

	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKALARI	Doküman No	TK.BS.PL.01
		İlk Yayın Tarihi	08.02.2016
		Revizyon Tarihi	11.02.2025
		Revizyon No	01
		Sayfa	1/2

Bilgi kaynakları, ofis ve cihazlar gibi Tiryaki Agro Gıda San. Ve Tic. A.Ş firması açısından büyük önem taşıyan varlıklardır. Bilgi varlıklarını ve kaynaklarını kullanan veya bilgi sağlayan herhangi bir kişi, bilgi varlıklarını korumakla yükümlüdür.

Ortak bilgi varlıklarını kullanan tüm çalışanların, gereken duyarlılığı göstermesi ve diğer meslektaşlarını, kurum çalışanlarını ve kurumsal değerleri gözeterek hareket etmesi beklenir.

Kurumsal değerlerin gereği olarak gizliliğe önem verilir, her türlü kişisel bilgi en yüksek güvenlik standartlarına sahip sistemlerle korunur. Bilginin sahibi istemedikçe, yetki verilmedikçe veya yasal gereklilikler oluşmadıkça bilgi paylaşılmaz.

Tiryaki Agro Gıda San. Ve Tic. A.Ş firması için tüm bu bilgi varlıkları ve kaynakları içerisinde en kritik olanı, özenle korunması, gizliliğinin sağlanması, ihtiyaç duyulduğu anda erişilmesi gereken bilgi varlıkları, sunucu sistemi üzerinde ve ofistedir.

Bilgi varlıkları ve kaynakları farklı konumlarda veya ortamlarda bulunabilir. Hangi konumda veya ortamda olursa olsun müşteri iletişim gereksinimleri ve kurumsal değerler bu varlıkların ve kaynakların kullanımını belirler.

Bilgi güvenliği, sadece bilginin gizliliğinin değil, bütünlüğünün ve kullanılabilirliğinin de sağlanması ile mümkündür. Bilginin gizlilik gerekliliği, sadece yetkilendirme dâhilinde gereken bilgi varlıklarına erişim verilmesi anlamına gelir. Bilginin bütünlüğü, tüm bilgi varlıklarının tamlığını ve doğruluğunu sağlamayı gerektirir.

Bilginin kullanılabilirliği, bilgi varlıklarının ihtiyaç duyulduğu anda ulaşılabilir ve kullanılabilir olması anlamına gelir.

Bilginin kullanımı, yerleşimi ve korunması ile ilgili ihtiyaçların karmaşıklığı ve çokluğu, kapsamlı ve geniş bilgi güvenliği süreçlerinin ve politikalarının tanımlanmasını zorunlu kılmaktadır. Bu nedenle belirlenen süreçler doğrultusunda bilgi güvenliği riskleri, bilgi varlığından sorumlu olan kişiler tarafından değerlendirilir, risklerin önceliği belirlenir ve gereken önlemler alınır.

Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel dernekler ile uygun iletişime geçilir. Üst yönetim ve teknik çalışanlar özellikle güvenlik alanında kurumlardan gelen bildirimler takip edilmektedir.

Sistem odası ve sunucuların güvenliğinin sağlanması öncelikli olarak ele alınır. Varlık envanterinin ve bu envanterin olası risklerinin önceden belirlenerek müşterilerin güven içinde ve kesintisiz hizmet almaları için çalışılır.

Karar ve eylemlerde, güvenilir nesnel bilgiler ile teknolojinin tüm olanaklarının kullanılmasına önem ve öncelik verilir. *Hareketler sezgilere, duygulara ya da doğru görüneneye göre değil; bilimsel ve teknolojik gerçeklerin ortaya koyduğu objektif esaslara göre düzenlenir.* Bunu sağlamak için bilgi dünyadaki en ileri kaynaklardan transfer edilir, benimsenir ve mesleki uygulamalar bu doğrultuda yapılır. Kaynaklar verimli kullanarak teknolojiye yatırım yapılır, gelişim bu doğrultuda sürdürülür.

Bu nedenle bilgi güvenliği yönetim sisteminin planlama, uygulama, izleme ve iyileştirme adımları ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına ve bu standardı destekleyen standartlara uygun olarak yürütülür.