Bilgi Güvenliği ve Kalite Politikası

TASLAK — Hukukçu onayı bekliyor. Köşeli parantezli alanlar yayından önce doldurulacaktır.

1. Taahhüt

[ŞİRKET UNVANI] (“Şirket”), İmza elektronik imza platformunda müşterilerinin belgelerini, imzalarını ve kişisel verilerini gizli, bütün ve erişilebilir tutmayı; hizmeti öngörülebilir kalitede, ölçülen ve iyileştirilen süreçlerle vermeyi taahhüt eder. Şirket şu anda **herhangi bir ISO sertifikasına sahip değildir**; bu politika, ISO/IEC 27001 ve ISO 9001'in ilkelerini yol gösterici olarak alır, ancak bir belgelendirme beyanı değildir. [KARAR: belgelendirme hedefi ve tarihi.]

2. Kapsam

Platform yazılımı (web uygulaması, imza motoru, masaüstü İmza Programı), sunucular ve yedekler, kaynak kodu deposu, tedarikçi hizmetleri (barındırma, e-posta, SMS, zaman damgası) ve bunlara erişen bütün kişiler.

3. İlkeler

1. **Gerekenden fazla veri yok:** imza PIN kodu ve özel anahtar Platforma hiç gelmez; zaman damgası hizmetine yalnız belge özeti gider; imzalı PDF hiçbir yolda yeniden üretilmez.
2. **Varsayılan güvenli:** yurt dışı hizmetler, yabancı ödeme geçitleri ve isteğe bağlı entegrasyonlar kapalı gelir; açılması ayrı karar ister.
3. **En az yetki:** her kullanıcı yalnız işi için gereken izne sahiptir; firmalar birbirinin verisini göremez.
4. **Kanıtlanabilirlik:** her önemli işlem değiştirilemez bir kayda bağlanır ve sonradan doğrulanabilir.
5. **Önce test, sonra yayın:** her değişiklik otomatik testlerden ve bağımsız incelemeden geçmeden canlıya çıkmaz.

4. Uyguladığımız teknik kontroller

Alan	Kontrol
Diskte şifreleme	Belge dosyaları, sürümler, imzalı PDF'ler ve dekontlar dosya kasasında XChaCha20-Poly1305 (libsodium, parçalı AEAD) ile şifrelenir; bozulmuş ya da değiştirilmiş dosya okunmaz, yanlış bayt döndürülmez. Anahtar yenileme desteklenir. [KARAR: canlıda KASA_YAZ=true ve göç tamamlanacak.]
Alan şifreleme	T.C. kimlik numarası, biyometrik ham veri ve KVKK başvurusundaki kişisel alanlar uygulama anahtarıyla (AES-256-CBC + HMAC) şifrelenir; T.C. kimlik numarası için arama yalnız anahtarlı özetle yapılır.
Aktarımda şifreleme	HTTPS; güvenli bağlantıda HSTS. İmza Programı yalnız kullanıcının bilgisayarında (127.0.0.1) dinler.
Erişim kontrolü	rol ve izin tabanlı yetki, firma verilerinin yalıtımı, iki adımlı doğrulama, satıcının kurulum hesaplarının canlıda engellenmesi, istemci kısıtlamaları.
Yalıtım testleri	iki firmanın birbirinin belgesine, imzasına, olayına

Alan	Kontrol
	ve API kaydına erişemediğini doğrulayan otomatik testler.
Denetim izi	belge geçmişi ve olay kayıtları özet zinciriyle bağlıdır; zincir her gün zaman damgasıyla çapalanır, haftada bir bütünlüğü denetlenir. Biyometrik veriye her erişim gerekçesiyle kaydedilir.
Tarayıcı güvenliği	X-Content-Type-Options, X-Frame-Options, Referrer-Policy, Permissions-Policy ve dar bir içerik güvenliği politikası; oturum çerezi HttpOnly ve SameSite.
Kötüye kullanım	giriş, imza, API, delil paketi ve KVKK başvurusu uçlarında istek sınırları; SMS ve e-posta kotaları; formlarda tuzak alan.
Dosya güvenliği	yüklenen dosyalarda tür ve boyut denetimi; virüs taraması [KARAR: canlıda tarayıcı kurulumu]; geçici düz dosyalar bellekte tutulan bir dizinde ve iş bitince silinir.
E-imza doğrulaması	imza AB DSS kütüphanesiyle doğrulanır; nitelikli sertifika, sertifika zinciri ve iptal durumu (OCSP/SİL) denetlenir.
Yedekleme	[KARAR: yedek sıklığı, saklama süresi, konumu, şifrelemesi ve geri yükleme denemesinin sıklığı.]
Günlük ve izleme	[KARAR: uygulama günlüğü döndürme ve hata izleme aracı.]

5. İdari kontroller

- Canlı sisteme, veriye ya da şifreleme anahtarına dokunan her iş yöneticinin açık onayıyla yapılır; veritabanını silen ya da sıfırlayan komutlar onaysız çalıştırılamaz.
- Sırlar (anahtarlar, parolalar) yalnız sunucunun ortam değişkenlerinde tutulur; kaynak koduna girmez.
- Her değişiklik otomatik test paketinden geçer; kod düzenli olarak bağımsız bir incelemeden (ayrı bir yapay zekâ modeliyle güvenlik ve doğruluk incelemesi) geçirilir ve bulgular kapatılmadan sürüm çıkmaz. [KARAR: canlıya çıkmadan önce bağımsız sızma testi.]
- Tedarikçilerle gizlilik ve veri işleme şartları yazılı olarak belirlenir [KARAR].
- Çalışanlar ve iş ortakları gizlilik taahhüdü verir ve bilgi güvenliği ile KVKK eğitimi alır [KARAR].

6. Güvenlik açığı bildirimi

Platformda bir güvenlik açığı bulduğunuzu düşünüyorsanız [E-POSTA] adresine yazın. Bildirimleri en geç [KARAR: öneri 3 iş günü] içinde yanıtlar, önem derecesine göre önceliklendirir ve düzeltme yayımlanana kadar ayrıntıyı gizli tutarız. İyi niyetle, verilere zarar vermeden ve başkalarının verisine erişmeden yapılan araştırmalar için hukuki yola başvurmayız. Kişisel verileri etkileyen bir ihlal, KVKK md. 12/5 uyarınca Kurula ve ilgili kişilere bildirilir.

7. Kalite hedefleri

- İmza sürecinin uçtan uca doğrulanabilir olması: her imzalı belge için doğrulama sayfası ve delil paketi.
- Kesintisiz hizmet: planlı bakımların önceden duyurulması; [KARAR: erişilebilirlik hedefi, ör. aylık

%99,5].
- Müşteri taleplerine zamanında yanıt: KVKK başvurularında yasal 30 günlük süre panelde geri sayımla izlenir.
- Sürekli iyileştirme: hatalar ve inceleme bulguları kayıt altına alınır, kök nedeni giderilir, gerekiyorsa test eklenir.

8. Gözden geçirme

Bu politika yılda bir kez, önemli bir güvenlik olayından sonra ve mimari değiştiğinde gözden geçirilir. Sorumlu: [KVKK SORUMLUSU] / [SİSTEM YÖNETİCİSİ]; onay: [ONAYLAYAN: Genel Müdür].

Revizyon geçmişi

Sürüm	Tarih	Açıklama
1.0	29.11.2026	İlk yayın (taslak, hukukçu onayı bekliyor)

Mevzuat atıflarının son kontrol tarihi: 29 Kasım 2026. Güncel sürüm: http://imza.test/page/bilgi-guvenligi-ve-kalite-politikasi

TASLAK