

ERIKLABS

Entegre Kalite ve Bilgi Güvenliği Politikası

ISO 9001:2015 Madde 5.2 ve ISO/IEC 27001:2022 Madde 5.2

Doküman Kodu	Revizyon	Yayın Tarihi	Gizlilik
PL-01	00	31.07.2026	Kamuya Açık

Hazırlayan	Kontrol Eden	Onaylayan
Kalite ve BGYS Sorumlusu	Yazılım Geliştirme Yöneticisi	Genel Müdür

Politikanın Amacı: ErikLabs'ın yazılım geliştirme ve müşterilere sunulan yazılım test hizmetlerini; müşteri memnuniyeti, güvenilir hizmet, bilgi güvenliği, risk yönetimi ve sürekli iyileştirme ilkeleri doğrultusunda yönetmek için ortak yön ve taahhütleri belirlemektir.

1. Politika Beyanı

ErikLabs; yazılım geliştirme, yazılım test hizmetleri, teknik bakım ve ilgili destek süreçlerinde müşterilerine güvenilir, doğrulanabilir, güvenli ve sürdürülebilir ürün ve hizmetler sunmayı amaçlar. Kalite Yönetim Sistemi ile Bilgi Güvenliği Yönetim Sistemini kuruluşun amacı, stratejik yönü, faaliyetlerinin niteliği ve riskleriyle uyumlu olarak kurar, uygular, sürdürür ve sürekli iyileştirir.

Üst yönetim bu politika aracılığıyla aşağıdaki taahhütlerde bulunur:

- Müşteri ihtiyaçlarını, sözleşme ve kabul kriterlerini doğru anlamak; uygulanabilir şartları karşılamak ve müşteri memnuniyetini sürekli geliştirmek.
- Yazılım geliştirme ve müşterilere sunulan test hizmetlerini planlı, izlenebilir, tarafsız, tekrarlanabilir ve kanıta dayalı yöntemlerle yürütmek.

- Ürün ve hizmet kalitesini; gereklilik yönetimi, güvenli tasarım, kod inceleme, test, doğrulama, geçerli kılma, kontrollü yayın ve hizmet sonrası izleme yoluyla güvence altına almak.
- Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak; yetkisiz erişim, değişiklik, ifşa, kayıp ve hizmet kesintisi risklerini uygun kontrollerle yönetmek.
- Müşteri kaynak kodu, test ortamı, test verisi, bulgu ve raporları dâhil olmak üzere emanet edilen bilgi varlıklarını sınıflandırmak ve amaçla sınırlı şekilde korumak.
- Bilgi güvenliği ve kalite risklerini sistematik biçimde değerlendirmek; kabul edilemez riskleri azaltmak ve fırsatları değerlendirmek.
- Uygulanabilir yasal, düzenleyici, sözleşmesel, müşteri ve diğer ilgili taraf gerekliliklerine uymak.
- Kalite ve bilgi güvenliği hedeflerinin belirlenmesi, izlenmesi ve gözden geçirilmesi için ölçülebilir bir çerçeve sağlamak.
- Çalışanların ve ilgili dış kaynakların yetkinliğini, farkındalığını, sorumluluk bilincini ve güvenli çalışma davranışlarını geliştirmek.
- Olay, hata, uygunsuzluk, müşteri geri bildirimi, denetim ve performans sonuçlarından öğrenmek; nedenleri ortadan kaldırmak ve tekrarları önlemek.
- Kalite Yönetim Sistemi ve Bilgi Güvenliği Yönetim Sisteminin uygunluğunu, yeterliliğini ve etkinliğini sürekli iyileştirmek.
- Bu politika ve sistemlerin uygulanması için gerekli insan, teknoloji, altyapı, zaman ve finansal kaynakları sağlamak.

2. ErikLabs Kalite İlkeleri

- Müşteri odaklılık: İhtiyaçlar, kullanım amacı, kabul kriterleri ve geri bildirimler ürün ve hizmet kararlarının girdisidir.
- Süreç yaklaşımı: Geliştirme planlama ve kapsam, teknik tasarım, kodlama, kod inceleme, test/yayına hazırlık, bakım ve teknik iyileştirme süreçleri ölçülebilir çıktılarla yönetilir.
- Kanıta dayalı karar: Test sonuçları, hata eğilimleri, KPI'lar, müşteri memnuniyeti, teslim performansı ve denetim sonuçları kararların temelidir.
- Kusuru önleme: Hataları yalnızca son kontrolde yakalamak yerine risk bazlı planlama, gözden geçirme, otomasyon ve erken testlerle önlemek esastır.
- Hizmet güvenilirliği: Müşterilere sunulan test hizmetlerinde kapsam, yöntem, ortam, sürüm, kanıt ve rapor bütünlüğü korunur; yanlış pozitif/negatif bulgular azaltılır.
- Sürekli iyileştirme: Performans hedefleri, kök neden analizleri, öğrenilen dersler, teknik borç ve iyileştirme fırsatları düzenli olarak ele alınır.

3. ErikLabs Bilgi Güvenliği İlkeleri

- En az ayrıcalık ve bilmesi gereken prensibiyle erişim sağlanır; kimlik doğrulama, yetkilendirme ve erişim kayıtları uygulanır.
- Geliştirme, test ve üretim ortamları ayrılır; üretim verisi testte varsayılan olarak kullanılmaz, gerekli durumda maskeleyme/anonimleştirme ve yetkili onayı uygulanır.
- Kaynak kod, yapılandırma, sırlar, bağımlılıklar ve yazılım paketleri güvenli geliştirme yaşam döngüsü kapsamında korunur.
- Bilgi varlıkları sınıflandırılır; saklama, aktarım, yedekleme, imha ve geri yükleme kontrolleri riskle orantılı uygulanır.
- Bilgi güvenliği olayları ve zayıflıkları gecikmeden bildirilir, kayıt altına alınır, müdahale edilir ve olaylardan öğrenilir.
- Tedarikçiler, bulut hizmetleri ve dış kaynaklar bilgi güvenliği, gizlilik, süreklilik ve hizmet şartlarına göre seçilir ve izlenir.
- İş sürekliliği ve teknik dayanıklılık için yedekleme, izleme, kapasite, olay müdahalesi ve geri dönüş kabiliyetleri sürdürülür.

4. Kalite ve Bilgi Güvenliği Hedefleri İçin Çerçeve

Hedefler; bu politikayla uyumlu, ölçülebilir, sorumlusu ve süresi belirli olacak şekilde planlanır. Hedefler oluşturulurken müşteri ve ilgili taraf beklentileri, risk ve fırsatlar, süreç performansı, yasal/sözleşmesel şartlar, teknolojik değişiklikler ve kaynaklar dikkate alınır. En az aşağıdaki alanlarda hedef ve göstergeler belirlenir:

Hedef alanı	Örnek izleme göstergeleri
Müşteri ve hizmet kalitesi	Müşteri memnuniyeti, zamanında teslim, ilk kabul oranı, test raporu ilk kabul oranı.
Yazılım kalitesi	Üretime kaçan hata, ilk test geçişi, yeniden açılan hata, kod inceleme uyumu.
Bilgi güvenliği	Olay sayısı/etkisi, zafiyet kapatma süresi, erişim gözden geçirme, farkındalık sonuçları.
Hizmet sürekliliği	Kullanılabilirlik, yedekleme başarısı, geri yükleme/rollback süresi, değişiklik başarı oranı.
Yetkinlik ve iyileştirme	Yetkinlik gelişimi, düzeltici faaliyet etkililiği, tekrar eden uygunsuzluk, iyileştirme aksiyonları.

Hedeflerin sonuçları belirlenen sıklıkta izlenir. Hedefe ulaşamadığında sapma, neden, etki, düzeltme/düzeltilici faaliyet, sorumlu ve termin kayıt altına alınır; sonuçlar yönetimin gözden geçirmesine sunulur.

5. Roller ve Sorumluluklar

Politikanın sahipliği üst yönetime aittir. Üst yönetim, politikanın kuruluşun bağlamı ve stratejik yönüyle uyumunu, sistemlere entegre edilmesini ve gerekli kaynakların sağlanmasını güvence altına alır. Tüm çalışanlar ve ErikLabs adına çalışan ilgili taraflar; bu politikaya, görevlerine ilişkin prosedürlere ve kendilerine bildirilen güvenlik/kalite şartlarına uymakla sorumludur.

- Kalite ve BGYS Sorumlusu politikanın dokümente edilmesini, yayımlanmasını, farkındalığını, performansını ve gözden geçirilmesini koordine eder.
- Süreç sahipleri politika taahhütlerini süreç hedefleri, kontroller, kayıtlar ve iyileştirme faaliyetleriyle uygular.
- Çalışanlar müşteri şartlarını korur, hataları/uygunsuzlukları ve bilgi güvenliği olaylarını bildirir, yetkisi dışındaki işlemleri gerçekleştirmez.
- Tedarikçi ve dış kaynaklar sözleşmelerde belirlenen kalite, gizlilik, güvenlik ve raporlama şartlarına uyar.

6. İletişim, Anlama ve Erişilebilirlik

Politika, belgelenmiş bilgi olarak güncel sürümde tutulur. Kuruluş içinde işe giriş/oryantasyon, periyodik farkındalık eğitimi, toplantılar, kurum içi iletişim kanalları ve doküman yönetim sistemi yoluyla duyurulur. Çalışanların politikayı anlaması eğitim katılımı, kısa değerlendirmeler, görüşmeler, iç denetimler ve uygulama gözlemleriyle doğrulanır.

Politika müşteriler, tedarikçiler, iş ortakları, kamu kurumları ve diğer ilgili tarafların erişimine uygun olduğunda internet sitesi, teklif/sözleşme eki veya kontrollü paylaşım kanalı üzerinden sunulur. Ticari sır veya güvenlik açısından hassas uygulama ayrıntıları kamuya açık politika metnine dâhil edilmez.

7. Gözden Geçirme ve Güncelleme

Politika en az yılda bir kez Yönetimin Gözden Geçirmesi kapsamında ayrıca kuruluşun amacı, stratejik yönü, kapsamı, ilgili taraf ihtiyaçları, mevzuat, teknoloji, risk profili, müşteri şartları veya önemli olaylarda değişiklik olduğunda gözden geçirilir. Gözden geçirmede politikanın uygunluğu, yeterliliği, etkinliği, anlaşılma düzeyi ve hedeflerle uyumu değerlendirilir. Değişiklikler üst yönetim tarafından onaylanır, revizyon kontrollü yayımlanır ve ilgili taraflara bildirilir.

Ek A – ISO 9001 ve ISO/IEC 27001 Madde 5.2 Uyum Matrisi

Gereklilik	Politikadaki karşılığı	Uygulama/kanıt
Kuruluşun amacı ve bağlamına uygunluk	Politika Beyanı; ErikLabs faaliyetleri ve stratejik yönü	Bağlam analizi, kapsam, YGG kaydı
Kalite hedefleri için çerçeve	Bölüm 4 – Kalite ve Bilgi Güvenliği Hedefleri için Çerçeve	Hedef planı, KPI sonuçları, aksiyonlar
Bilgi güvenliği hedefleri veya hedeflerin belirlenmesi için çerçeve	Bölüm 3 ve 4	BGYS hedefleri, risk işleme ve izleme kayıtları
Uygulanabilir şartları karşılama taahhüdü	Politika Beyanındaki müşteri, yasal, sözleşmesel ve ilgili taraf taahhüdü	Mevzuat/şart listesi, sözleşme gözden geçirme
KYS'nin sürekli iyileştirilmesi	Kalite İlkeleri ve politika taahhütleri	DÖF, KPI, iç denetim, YGG
BGYS'nin sürekli iyileştirilmesi	Bilgi Güvenliği İlkeleri ve politika taahhütleri	Risk, olay, denetim, DÖF ve YGG
Belgelenmiş bilgi olarak mevcut olma	Bölüm 6	Onaylı politika, revizyon geçmişi
Kuruluş içinde iletişim, anlaşılma ve uygulanma	Bölüm 6	Eğitim/farkındalık, görüşme, iç denetim
İlgili taraflara uygun şekilde sunulma	Bölüm 6	İnternet sitesi, teklif/sözleşme eki, kontrollü paylaşım