ARSAN HOLDİNG A.Ş. BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Bu politikanın amacı; Arsan Holding A.Ş. ("Şirket") bünyesindeki bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini güvence altına almak; olası güvenlik ihlallerini önlemek, kurumsal itibarı, paydaşların, yatırımcıların ve müşterilerin verilerini korumaktır. Politika, bilgi varlıklarının iş sürekliliğinin sağlanması, siber risklerin yönetilmesi ve varlıkların iş amaçlarına uygun kullanılması için gerekli kuralları ve kurumsal yaklaşımları tanımlar.

2. Kapsam

Bu politika; Arsan Holding A.Ş. bünyesinde kullanılan tüm bilgi sistemleri, veri tabanları, ağ altyapısı, uygulamalar, bulut sistemleri, hizmet sağlayıcılar, yazılım ve donanım çözümlerini kapsar. Şirket içi tüm birimleri, çalışanları, yöneticileri, stajyerleri, taşeronları ve bilgi sistemleri ağını kullanan tüm üçüncü taraf hizmet sağlayıcıları ile iş ortaklarını bağlar.

3. Temel Güvenlik İlkeleri ve ISO 27001 Uyumu

Şirket faaliyetleri yürütülürken bilginin alınması, oluşturulması, işlenmesi, aktarılması, tutulması ve arşivlenmesi süreçlerinde **Bilgi Güvenliği Yönetim Sistemi (BGYS)** standartları (ISO/IEC 27001) uygulanır. Bilgi güvenliği yönetimi şu üç temel sacayağına dayanır:

- **Gizlilik:** Bilginin sadece yetkilendirilmiş kişiler tarafından erişilebilir olması.
- **Bütünlük:** Bilginin yetkisiz kişilerce değiştirilememesi, silinememesi veya bozulmaması.
- **Erişilebilirlik:** Bilginin, ihtiyaç duyulduğunda yetkili kullanıcılar tarafından kesintisiz kullanılabilir olması.

4. Kurumsal Yönetişim, Sermaye Piyasası Mevzuatı ve Yatırımcı Hakları

Şirketimiz halka açık bir ortaklık olmanın getirdiği sorumluluk bilinciyle, siber güvenliği finansal istikrarın ve yatırımcı güveninin ayrılmaz bir parçası olarak görür:

- **İçsel Bilgilerin Güvenliği:** Kamuya açıklanmamış içsel bilgilerin, finansal raporların ve stratejik verilerin siber casusluk veya sızıntılara karşı korunması esastır. Bu verilere erişim "bilmesi gereken" prensibine göre kısıtlanır ve İçsel Bilgilere Erişenler Listesi (Insider List) ile tam uyumlu yönetilir.
- **KAP Veri Giriş Güvenliği:** Kamuyu Aydınlatma Platformu (KAP) sistemine veri girişi sağlayan yetkili personelin kullanıcı hesapları ve donanımları, Çok Faktörlü Doğrulama (MFA) ve özel siber savunma araçları ile en üst düzeyde korunur.

- **Sürdürülebilirlik ve ESG Uyumu:** Şirketimiz siber güvenliği bir Çevresel, Sosyal ve Yönetişim (ESG) kriteri olarak kabul eder. Bu alandaki kurumsal olgunluk ve performans, yıllık faaliyet ve sürdürülebilirlik raporlarında şeffafça paylaşılır.

5. Risk Yönetimi, Finansal Koruma ve Bağımsız Denetim

- **Finansal Etki Yönetimi:** Siber risklerin şirket hisse değeri ve karlılığı üzerindeki olumsuz etkilerini azaltmak amacıyla siber sigorta (Cyber Insurance) dahil finansal koruma mekanizmaları değerlendirilir. Risk analizleri, Yönetim Kurulu bünyesindeki **Riskin Erken Saptanması Komitesi**'ne düzenli olarak raporlanır.
- **Bağımsız Bilgi Sistemleri Denetimi:** Şirket bilgi sistemleri ve güvenlik altyapısı, SPK'nın VII-128.10 sayılı Tebliği uyarınca, yılda en az bir kez bağımsız bilgi sistemleri denetim firmaları tarafından denetlenir ve raporlar **Denetimden Sorumlu Komite**'ye sunulur.

6. Sorumluluklar ve Organizasyonel Yapı

- **Çalışan Taahhüdü ve Farkındalık:** Tüm kullanıcılar bu politikayı okuyarak kurallara uymayı taahhüt eder. Personelin siber farkındalığını artırmak üzere düzenli olarak teknik, pratik (oltalama simülasyonları vb.) ve davranışsal eğitimler düzenlenir.
- **Yönetim Yapısı:** BGYS'nin günlük operasyonel işletilmesinden **Bilgi İşlem Personeli** sorumludur. Sistemin kurulması, yürütülmesi, risk yönetimi ve sürekli geliştirilmesinden üst yönetime doğrudan bağlı çalışan **Bilgi Güvenliği Sorumlusu** yetkili ve sorumludur.

7. Kullanıcı Sorumlulukları ve Erişim Kontrolü

- **Parola Politikası:** Hesaplarda en az 8 karakterden oluşan, büyük/küçük harf, rakam ve özel karakter içeren karmaşık parolalar zorunludur. Parolalar hiçbir surette paylaşılamaz.
- **Cihaz ve Çalışma Alanı Güvenliği:** Ofis içi veya uzaktan çalışmalarda bilgisayardan ayrılırken ekranlar kilitlenmelidir. Taşınabilir cihazlar (laptop, şifreli USB vb.) fiziksel hırsızlığa karşı koruma altına alınmalıdır. "Temiz Masa ve Temiz Ekran" ilkesi uyarınca, gizlilik dereceli basılı evraklar masada bırakılamaz, kilitli dolaplarda saklanır.

8. E-Posta, İnternet ve Ağ Güvenliği

- Kurumsal e-posta adresleri kişisel amaçlarla kullanılamaz. Kaynağı bilinmeyen e-postalar açılmamalı, ekleri indirilmemeli ve bağlantılarına tıklanmamalıdır.
- Şirket ağı üzerinden yasa dışı, telif hakkı ihlali barındıran veya zararlı yazılım içeren web sitelerine erişim sistem seviyesinde engellenir ve bu sitelere giriş yasaktır.

9. Veri Yedekleme, Donanım ve Yazılım Güvenliği

- Kurumsal ve finansal veriler, iş sürekliliği planları çerçevesinde belirlenen periyotlarda şifreli ve yedekli olarak güvenli ortamlarda saklanır.
- Verilerin işlenmesinde başta KVKK (Kişisel Verilerin Korunması Kanunu) ve SPK tebliğleri olmak üzere tüm yasal mevzuata tam uyum sağlanır. Veriler yetkisiz üçüncü taraflarla paylaşılamaz.

- Şirket donanımlarına izinsiz, lisanssız yazılım yüklenmesi yasaktır. Merkezi antivirüs, EDR (Uç Nokta Tehdit Algılama) ve Güvenlik Duvarı (Firewall) sistemleri daima aktif tutulur. Sistem odalarına fiziksel erişim sıkı şekilde kontrol edilir.

10. İhlal Bildirimi, Kamuyu Aydınlatma ve Yaptırımlar

- **Olay Müdahale ve KAP Bildirimi:** Şirketin iş sürekliliğini, operasyonlarını veya finansal yapısını önemli ölçüde etkileyebilecek siber güvenlik ihlalleri; SPK'nın Özel Durumlar Tebliği (II-15.1) ve KVKK mevzuatı çerçevesinde yasal süreleri içinde ivedilikle **Kamuyu Aydınlatma Platformu (KAP)** ve ilgili otoriteler üzerinden kamuoyuna duyurulur.
- **Disiplin Süreçleri:** Bu politikayı kasıtlı olarak ihlal eden, ihmalkar davranan veya şirket verilerini riske atan personel hakkında disiplin yönetmeliği hükümleri ve gerekli hukuki/cezai işlemler başlatılır.

11. Yürürlük ve Gözden Geçirme

İşbu politika, Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girer. Yılda en az bir kez veya şirketin altyapısında/mevzuatta önemli bir değişiklik olması durumunda sistematik olarak gözden geçirilerek güncellenir.

ARSAN HOLDİNG A.Ş.