BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Bu politikanın amacı; Turuncu Profesyonel Bilgi Teknolojileri A.Ş.'nin faaliyetleri kapsamında e-imza724.com platformu üzerinden işlenen tüm bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumaktır.

Bilgi Güvenliği Yönetim Sistemi (BGYS), ISO/IEC 27001 standardına uygun olarak kurulmuş, sürdürülmekte ve sürekli iyileştirilmektedir.

2. Kapsam

Bu politika, Turuncu Profesyonel Bilgi Teknolojileri A.Ş.'nin tüm bilgi sistemlerini, çalışanlarını, danışmanlarını, tedarikçilerini, iş ortaklarını ve e-imza724.com üzerinden işlem yapan tüm kullanıcılarını kapsar.

Politika; elektronik, basılı veya sözlü tüm bilgi varlıklarını içerir.

3. Kapsam Dışı Durumlar

Yalnızca kamuya açık, anonim bilgi paylaşımları kapsam dışındadır. Ancak bu bilgilerin bile doğruluk ve bütünlük ilkeleri korunur.

4. Hedefler

- Bilgi güvenliği risklerini belirlemek, analiz etmek ve yönetmek
- Kullanıcı ve müşteri verilerinin gizliliğini sağlamak
- Bilgi varlıklarının yetkisiz erişim, değişiklik, kayıp veya zarar görmesini önlemek
- Yasal, düzenleyici ve sözleşmesel yükümlülüklere tam uyum sağlamak
- Sürekli iyileştirme ve farkındalık kültürünü geliştirmek

5. Temel Bilgi Güvenliği İlkeleri

5.1 Gizlilik (Confidentiality)

Bilgilere yalnızca yetkili kişilerin erişebilmesi esastır.

Tüm kullanıcı ve müşteri verileri, yasal zorunluluklar dışında üçüncü kişilerle paylaşılmaz.

5.2 Bütünlük (Integrity)

Bilgi varlıklarının doğruluğu ve bütünlüğü korunur.

Verilerdeki her değişiklik kayıt altına alınır ve yetkilendirme kontrollerine tabidir.

5.3 Erişilebilirlik (Availability)

Yetkili kullanıcılar, bilgilere ihtiyaç duyduklarında kesintisiz ve güvenli şekilde erişebilmelidir.

Sistemlerin sürekliliği için yedekleme, felaket kurtarma ve iş sürekliliği planları uygulanır.

6. Bilgi Güvenliği Yönetimi

- Tüm bilgi güvenliği faaliyetleri, Bilgi Güvenliği Yönetim Temsilcisi tarafından koordine edilir.
- BGYS'nin etkinliğini sağlamak için düzenli iç denetimler yapılır.
- Risk değerlendirme süreçleri yılda en az bir kez gerçekleştirilir.
- Bilgi güvenliği olayları kayıt altına alınır, analiz edilir ve iyileştirme süreçleri başlatılır.

7. Bilgi Güvenliği Kontrolleri

- Sistem erişimleri iki faktörlü kimlik doğrulama (2FA) ile korunur.
- Kullanıcı verileri şifreli olarak saklanır (AES-256, SSL/TLS).
- Log kayıtları düzenli olarak izlenir ve yasal süreler boyunca saklanır.
- Çalışanlara düzenli olarak BGYS farkındalık eğitimleri verilir.
- Üçüncü taraf hizmet sağlayıcılarıyla yapılan tüm sözleşmelerde bilgi güvenliği yükümlülükleri tanımlanır.
- Yedekleme planları, kurtarma testleri ve erişim kontrol prosedürleri dokümante edilmiştir.

8. Yasal ve Düzenleyici Uyum

Turuncu Profesyonel Bilgi Teknolojileri A.Ş.,

- 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK),
- 5070 Sayılı Elektronik İmza Kanunu,
- BTK ve TÜBİTAK UEKAE tarafından belirlenen güvenlik standartları,
- ve ISO/IEC 27001:2022 gerekliliklerine uygun şekilde faaliyet yürütür.

9. Olay Yönetimi ve Bildirim

Bilgi güvenliği ihlali, tehdit veya şüphesi durumunda ilgili olay derhal Bilgi Güvenliği Yönetim Temsilcisine bildirilir.

Olayın etkisi değerlendirilir, kök neden analizi yapılır ve düzeltici faaliyetler uygulanır.

Yasal gereklilik halinde ilgili kurum ve kişiler bilgilendirilir.

10. Sürekli İyileştirme

BGYS performansı düzenli olarak ölçülür, yönetim gözden geçirmelerinde değerlendirilir ve iyileştirme fırsatları belirlenir.

Politika, yılda en az bir kez veya ihtiyaç duyulduğunda revize edilir.

11. Sorumluluklar

Tüm çalışanlar bilgi güvenliği politikasına uymakla yükümlüdür.

Yöneticiler, birimlerinde güvenlik kültürünün yerleşmesini sağlamakla sorumludur.

Tedarikçiler, sözleşmelerde belirtilen güvenlik şartlarına uymayı taahhüt eder.

12. Yayın ve Yürürlük

Bu politika, Turuncu Profesyonel Bilgi Teknolojileri A.Ş. tarafından onaylanmış olup, yayımlandığı tarih itibarıyla yürürlüğe girmiştir.

Politikanın güncel sürümü www.e-imza724.com adresinde kamuya açıktır.