1. AMAÇ

Bu politikanın amacı; ARK Dijital Yazılım A.Ş.'nin bilgi varlıklarını, bilgi sistemlerini, KEPHS yetkilendirme sürecinde kullanılan altyapı ve hizmetlerini, kişisel verileri, KEP delillerini, işlem kayıtlarını ve kritik iş süreçlerini gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda korumak için uygulanacak bilgi güvenliği yönetim çerçevesini tanımlamaktır.

Bu politika, ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi gereklilikleri, KEP mevzuatı, BTK düzenlemeleri, KVKK ve ilgili teknik usul/esaslar dikkate alınarak hazırlanmıştır. Politika, üst yönetimin bilgi güvenliği taahhüdünü, uygulanacak temel ilkeleri ve denetlenebilir sorumluluk yapısını ortaya koyar.

2. KAPSAM

Bu politika; ARK Dijital Yazılım A.Ş.'nin tüm çalışanlarını, yöneticilerini, dış kaynak hizmet sağlayıcılarını, tedarikçilerini, bilgi sistemlerini, uygulamalarını, ağ ve güvenlik altyapısını, veri merkezlerini, kayıt saklama ortamlarını ve KEPHS yetkilendirmesi kapsamında yürütülen faaliyetlerini kapsar.

Politika kapsamındaki başlıca alanlar şunlardır:

- KEP hizmetleri, KEP hesabı yönetimi, KEP rehberi, KEP delili üretimi, saklanması ve doğrulanması
- Elektronik kayıt saklama, elektronik veri arşivleme ve uzun dönem doğrulama süreçleri
- Kimlik doğrulama, işlem yetkilisi yönetimi, video doğrulama, PAdES ve elektronik imza süreçleri
- İşlem sertifikası, zaman damgası, sertifika doğrulama, CRL/OCSP, HSM/Ark Signer ve kriptografik anahtar yönetimi
- Kişisel veri işleme faaliyetleri, KVKK uyumu, veri sahibi hakları, saklama/imha ve kişisel veri ihlal yönetimi
- Sunucular, veri tabanları, ağ bileşenleri, güvenlik cihazları, uç kullanıcı cihazları ve yedekleme ortamları
- Loglama, izleme, olay müdahale, zafiyet yönetimi, erişim kontrolü, tedarikçi güvenliği ve iş sürekliliği ile ilişkili bilgi güvenliği kontrolleri

3. REFERANSLAR

Bu politikanın hazırlanmasında aşağıdaki mevzuat, standart ve kurumsal dokümanlar esas alınmıştır:

- ISO/IEC 27001:2022 — Bilgi Güvenliği Yönetim Sistemi
- ISO/IEC 27002:2022 — Bilgi Güvenliği Kontrolleri

- Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik
- Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Tebliğ
- KEPHS Birlikte Çalışabilirlik Usul ve Esasları
- KEP Rehberi düzenlemeleri
- İşlem Sertifikası Usul ve Esasları
- Elektronik Kimlik Doğrulama ve ilgili ikincil düzenlemeler
- 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili ikincil düzenlemeler
- ETSI TS 102 640 KEP hizmetleri teknik çerçevesi
- BS 10012:2017 Kişisel Bilgi Yönetim Sistemi
- ISO/IEC 27031:2025 BİT sürekliliği hazırlığı
- ARKD risk yönetimi, erişim kontrol, ağ güvenliği, kriptografik kontrol, olay yönetimi, yedekleme, iş sürekliliği, kişisel veri yönetimi ve dokümante edilmiş bilgi yönetimi prosedürleri

4. TANIMLAR

Terim / Kısaltma	Tanım
Bilgi Güvenliği	Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumaya yönelik yönetimsel, teknik ve fiziksel kontroller bütünü.
BGYS	ISO/IEC 27001:2022 esaslı Bilgi Güvenliği Yönetim Sistemi.
KEPHS	Kayıtlı Elektronik Posta Hizmet Sağlayıcısı.
KEP Delili	KEP iletisinin gönderim, teslim, kabul/red ve ilgili işlem kayıtlarının hukuki ispat değerini taşıyan elektronik delil kayıtları.
İşlem Sertifikası	KEPHS işlem ve delil süreçlerinde kullanılan, yetkili ESHS tarafından sağlanan sertifika.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
Kritik Bilgi Varlığı	KEP hizmetinin, bilgi güvenliğinin veya mevzuata uyumun sürdürülmesi için korunması zorunlu bilgi, sistem, kayıt veya altyapı bileşeni.
Olay	Bilgi güvenliği politikasına aykırılık, zafiyet, yetkisiz erişim, veri kaybı, hizmet kesintisi veya kişisel veri ihlali doğurabilecek durum.

5. SORUMLULUKLAR

Bilgi güvenliği sorumlulukları görev ayrılığı, hesap verebilirlik ve denetlenebilirlik prensipleriyle aşağıdaki şekilde tanımlanır:

Rol	Sorumluluk
Üst Yönetim / Genel Müdür	Bilgi güvenliği politikasını onaylamak, BGYS hedeflerini stratejik hedeflerle uyumlu belirlemek, gerekli kaynakları sağlamak, KEPHS mevzuat uyumunu sahiplenmek ve yönetimin gözden geçirmesi faaliyetlerini yürütmek.

EYS Yönetim Temsilcisi	Politikanın yayımlanması, güncelliğinin sağlanması, iç tetkiklerin koordine edilmesi, uygunsuzlukların ve düzeltici faaliyetlerin takibi, mevzuat ve standart uyumunun izlenmesi.
Ağ Yöneticisi	Bilgi güvenliği kontrollerinin teknik uygulanmasını desteklemek; ağ güvenliği, erişim kontrolü, loglama, yedekleme, olay müdahale ve BİT sürekliliğiyle ilişkili teknik işletim faaliyetlerini yürütmek; kritik sistem ve ağ değişikliklerinde ilgili departman üst yöneticisi onayıyla hareket etmek.
KVKK / Hukuk Sorumlusu	Kişisel veri işleme faaliyetlerinin KVKK ve BS 10012 gereklerine uygunluğunu izlemek; ihlal bildirimleri, aydınlatma, açık rıza, veri sahibi başvuruları ve saklama/imha süreçlerini koordine etmek.
Süreç Sahipleri	Sorumlu oldukları süreçlerde bilgi varlıklarını, riskleri, erişim yetkilerini, mevzuat yükümlülüklerini ve kontrol uygulamalarını yönetmek.
Tüm Çalışanlar	Bilgi güvenliği politikasına, prosedürlere, gizlilik yükümlülüklerine ve kabul edilebilir kullanım kurallarına uymak; olay, zafiyet ve uygunsuzlukları gecikmeksizin bildirmek.
Tedarikçiler ve Dış Kaynak Sağlayıcılar	Sözleşme ve gizlilik yükümlülüklerine, bilgi güvenliği şartlarına, erişim kısıtlarına ve KEPHS hizmetlerine ilişkin güvenlik gerekliliklerine uymak.

6. UYGULAMA

6.1 Genel Bilgi Güvenliği İlkeleri

ARK Dijital, bilgi güvenliğini risk temelli, süreç odaklı ve sürekli iyileştirmeye açık bir yönetim sistemi olarak uygular. Bilgi güvenliği kontrolleri; KEP mevzuatı, ISO/IEC 27001:2022 Ek A kontrolleri ve kurumsal risk iştahı dikkate alınarak belirlenir.

- Bilgi varlıkları tanımlanır, sınıflandırılır, sahipleri atanır ve riskleri periyodik olarak değerlendirilir.
- Gizlilik, bütünlük ve erişilebilirlik ilkeleri KEP hizmetleri, müşteri bilgileri, kişisel veriler, işlem kayıtları ve kurumsal bilgiler için uygulanır.
- Bilgi güvenliği hedefleri ölçülebilir şekilde belirlenir, izlenir ve yönetimin gözden geçirmesi toplantılarında değerlendirilir.
- Mevzuat, standart, sözleşme ve müşteri yükümlülükleri bilgi güvenliği yönetiminin ayrılmaz parçası olarak takip edilir.
- Politika ihlalleri, güvenlik olayları ve uygunsuzluklar kayıt altına alınır; kök neden analizi ve düzeltici faaliyetlerle yönetilir.

6.2 KEPHS Bilgi Güvenliği Taahhütleri

ARK Dijital'in KEPHS olarak yetkilendirilmesi ve faaliyet göstermesi kapsamında KEP mevzuatı ve BTK düzenlemeleri öncelikli kabul edilir. KEP hizmetleriyle ilişkili bilgi varlıkları yüksek hassasiyet seviyesinde yönetilir.

- KEP delilleri, KEP iletileri, işlem kayıtları ve loglar hukuki ispat değerini koruyacak şekilde bütünlük, erişim kontrolü, zaman bilgisi ve değiştirilemezlik prensipleriyle korunur.
- KEP delilleri ve ilgili kayıtlar mevzuatta öngörülen saklama süreleri, özellikle 20 yıllık saklama yükümlülüğü dikkate alınarak yönetilir.
- İşlem sertifikası, elektronik imza, zaman damgası, CRL/OCSP ve sertifika doğrulama süreçleri denetlenebilir kayıtlarla işletilir.
- KEP rehberi, hesap sahibi bilgileri, işlem yetkilileri ve kimlik doğrulama kayıtları yetkisiz erişime, değişikliğe, silmeye ve sızıntıya karşı korunur.
- KEP hizmetlerinin sürekliliği için yedekleme, yedek veri merkezi, felaketten kurtarma, izleme ve olay müdahale kontrolleri uygulanır ve periyodik test edilir.
- BTK, KVKK ve diğer yetkili kurum bildirimleri için olay kayıtları, etki analizleri ve delil setleri zamanında ve bütünlük içinde hazırlanır.

6.3 Risk Yönetimi

- Bilgi güvenliği riskleri varlık, tehdit, zafiyet, etki ve olasılık kriterleriyle değerlendirilir.
- KEP delilleri, işlem sertifikaları, kriptografik anahtarlar, kimlik doğrulama sistemleri, KEP arşivleri ve kişisel veri kayıtları kritik varlık olarak ele alınır.
- Risk işleme kararları; riski azaltma, aktarma, kabul etme veya kaçınma seçenekleriyle dokümante edilir.
- Seçilen kontroller ISO/IEC 27001:2022 Ek A ve KEPHS mevzuat gereklilikleriyle ilişkilendirilir.
- Yüksek ve kritik riskler üst yönetime raporlanır; risk azaltma aksiyonları takip edilir.

6.4 Erişim Kontrolü ve Kimlik Yönetimi

- Erişim yetkileri ihtiyaç kadar yetki, görev ayrılığı ve onaylı rol matrisleri esas alınarak verilir.
- Ayrıcalıklı kullanıcı hesapları kısıtlı, izlenebilir ve periyodik gözden geçirmeye tabi tutulur.
- Kimlik doğrulama mekanizmaları kritik sistemler için güçlü parola, çok faktörlü doğrulama veya eşdeğer güvenlik kontrolleriyle desteklenir.
- İşe giriş, görev değişikliği ve işten ayrılış süreçlerinde erişim hakları zamanında açılır, değiştirilir veya kapatılır.
- KEPHS sistemlerine erişimler loglanır; yetkisiz erişim denemeleri izlenir ve olay yönetimi sürecine aktarılır.

6.5 Kriptografi ve Anahtar Yönetimi

- Kriptografik kontroller, bilgi sınıflandırması, mevzuat gerekliliği ve risk değerlendirme sonucuna göre seçilir.
- İşlem sertifikası, özel anahtarlar, HSM/Ark Signer bileşenleri ve sertifika doğrulama altyapısı yetkisiz erişime karşı korunur.
- TLS/mTLS, elektronik imza, zaman damgası, sertifika zinciri doğrulama, CRL/OCSP ve uzun dönem doğrulama kontrolleri KEP hizmet gereklerine göre uygulanır.

- Anahtar üretimi, dağıtımı, kullanımı, yedeklenmesi, yenilenmesi, iptali ve imhası kontrollü ve kayıtlı şekilde yürütülür.

6.6 Kişisel Verilerin Korunması

- Kişisel veriler KVKK, BS 10012 ve ilgili mevzuata uygun şekilde hukuka uygunluk, ölçülülük, amaçla sınırlılık ve saklama süresi ilkeleriyle işlenir.
- Tasarımdan İtibaren Gizlilik (Privacy by Design) yaklaşımı yeni sistem, süreç ve entegrasyonlarda uygulanır.
- KEP hesap sahipleri, işlem yetkilileri, kimlik doğrulama kayıtları, video doğrulama kayıtları, PAdES işlem belgeleri ve KEP rehberi kayıtları yüksek hassasiyette değerlendirilir.
- Kişisel veri ihlali şüphesi halinde olay yönetimi, KVKK bildirimi ve delil koruma süreçleri birlikte işletilir.

6.7 Operasyonel Güvenlik, Loglama ve İzleme

- Sistemler güvenli yapılandırma esaslarına göre kurulur, değişiklikler kontrollü şekilde uygulanır ve kritik değişiklikler onaylanır.
- Loglar; kullanıcı, sistem, ağ, uygulama, güvenlik ve KEP işlem kayıtlarını kapsayacak şekilde üretilir, korunur ve izlenir.
- Zafiyet yönetimi, yama yönetimi, kötü amaçlı yazılımdan korunma, yedekleme ve kapasite izleme faaliyetleri düzenli olarak yürütülür.
- Bilgi güvenliği olayları sınıflandırılır, önceliklendirilir, müdahale edilir, raporlanır ve tekrarını önleyici faaliyetlerle kapatılır.

6.8 Tedarikçi ve Dış Kaynak Güvenliği

- Tedarikçiler bilgi güvenliği, gizlilik, kişisel veri koruma, süreklilik ve denetim yükümlülükleri açısından değerlendirilir.
- KEPHS hizmetlerini etkileyen dış kaynak kullanımlarında sözleşmesel güvenlik şartları, SLA, olay bildirimi, erişim kontrolü ve veri lokasyonu gereklilikleri açıkça tanımlanır.
- Tedarikçi erişimleri süreli, yetkilendirilmiş, izlenebilir ve gerektiğinde iptal edilebilir şekilde yönetilir.

6.9 Farkındalık, Eğitim ve Disiplin

- Tüm çalışanlara bilgi güvenliği, KVKK, sosyal mühendislik, olay bildirimi, güvenli kullanım ve KEPHS özel yükümlülükleri hakkında farkındalık eğitimleri verilir.
- Kritik görevlerde bulunan çalışanların teknik yeterlilikleri ve güvenlik farkındalıkları periyodik olarak geliştirilir.
- Politika ve prosedür ihlalleri, olayın niteliğine göre disiplin, sözleşme ve hukuki süreçler kapsamında değerlendirilir.

6.10 Sürekli İyileştirme

- Bilgi güvenliği performansı; hedefler, riskler, olaylar, iç tetkik sonuçları, düzeltici faaliyetler ve yönetimin gözden geçirmesi çıktılarıyla izlenir.
- Politika yılda en az bir kez veya önemli mevzuat, organizasyon, teknoloji, hizmet veya risk değişikliği olduğunda gözden geçirilir.
- İç tetkik, dış denetim, BTK incelemesi, müşteri geri bildirimi ve olay sonrası değerlendirme çıktıları iyileştirme girdisi olarak kullanılır.

7. KAYITLAR

Kayıt	Sorumlu	Saklama / Kontrol
Bilgi güvenliği risk değerlendirme kayıtları	EYS Yönetim Temsilcisi / Ağ Yöneticisi	Güncel risk yönetimi prosedürüne göre
Varlık envanteri ve sınıflandırma kayıtları	Ağ Yöneticisi / Süreç Sahipleri	Güncel ve erişim kontrollü
Erişim yetki matrisi ve erişim gözden geçirme kayıtları	Ağ Yöneticisi	Periyodik gözden geçirme kayıtlarıyla
Olay ve ihlal kayıtları	EYS Yönetim Temsilcisi / Ağ Yöneticisi	Olay yönetimi prosedürüne göre
Log kayıtları ve KEP işlem kayıtları	Ağ Yöneticisi	Mevzuat, risk ve saklama gerekliliklerine göre
Eğitim ve farkındalık kayıtları	EYS Yönetim Temsilcisi / İK	Eğitim planı ve kayıt prosedürüne göre
Yönetimin gözden geçirmesi ve iç tetkik kayıtları	EYS Yönetim Temsilcisi	EYS kayıt kontrol prosedürüne göre

8