1. Amaç

Bu politikanın amacı; MİMSOFT ARGE ARŞİVLEME TEKNOLOJİLERİ A.Ş. bünyesinde 509 Sıra No.lu Vergi Usul Kanunu (VUK) Genel Tebliği kapsamında sunulan özel entegratörlük hizmetlerinin yüksek hizmet kalitesi, kesintisizlik ve bilgi güvenliği standartlarında yürütülmesini güvence altına almak üzere ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 20000-1:2018 BT Hizmet Yönetim Sistemi ve ISO 22301:2019 İş Sürekliliği Yönetim Sistemi gerekliliklerini bütünleştiren Üst Yönetim taahhütlerini, temel ilkeleri ve kurumsal yönelimi belirlemektir.

2. Kapsam

Bu politika; MİMSOFT ARGE ARŞİVLEME TEKNOLOJİLERİ A.Ş.'nin özel entegratörlük kapsamındaki e-Fatura, e-Arşiv Fatura, e-İrsaliye, e-Müstahsil Makbuzu (e-MM) ve e-Serbest Meslek Makbuzu (e-SMM) hizmetlerini,REST/SOAP API uç noktalarını, müşteri/bayi/yönetim web arayüzlerini, yerel imza aracını, müşteri destek operasyonlarını, Merkez Ofis çalışma alanını, İstanbul Birincil Veri Merkezi ile Ankara Felaket Kurtarma Merkezi (FKM) altyapılarını, tüm yönetsel ve operasyonel görev unvanlarını (Yönetim Kurulu Başkanı, EYS Yöneticisi, Ekip Başkanı,Ağ ve Ağ Güvenliği Uzmanı, Müşteri Destek Sorumlusu) ve hizmet yaşam döngüsüne dahil olan tüm dış tedarikçi ve iş ortağı arayüzlerini kapsar.

3. Uygulama

MİMSOFT ARGE ARŞİVLEME TEKNOLOJİLERİ A.Ş. Üst Yönetimi ve tüm çalışanları, Entegre Yönetim Sistemi (EYS) kapsamındaki faaliyetlerini aşağıdaki temel ilkeler doğrultusunda uygular:

- **Stratejik Uyum ve Kaynak Taahhüdü:** Üst Yönetim, Entegre Yönetim Sistemi'nin kuruluşun stratejik yönüyle tam uyumlu olmasını, ölçülebilir EYS hedeflerinin belirlenip izlenmesini ve sistemin kurulması, işletilmesi, sürdürülmesi ve iyileştirilmesi için ihtiyaç duyulan insan, teknoloji, altyapı ve bütçe kaynaklarının eksiksiz tahsis edilmesini taahhüt eder.

- **Bilgi Güvenliğinin Korunması (BGYS):** Müşterilere ait e-belge içeriklerinin, kişisel verilerin, veritabanlarının, kaynak kodların, erişim kimlik bilgilerinin ve TÜBİTAK Kamu SM mali mühür/zaman damgası varlıklarının gizlilik, bütünlük ve erişilebilirliği risk tabanlı yaklaşımla korunur. Yetkisiz erişimleri önlemek amacıyla en az yetki ve görevlerin ayrılığı ilkeleri, güçlü şifreleme, çok faktörlü kimlik doğrulama (MFA), güvenli yazılım geliştirme (SDLC) ve 10 yıllık değiştirilemez arşiv bütünlüğü kontrolleri kesintisiz uygulanır.

- **BT Hizmet Kalitesi ve Erişilebilirlik (HYS):** Müşterilerin, bayilerin, mali müşavirlerin ve entegratör ERP iş ortaklarının ihtiyaç ve beklentilerini karşılamak üzere hizmetler planlı şekilde tasarlanır, test edilir ve kontrollü değişiklik/sürüm yönetimiyle canlı ortama aktarılır. Tüm temel e-belge servisleri ve API uç noktaları için aylık minimum %99,5 erişilebilirlik oranı ile destek çağrılarında taahhüt edilen ilk yanıt ve çözüm sürelerine (SLA) tam uyum hedeflenir.

- **İş Sürekliliği ve Olağanüstü Durum Dayanıklılığı (İSYS):** Kritik iş süreçleri ve bağımlılıklar İş Etki Analizi (BIA) ile belirlenir; olası bir siber saldırı, donanım arızası veya veri merkezi felaketi durumunda hizmetlerin belirlenen Kurtarma Süresi Hedefi (RTO) ve Kurtarma Noktası Hedefi (RPO) dahilinde sürdürülmesi sağlanır.Birincil veri merkezindeki yedekli mimari ve ikincil lokasyondaki Ankara Felaket Kurtarma Merkezi (FKM) altyapısı düzenli yedekleme ve yıllık tatbikatlarla doğrulanır.

- **Yasal, Düzenleyici ve Sözleşmesel Uyum:** Faaliyetlerin yürütülmesinde başta VUK 509 Sıra No.lu Genel Tebliğ ve Gelir İdaresi Başkanlığı (GİB) teknik kılavuzları olmak üzere; 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK), 5651 Sayılı Kanun, Türk Ticaret Kanunu ve müşterilerle, bayilerle ve dış tedarikçilerle imzalanan sözleşme hükümlerine eksiksiz riayet edilir.

- **Sürekli İyileştirme ve Gözden Geçirme:** Entegre Yönetim Sistemi'nin uygunluğu, yeterliliği ve etkililiği; periyodik iç ve dış denetimler, sızma testleri, kapasite ve performans ölçümleri, müşteri memnuniyeti değerlendirmeleri, olay/problem kök neden analizleri ve düzeltici faaliyetler yoluyla sürekli iyileştirilir. Bu politika, Yönetim Kurulu Başkanı liderliğinde gerçekleştirilen Yönetimin Gözden Geçirmesi (YGG) toplantılarında yılda en az bir kez veya mevzuat/organizasyon değişikliklerinde gözden geçirilerek güncellenir.

- **Sorumluluk, İletişim ve Yaptırım:** Bu politikanın onaylanması ve kurumsal düzeyde sahiplenilmesi Yönetim Kurulu Başkanı'nın; uygulanmasının koordinasyonu ve izlenmesi EYS Yöneticisi'nin; teknik ve operasyonel icrası ise Ekip Başkanı, Ağ ve Ağ Güvenliği Uzmanı ve Müşteri Destek Sorumlusu'nun sorumluluğundadır. Politika tüm çalışanlara tebliğ edilir, farkındalık eğitimleriyle pekiştirilir ve dış paydaşların erişimine açık tutulur (mimsoft.com.tr). Politika hükümlerine aykırı davranışlar disiplin ve sözleşme yaptırımlarına tabidir.

Onaylayan: Yönetim Kurulu Başkanı — MİMSOFT ARGE ARŞİVLEME TEKNOLOJİLERİ A.Ş.