

BİLGİ GÜVENLİĞİ VE BİLGİ SİSTEMLERİ YÖNETİMİ POLİTİKASI

1. Amaç ve Dayanak

Bu politikanın amacı; **Tukaş Gıda Sanayi ve Ticaret A.Ş.’nin** bilgi sistemleri ve bilgi varlıklarının gizlilik, bütünlük ve yetkiler dâhilinde erişilebilirlik ilkeleri doğrultusunda korunmasını sağlamak; bilgi sistemleri yönetiminin etkin, güvenli ve sürdürülebilir bir şekilde yürütülmesini temin etmektir.

İşbu politika, Sermaye Piyasası Kurulu’nun **VII-128.10 sayılı “Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği”** başta olmak üzere, ilgili sermaye piyasası mevzuatı, yürürlükteki diğer yasal düzenlemeler çerçevesinde hazırlanmıştır.

2. Kapsam

Bu politika;

- **Tukaş Gıda Sanayi ve Ticaret A.Ş.’nin** sahip olduğu veya yönettiği tüm bilgi sistemlerini,
- Elektronik, yazılı, sözlü veya görsel tüm bilgi varlıklarını,
- Şirket çalışanlarını, yöneticilerini, danışmanlarını, tedarikçilerini ve bilgi sistemlerine erişimi bulunan üçüncü tarafları

kapsar.

3. Yönetim Kurulu’nun Rolü ve Gözetim

SPK VII-128.10 sayılı Tebliğ uyarınca; bilgi sistemleri yönetimi, **Yönetim Kurulu’nun gözetim ve sorumluluğu** altında yürütülür. Yönetim Kurulu;

- Bilgi sistemleri yönetimine ilişkin politika ve stratejilerin onaylanmasını,
- Bilgi güvenliği risklerinin etkin şekilde yönetilmesini,
- Kontrol yapısının tesis edilmesini ve etkinliğinin izlenmesini sağlar.

4. Bilgi Güvenliği Sorumlusunun Belirlenmesi

Bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hususunda üst yönetime rapor veren bir bilgi güvenliği sorumlusu belirlenir. Bilgi güvenliği sorumlusunun, bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevinin bulunmaması ve üst yönetime bağlı çalışması sağlanır.

5. Temel Bilgi Güvenliđi İlkeleri

Tukař Gıda Sanayi ve Ticaret A.ř. bilgi güvenliđi ve bilgi sistemleri yönetimini ařađıdaki temel ilkeler çerçevesinde yürütür:

- Kurumsal bilginin gizliliđini, bütünlüğünü, yetkiler dâhilinde erişilebilirliğini ve sürekliliđini sağlamak,
- Bilgi sistemlerini hedef alan iç ve dış, kasıtlı veya kasıtsız her türlü tehdide karşı koruma sağlamak,
- Bilgi sistemleriyle ilgili riskleri belirlemek, analiz etmek ve sistematik olarak yönetmek,
- Bilgi güvenliđi kontrollerini tesis etmek, test etmek ve etkinliğini izlemek,
- Yasal, düzenleyici ve sözleşmesel yükümlölüklerle uyum sağlamak,
- İş sürekliliđi ve operasyonel dayanıklılıđı desteklemek.

6. Risk Yönetimi ve Kontrol Yapısı

Bilgi sistemlerine ve bilgi varlıklarına ilişkin riskler, SPK Tebliđi'nde belirtilen esaslar doğrultusunda düzenli olarak değerlendirilir. Bu kapsamda:

- Bilgi varlıkları tanımlanır ve sınıflandırılır,
- Potansiyel tehdit ve zafiyetler analiz edilir,
- Riskleri azaltmaya yönelik önleyici ve düzeltici kontroller uygulanır.

Bilgi güvenliđi risklerinin tamamen ortadan kaldırılamayacağı kabul edilmekte olup, mevcut risklerin kabul edilebilir seviyelerde tutulması ve **artık riskin** en aza indirilmesi hedeflenir.

7. Bilgi Güvenliđi Olay Yönetimi

Bilgi sistemlerini hedef alan siber saldırılar ve bilgi güvenliđi ihlalleri, bilgi güvenliđi olay yönetimi kapsamında ele alınır. Gerçekleşen veya řüphe uyandıran olaylar derhal raporlanır, gerekli incelemeler yapılır ve kontrol yapısının güçlendirilmesine yönelik aksiyonlar alınır.

8. Eğitim, Farkındalık ve Kullanıcı Sorumlulukları

Bilgi sistemleri yönetiminin etkinliđi; kullanıcıların farkındalıđı ve sorumluluklarını yerine getirmesi ile mümkündür. Bu doğrultuda **Tukař Gıda Sanayi ve Ticaret A.ř.**, çalışanlarının bilgi güvenliđi ve bilgi sistemleri yönetimi farkındalıđını artırmak amacıyla düzenli eğitim ve bilgilendirme faaliyetleri yürütür.

9. Yürürlük, Gözden Geçirme ve Güncelleme

İřbu politika, **Tukař Gıda Sanayi ve Ticaret A.ř.**, **Yönetim Kurulu** tarafından onaylandıđı tarihte yürürlüğe girer. SPK VII-128.10 sayılı Tebliđ uyarınca; politika **en az yılda bir kez** veya mevzuat, organizasyonel yapı, iş ihtiyaçları ya da tehdit ortamındaki deđişiklikler doğrultusunda gözden geçirilir ve güncellenir.