

|                                                                                   |                                   |                 |                 |   |
|-----------------------------------------------------------------------------------|-----------------------------------|-----------------|-----------------|---|
|  | <b>Bilgi Güvenliđi Politikası</b> |                 |                 |   |
|                                                                                   | Doküman No                        | Hol_Sur_Pol_5.1 | Revizyon Tarihi | - |
|                                                                                   | Yayın Tarihi                      | 16.08.2024      | Revizyon No     | - |

## Bilgi Güvenliđi Politikası

### MADDE 1- AMAÇ

Şirket, kurumsal bilgiyi son derece değerli bir varlık olarak kabul etmektedir. Şirket Bilgi Güvenliđi Politikası ("Bilgi Güvenliđi Politikası" veya "Politika")'nın amacı da, Şirket ve bađlı ortaklıklarının iş sürekliliđini sağlamak ve potansiyel tehditlerin etkisini azaltmak için bilgi güvenliđi olaylarını engellemek veya hasar riskini minimize etmektir.

### MADDE 2- KAPSAM

Bilgi Güvenliđi Politikası, tüm lokasyonlardaki çalışanlar, lokasyon içi ve dışı tedarikçiler / yüklenici tarafından uygulanır.

### MADDE 3- BİLGİ GÜVENLİĐİ

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

Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduđunun garanti edilmesi  
Bütünlük: Bilginin ve işleme yöntemlerinin doğruluđunun ve yetkisiz deđiştirilememesinin temin edilmesi  
Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduđunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerinin garanti edilmesi

### MADDE 4- BİLGİ SİSTEMLERİ YÖNETİMİ

Bilgi Sistemleri Yönetimine şunlar dahildir:

- (i) Bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi,
- (ii) Bilgi güvenliđi politikasının personele duyurulması,
- (iii) Bilgi güvenliđi politikasının uygulanması, gözetimi ve kontrolü
- (iv) Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projelerin gözden geçirilmesi ve bunlara ilişkin risklerin yönetilebilirliđi göz önünde bulundurularak onaylanması,
- (v) Bilgi güvenliđi önlemlerinin uygun düzeye getirilmesi ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynađı tahsis edilmesi,
- (vi) Bilgi güvenliđi 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 güvenliđi ihlallerine ilişkin olayların izlenmesi ve her yıl deđerlendirilmesi,
- (ix) Tüm çalışanların bilgi güvenliđi farkındalıđını artırmaya yönelik çalışmaların yapılması ve eđitimlerin verilmesi,



## Bilgi Güvenliđi Politikası

|              |                 |                 |   |
|--------------|-----------------|-----------------|---|
| Doküman No   | Hol_Sur_Pol_5.1 | Revizyon Tarihi | - |
| Yayın Tarihi | 16.08.2024      | Revizyon No     | - |

- (x) Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürlerin, Şirket'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 sürekliliđini sağlamak için iş sürekliliđi 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, güncelliđinin sağlanması ve gerekli yönetsel sorumlulukların tanımlanması,
- (xiii) Şirket'in sahip olduđu bilgi varlıklarını ve bu varlıkların sorumlularının belirlenmesi, bu varlıkların envanterinin oluşturulması ve envanterin güncelliđinin 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 diđer 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 gizliliđini sağlayacak önlemlerin alınması,
- (xix) Bilgi sistemleri üzerindeki risklerin, sistem veya faaliyetlerin karmaşıklıđını ve kapsamının genişliđini 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 5- ÇALIŞAN VE ÜÇÜNCÜ KİŞİ SORUMLULUĐU

Bilgi Güvenliđi Politikası'na uyum, ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, Akfen Holding ve/veya bađlı ortaklık bilgilerini veya iş sistemlerini kullanan tüm personel için, cođrafik konumdan veya iş biriminden bađımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve Şirket bilgilerine, sağladıđı hizmet nedeniyle erişimi olan üçüncü kişi hizmet sağlayıcıları ve bunların bađlı destek personelinin Politika düzenleme ve yükümlülüklerine bađlı hareket etmesi şarttır.

Şirket bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişenler:

- (i) Kişisel ve elektronik iletişimde Şirket'e ait bilginin gizliliđini, bütünlüğünü ve erişilebilirliğini sağlarlar.
- (ii) Risk düzeylerine göre belirlenen güvenlik önlemlerini alırlar.
- (iii) Bilgi güvenliđi ihlal olaylarını bildirerek raporlar ve bu ihlalleri engelleyecek önlemleri alırlar.
- (iv) Şirket içi bilgi kaynaklarını (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletmezler.

|                                                                                   |                                   |                 |                 |   |
|-----------------------------------------------------------------------------------|-----------------------------------|-----------------|-----------------|---|
|  | <b>Bilgi Güvenliđi Politikası</b> |                 |                 |   |
|                                                                                   | Doküman No                        | Hol_Sur_Pol_5.1 | Revizyon Tarihi | - |
|                                                                                   | Yayın Tarihi                      | 16.08.2024      | Revizyon No     | - |

- (v) Şirket bilişim kaynaklarını, mevzuata aykırı faaliyetler amacıyla kullanmazlar.
- (vi) Yatırımcılar, iş ortakları, tedarikçiler veya diđer üçüncü kişilere ait bilgilerin gizliliđini, bütünlüğünü ve erişilebilirliğini korurlar.

## **MADDE 6- RİSK YÖNETİMİ**

Şirket'in risk yönetim çerçevesi; bilgi güvenliđi risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar, risk analizi ve risk işleme planı bilgi güvenliđi ve hizmet yönetimi risklerinin nasıl kontrol edildiđini tanımlar.

## **MADDE 7- KONTROL VE GÖZETİM**

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