BİLGİ GÜVENLİĞİ POLİTİKASI

MADDE 1. AMAÇ ve KAPSAM

İşbu Bilgi Güvenliği Politikasının ("Politika") amacı, Akfen Holding Anonim Şirketi ("Akfen Holding" veya "Şirket") ve bağlı şirketlerinin (Akfen Holding ve bağlı ortaklıkları birlikte "Şirketler"), Şirketler'in iş sürekliliğini sağlamak ve potansiyel tehditlerin etkisini azaltmak için bilgi güvenliği olaylarını engellemek veya hasar riskini minimize etmektir.

MADDE 2. BİLGİ GÜVENLİĞİ

Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir şirket için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği iş sürekliliğini sağlamak, kayıpları en aza indirmek için bilgiyi tehlike ve tehdit alanlarından korur. Bilgi güvenliği, Politika'da aşağıdaki bilgi niteliklerinin korunması olarak tanımlanmaktadır:

Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesi

Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunun ve yetkisiz değiştirilememesinin temin edilmesi

Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerinin garanti edilmesi

MADDE 3. BİLGİ SİSTEMLERİ YÖNETİMİ

Bilgi Sistemleri Yönetimine şunlar dahildir:

(i) Bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi,
(ii) Bilgi güvenliği politikasının personele duyurulması,
(iii) Bilgi güvenliği politikasının uygulanması, gözetimi ve kontrolü
(iv) Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projelerin gözden geçirilmesi ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanması,
(v) Bilgi güvenliği önlemlerinin uygun düzeye getirilmesi ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis edilmesi,
(vi) Bilgi güvenliği politikalarının ve tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması,
(vii) 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,
(viii) Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,
(ix) Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi,
(x) Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürlerin, Şirketler'in organizasyonel ve yönetsel yapısı içerisinde fiili olarak işleyecek şekilde yerleştirilmesi ve işlerliğine ilişkin gözetim ve takiplerin gerçekleştirilmesi,
(xi) Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlanması,
(xii) Bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak üzere

bulunan verilerin gizlilik, bütünlük ve erişilebilirliklerini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesinin, işletilmesinin, güncelliğinin sağlanması ve gerekli yönetsel sorumlulukların tanımlanması,

(xiii) Şirketler'in sahip oldukları bilgi varlıklarını ve bu varlıkların sorumlularının belirlenmesi, bu varlıkların envanterinin oluşturulması ve envanterin güncelliğinin sağlanması, bilgi varlıklarının önem derecelerine göre sınıflandırılması,

(xiv) Fiziksel erişimin yalnızca yetkilendirilmiş kişilerce yapılmasını sağlamak amacıyla, güvenli alanların gerekli giriş kontrolleriyle korunmasının sağlanması,

(xv) Yangın, sel, deprem, patlama, yağma ve diğer doğal ya da insan kaynaklı felaketlerden kaynaklanan hasara karşı fiziksel koruma tasarlanması ve uygulanması,

(xvi) Ağların tehditlere karşı korunması ve ağları kullanan sistem, veri tabanı ve uygulamaların güvenliğinin sağlanması için kontroller tesis edilmesi ve etkin bir şekilde yönetilmesi,

(xvii) Bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli önlemlerin alınması,

(xviii) Bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemlerin alınması,

(xix) Bilgi sistemleri üzerindeki risklerin, sistem veya faaliyetlerin karmaşıklığını ve kapsamının genişliğini göz önünde bulundurarak bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizmasının tesis edilmesi,

(xx) Bu hizmetlerin dışarıdan alınmasına ilişkin iş ve işlemlerin yürütülmesi.

MADDE 4. ÇALIŞAN VE ÜÇÜNCÜ KİŞİ SORUMLULUĞU

Bilgi Güvenliği Politikası'na uyum, ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, Şirketler'in bilgilerini ve/veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve şirket bilgilerine, sağladığı hizmet nedeniyle erişimi olan üçüncü kişi hizmet sağlayıcıları ve bunların bağlı destek personelinin, Politika düzenleme ve yükümlülüklerine bağlı hareket etmesi şarttır.

Şirketler'in bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişenler:

(i) Kişisel ve elektronik iletişimde Şirketler'e ait bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlarlar.

(ii) Risk düzeylerine göre belirlenen güvenlik önlemlerini alırlar.

(iii) Bilgi güvenliği ihlal olaylarını bildirerek raporlar ve bu ihlalleri engelleyecek önlemleri alırlar.

(iv) Şirket içi bilgi kaynaklarını (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletmezler.

(v) Bilişim kaynaklarını, mevzuata aykırı faaliyetler amacıyla kullanmazlar.

(vi) Yatırımcılar, iş ortakları, tedarikçiler veya diğer üçüncü kişilere ait bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korurlar.

MADDE 5. RİSK YÖNETİMİ

Risk yönetim çerçevesi; bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar, risk analizi ve risk işleme planı bilgi güvenliği ve hizmet yönetimi risklerinin nasıl kontrol edildiğini tanımlar.

MADDE 6. KONTROL, GÖZETİM VE SORUMLULUK

Bilgi Güvenliği Politikası ihlalleri, Şirketler'in risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca hukuki, idari ve/veya cezai sorumluluğuna sebep olabilecektir. Dolayısıyla, Politika'da açıkça düzenlenen kontrol ve gözetim sorumlulukları dışında, Şirketler'in her birim yöneticisi de Bilgi Güvenliği Politikası'na uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetmekten sorumludur.

MADDE 7. İLETİŞİM

E-posta: surdurulebilirlik@akfen.com.tr
Adres: Ankara Merkez Ofis Kazım Özalp Mahallesi, Koza Caddesi No:22 Çankaya Ankara / Turkey 06700

MADDE 8. YÜRÜRLÜK

İşbu Politika, Akfen Holding'in 10.09.2026 tarihli Yönetim Kurulu kararıyla kabul edilmiş olup yayımı tarihinde yürürlüğe girmiştir.

İşbu Politika Yönetim Kurulu tarafından yürürlükten kaldırılmadığı veya değiştirilmediği sürece geçerliliğini korur.