BASF Türkiye & Azerbaycan

Bilgi Güvenliği Politikası

Bilgi Güvenliği önlemleri, ticari bilgilerin kötüye kullanılmasını, ifşa edilmesini, değiştirilmesini veya kaybolmasını önleyerek, riskleri etkin bir şekilde sınırlandırıp BASF'nin zarar görmesini önler. Bununla birlikte, bilgilerin BASF içinde ve üçüncü şahıslarla verimli bir şekilde işlenmesi, aktarılması veya depolanması için güvenli bir ortam yaratılmalı ve sürdürülmelidir. BASF'nin dijital olarak etkinleştirilen bölümlerine yönelik artan ve gelişen tehditler nedeniyle, BASF'nin performansı ve genel başarısı önemli ölçüde Bilgi Güvenliğine bağlıdır. BASF'nin Kurumsal Stratejisine dayanan dijital dönüşüm, BASF'nin tamamı için bir önceliktir ve tüm dijital çözümlerde bilgilerin kalitesini, gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamalıdır. Risk temelli bir yaklaşımda, dijitalleşmeyi yönlendirmek için en son teknolojilere, uzmanlığa ve ilhamlara güvenli bir erişim sağlanmalıdır.

ISO / IEC 27001 uluslararası standardı ile uyumlu, en son uluslararası standartları ve en iyi uygulamaları yakından takip eden bütünsel, iyi yapılandırılmış, sertifikalı ve sürekli iyileştirilmiş bir Bilgi Güvenliği Yönetim Sistemi (BGYS)'nin birincil önem konusu verilerin ve bunları depolayan, işleyen sistemlerin gizliliğini, bütünlüğünü ve erişimini sağlamaktır.

Risk temelli yaklaşımımız bağlamında, BASF bünyesindeki Bilgi Güvenliğinin hedefleri şunlardır:

- Bilgi Güvenliği için geçerli yasal ve düzenleyici gerekliliklere, yükümlülüklere ve şirket içi gerekliliklere uygunluk
- Senaryoların işlenmesi, aktarılması veya depolanmasındaki sistemlerin, bilgilerin ve verilerin bütünlüğü
- Bilgi Güvenliği için uçtan uca hesap verebilirlik sağlama, dokümante etme ve doğrulama
- Mümkün olan en yüksek risk şeffaflığı
- Dijital veya dijital olmayan her türlü bilgi için yeterli ve kapsamlı bir temel koruma
- Bilgilerin gizliliği (yetkisiz kullanımın engellenmesi)
- Altyapı, bilgi ve verilerin her zaman mevcudiyeti
- Sürekli değişen tehditlere tepki verme yeteneği
- Gelişmiş siber saldırılara karşı dayanıklılık
- Sürekli iyileştirmeyi sağlamak için doğal bir metodoloji ve yaklaşım
- Hataları ve ayrıca Bilgi Güvenliği ihlallerini tespit etmek ve değerlendirmek için proaktif bir yaklaşım