üstlenen kişidir.

BGYS Ekibi: Şirket'in üst yönetimi tarafından görevlendirilen BGYS ekibi, Bilgi Güvenliği Politikasının Şirket ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya kurum politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.

Tüm Personel: Bilgi Güvenliği Politikasının gereklerinin görev alanlarının gerektirdiği biçimde yerine getirilmesinden sorumludur.

5. UYGULAMA

5.1 Yönetim Desteği

- Üst yönetim, BGYS ekibi çatısı altında gerçekleştirdiği faaliyetler, BGYS Temsilcisi ve BGYS İç Denetçi personel atamaları, BGYS yatırım, masraf ve eğitim bütçeleri, yönetim gözden geçirme aktiviteleri ile fiili olarak BGYS'yi destekler.
- Üst yönetim, BGYS politika ve prosedürlerine uyarak ve uyulmasını teşvik ederek BGYS hedeflerine ulaşmak için liderlik eder.
- Üst yönetim, bilgi güvenliği risklerinin yönetiminin kurumun itibarı ve faaliyetlerin sürekliliği açısından önemini yönetsel faaliyetleri uygulayarak ve kurumsal politikalar aracılığı ile ifade eder.
- Yılda en az bir kez riskleri değerlendirir ve Bilgi Güvenliği Politikasını gözden geçirerek sistemin sürekliliğini, sürdürülebilirliğini temin eder.

5.2 Bilgi Güvenliği Politikası

Arzum nezdinde bulunan her türlü bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden ve dışarıdan gelebilecek tüm tehditlerden korunması ve yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesini temin etmek üzere Şirket, ISO 27001 Bilgi Güvenliği Yönetim Sistemini (BGYS) kurmuş ve şartlarını yerine getirmeyi, etkinliğini sürdürmeyi ve sürekli geliştirme faaliyetini devam ettirmeyi, yasal şartlar, standart gereksinimleri, sözleşme şartları ile yükümlülükleri ve müşteri şartlarını da göz önünde bulundurarak, mevcut ve oluşabilecek riskleri de dikkate almak yoluyla bilgi güvenliği gereksinimlerini karşılamayı politikası olarak belirlemiş ve ilgili taraflara sunmuştur. Bu doğrultuda; personelini, sistemlerini, bilgi ve varlıklarını, kişisel veri envanterlerini, uyulması gereken iş kurallarını, ölçülebilir ve uygulanabilir hedefler ile sürekli gözden geçirerek, güncelleyerek bu hedefler kapsamında iş sürekliliğini sağlayarak ilerlemektedir.

Bilgi Güvenliği kapsamında temel hedeflerimiz kapsamında;

- ✓ Şirketimiz güvenirliğini ve itibarını korumayı,
- ✓ Bilgi güvenliği yönetim sistemimizin ISO 27001:2013 standardının gereklerini yerine getirecek şekilde dokümante edilmesi, belgelendirilmesi ve sürekli iyileştirilmesini sağlamayı,
- ✓ Tüm çalışanlarımızın bilgi güvenliği farkındalığını artırmayı,
- ✓ Stratejik iş planı ve risk yönetimi çerçevesinde, bilgi güvenliği yönetim sisteminin kurulup sürekliliğinin sağlanması için ilgili riskleri tanımlamayı, belirlemeyi, değerlendirmeyi ve kontrol etme işlevini yerine getirmeyi,
- ✓ Bilgi güvenliği ile ilgili tüm yasal mevzuat ve sözleşmelere uyulmasını,
- ✓ Bilgi varlıklarına yönelik risklerin sistematik olarak yönetilmesini,
- ✓ Şirketimiz ve iş ilişkimiz ya da ticari faaliyetlerimiz dolayısıyla aldığımız ve korumakla yükümlü olduğumuz tüm paydaş bilgilerinin gizliliğini ve bütünlüğünü sağlamayı,
- ✓ Kişisel veri envanterlerinde bulunan ve Şirket faaliyetleri kapsamında işlenen kişisel verilerin ve özel nitelikli kişisel verilerin hukuka aykırı işlenmesini ve erişilmesini önelemeyi,
- ✓ Kişisel verilerin ve özel nitelikli kişisel verilerin KVKK hükümlerine uygun olarak muhafazasını sağlamayı,
- ✓ Sektör içerisinde bilgi güvenliği açısından örnek bir kuruluş olmak için özveri ile çalışmayı

taahhüt ederiz.

5.2.1 Gözden Geçirme ve İyileştirme

Arzum'un bilgi güvenliği yönetim sisteminin uygunluğu, yeterliliği ve etkinliğinin gözden geçirilmesi Kalite Departmanı ve Bilgi Teknolojileri Departmanı tarafından sağlanır. Öyle ki; bilgi sistemleri kontrolleri kapsamında her kontrol süreci için süreç sahibinin, rollerin, faaliyetlerin ve sorumlulukların açık bir şekilde tanımlanması, kontrol süreçlerinin periyodik biçimde tanımlanması, her kontrol sürecinin hedef ve amaçlarının açıkça tanımlanmış olması ve performansının ölçülebilir olması da yine Bilgi Teknolojileri Departmanı gözetimindedir. Bilgi Teknolojileri Departmanının öncülüğünde, gerekli durumlarda tüm bilgi güvenliği sistemlerine ilişkin bağımsız gözden geçirme yapılır ve elde edilen sonuçlar, yönetime raporlanarak saklanır.

5.2.2 Yetki ve Sorumluluk

Bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik olarak Üst yönetim, asgari olarak aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

- Bilgi güvenliği politikalarının ve tüm sorumlulukların her yıl gözden geçirilmesi ve gerekli durumlarda yapılacak güncellemelerin onaylanması,
- Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,
- Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,
- Tüm çalışanların her yıl bilgi güvenliği ve kişisel verilerin korunması farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi için gerekli kaynağın sağlanması,
- Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreçlerin fiili olarak işleyecek şekilde gözetim ve takiplerinin yapılmasının sağlanması,
- Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir bilgi sistemleri güvenliği sorumlusunun belirlenmesi,
- Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için Bilgi Teknolojileri Departmanı tarafından hazırlanan iş sürekliliği planının incelenmesi ve planda kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybının belirlenmesi.

6. DAĞITIM

Bu politika, Arzum bilgisini ve iş sistemlerini kullanmakta olan tüm çalışanları, Şirket adına çalışan danışmanları ve ilgili tarafları kapsamaktadır.

7. YAPTIRIM

Bu dokumana aykırı davranılması durumunda **Disiplin Yönetmeliği** dikkate alınarak işlem yapılacaktır.

8. YÜRÜRLÜK

İşbu Politikası 15.06.2022 tarihli ve 2022/018 numaralı Yönetim Kurulu Kararı ile düzenlenerek yürürlüğe girmiş olup, bu politikada yapılacak değişiklikler Yönetim Kurulu onayına tabidir.