

BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Ahlatıcı Holding A.Ş. ("Şirket"), faaliyetlerinin sürdürülebilirliği, bilgi varlıklarının korunması ve güvenilir hizmet sunulması amacıyla bilgi güvenliğini temel önceliklerinden biri olarak kabul etmektedir.

Bu Bilgi Güvenliği Politikası'nın amacı;

- * Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda korunmasını,
- * Bilgi güvenliği risklerinin etkin şekilde yönetilmesini,
- * Yetkisiz erişim, kullanım, açıklama, değiştirme veya kayıp risklerinin azaltılmasını,
- * Bilgi güvenliği farkındalığının geliştirilmesini,
- * Yasal ve düzenleyici yükümlülüklerle uyum sağlanmasını

temin etmektedir.

2. KAPSAM

Bu politika;

- * Ahlatıcı Holding A.Ş. çalışanlarını,
- * yöneticilerini,
- * stajyerleri,
- * danışmanları,
- * hizmet sağlayıcıları,
- * iş ortaklarını,
- * Şirket bilgi varlıklarına erişimi bulunan tüm üçüncü tarafları

kapsar.

Politika; elektronik ortamda bulunan bilgiler, fiziksel belgeler, bilgi sistemleri, iletişim altyapıları ve bilgi işleme süreçleri için uygulanır.

3. BİLGİ GÜVENLİĞİ TEMEL İLKELERİ

Ahlatıcı Holding A.Ş., bilgi güvenliği yönetimini aşağıdaki temel ilkeler doğrultusunda yürütür:

3.1. Gizlilik

Bilgilere yalnızca yetkilendirilmiş kişi ve sistemlerin erişebilmesi sağlanır.

Gizli bilgiler; yetkisiz erişime, izinsiz paylaşımına ve kötüye kullanımına karşı korunur.

3.2. Bütünlük

Bilgilerin doğruluğunun, eksiksizliğinin ve güvenilirliğinin korunması sağlanır. Yetkisiz değişikliklerin önlenmesi için gerekli teknik ve idari kontroller uygulanır.

3.3. Erişilebilirlik

Yetkili kullanıcıların ihtiyaç duydukları bilgi ve sistemlere zamanında erişebilmesi sağlanır. Bilgi sistemlerinin sürekliliği için gerekli yedekleme, bakım ve iyileştirme çalışmaları gerçekleştirilir.

4. BİLGİ VARLIKLARININ YÖNETİMİ

Şirket, sahip olduğu bilgi varlıklarını belirler, sınıflandırır ve uygun güvenlik seviyelerine göre koruma altına alır.

Bilgi varlıkları kapsamında; kurumsal bilgiler, finansal bilgiler, müşteri bilgileri, çalışan bilgileri, kişisel veriler, yazılım ve donanım varlıkları ve elektronik kayıtlar yer almaktadır.

5. ERIŞİM KONTROLÜ

Bilgi sistemlerine erişimler; görev gereklilikleri, yetki seviyeleri ve iş ihtiyaçları esas alınarak sınırlandırılır.

Şirket;

- * kullanıcı hesaplarının yönetimini,
- * yetkilendirme süreçlerini,
- * erişim kayıtlarının izlenmesini,
- * gereksiz erişimlerin kaldırılmasını

sağlamak için gerekli kontrolleri uygular.

6. PAROLA VE KİMLİK DOĞRULAMA GÜVENLİĞİ

Kullanıcılar;

- * kendilerine tanımlanan erişim bilgilerini gizli tutmak,
- * başkalarıyla paylaşmamak,
- * güçlü parola kullanmak,
- * şüpheli durumları bildirmek

ile yükümlüdür.

Gerekli görülen sistemlerde çok faktörlü kimlik doğrulama yöntemleri uygulanabilir.

7. BİLGİ TEKNOLOJİLERİ KULLANIMI

Çalışanlar, Şirket tarafından sağlanan bilgi teknolojileri kaynaklarını; güvenli, hukuka uygun ve iş amaçlarıyla uyumlu şekilde kullanmalıdır.

Bilgi sistemlerinin;

- * yetkisiz yazılımlar,
- * zararlı içerikler,
- * güvenlik açıkları

nedeniyle riske atılmasına izin verilmez.

8. KİŞİSEL VERİLERİN GÜVENLİĞİ

Ahlatıcı Holding A.Ş., kişisel verilerin korunmasına yönelik olarak;

- * 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- * ilgili mevzuat,
- * Kişisel Verileri Koruma Kurulu kararları

ile uyumlu hareket eder.

Kişisel verilerin güvenliğinin sağlanması amacıyla gerekli teknik ve idari tedbirler uygulanır.

9. VERİ YEDEKLEME VE İŞ SÜREKLİLİĞİ

Şirket, kritik bilgi varlıklarının sürekliliğini sağlamak amacıyla;

- * düzenli yedekleme,
- * veri kurtarma,
- * iş sürekliliği planları,
- * felaket kurtarma süreçleri

oluşturur ve gerektiğinde günceller.

10. BİLGİ GÜVENLİĞİ OLAYLARININ YÖNETİMİ

Bilgi güvenliği olayları;

- * yetkisiz erişim,
- * veri kaybı,
- * zararlı yazılım,
- * bilgi sızıntısı,
- * sistem kesintisi

gibi durumları kapsayabilir.

Tespit edilen bilgi güvenliği olayları en kısa sürede ilgili birimlere bildirilir ve gerekli inceleme süreçleri yürütülür.

11. ÜÇÜNCÜ TARAF BİLGİ GÜVENLİĞİ

Şirket ile bilgi erişimi bulunan üçüncü tarafların;

- * bilgi güvenliği kurallarına uyması,
- * gizlilik yükümlülüklerini yerine getirmesi,
- * gerekli güvenlik tedbirlerini uygulaması

beklenir.

Gerekli durumlarda üçüncü taraflarla bilgi güvenliği hükümleri içeren sözleşmeler yapılır.

12. FİZİKSEL GÜVENLİK

Bilgi işleme ortamları ve fiziksel bilgi varlıklarının korunması amacıyla;

- * yetkisiz erişimlerin önlenmesi,
- * güvenli alan uygulamaları,
- * fiziksel erişim kontrolleri

uygulanır.

13. ÇALIŞANLARIN SORUMLULUKLARI

Tüm çalışanlar;

- * bilgi güvenliği politikalarına uymak,
- * kendilerine verilen erişim yetkilerini doğru kullanmak,
- * güvenlik ihlallerini bildirmek,
- * gizli bilgileri korumak ile sorumludur.

14. BİLGİ GÜVENLİĞİ FARKINDALIĞI

Şirket, çalışanların bilgi güvenliği konusunda bilinçlendirilmesi amacıyla; eğitimler, bilgilendirmeler ve farkındalık çalışmaları gerçekleştirebilir.

15. DENETİM VE İZLEME

Bilgi güvenliği uygulamalarının etkinliği;

- * iç kontroller,
- * denetimler,
- * teknik izleme faaliyetleri

aracılığıyla değerlendirilebilir.

Tespit edilen uygunsuzluklar için gerekli iyileştirme çalışmaları gerçekleştirilir.

16. POLİTİKANIN İHLALİ

Bu politikaya aykırı davranışlar;

- * bilgi güvenliği risklerine,
- * hukuki sorumluluklara,
- * kurumsal itibar kaybına

neden olabilir. Politika ihlalleri, Şirket iç düzenlemeleri kapsamında değerlendirilir.

17. YÜRÜRLÜK VE GÜNCELLEME

Ahlatcı Holding A.Ş., teknolojik gelişmeler, mevzuat değişiklikleri ve kurumsal ihtiyaçlar doğrultusunda bu Bilgi Güvenliği Politikası'nı güncelleme hakkını saklı tutar.

Güncellenen politika yayımlandığı tarihten itibaren yürürlüğe girer.

İLETİŞİM BİLGİLERİ

Ahlatıcı Holding A.Ş.

Adres:

E-posta:

Telefon:

Web Sitesi:

KEP Adresi: