TÜRK KIZILAY	**BİLGİ GÜVENLİĞİ POLİTİKASI**	Doküman No	PLT.001
		İlk Yürürlük Tarihi	03.07.2019
		Revizyon No	01
		Revizyon Tarihi	29.03.2021
		Sahibi	Strateji ve Bilgi Teknolojileri Genel Müdür Yardımcılığı

1. GİRİŞ

Bilgi güvenliğinin konusu bir bilgi sisteminin bütünlüğüne, gizliliğine ve kullanılabilirliğine yönelik her türlü saldırı tehdidini bertaraf etmek, bu tehditlerin faydalanabileceği her türlü güvenlik açığını tespit edip kapatmaktan ibarettir. Tanım olarak basit görünmesine rağmen bilgi sistemlerinin güvenliğinin sağlanması, saldırıların çeşitlenip karmaşıklaştığı günümüzde iyice zorlaşmaktadır.

Bilgi güvenliğinin sağlanması; tüm dünyada yaşamın bir parçası haline gelen internet kullanımının yaygınlaşması, siber suç oranlarındaki artış, iş dünyası ve kişisel bilgi gizliliğini tehdit eden bilgi teknolojilerine bağlı unsurların etkisinin artması, yasal sorumlulukların artması, tehditlerin çoğalması ve daha karmaşık bir yapıya dönüşmesi nedeniyle zorunlu hale gelmiştir.

Güçlü bir bilgi güvenliği yönetim sistemi için gerekliliklerin detaylandırıldığı, uluslararası bilgi güvenliği yönetim standardı olan ISO/IEC 27001, risk tabanlı yaklaşımı ile kuruluşların bu süreçlerinde bilgi ve bilgi varlıklarının korunması için doğru insan kaynağı, kurumsal mevzuat ve bilgi teknolojileri altyapısı ile hedeflenen güvenlik düzeyini sağlamaktadır.

Türkiye Kızılay Derneği, Bilgi Güvenliği Yönetim Sistemi Standardına uygun bir yönetim sistemi kurmuş olup, bilgi güvenliğimize ve bilgi varlıklarımıza yönelik her türlü riski yönetmek için ISO/IEC 27001 standardının gereklerini yerine getirerek ve iyileştirerek işletmektedir.

2. TANIMLAR

- **Bilgi:** Kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken süreç ve varlıktır.
- **Bütünlük:** Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini, kazara veya kasıtlı olarak bilginin bozulmamasını temin etmektir.
- **Erişilebilirlik:** Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmektir.
- **Gizlilik:** Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmektir.
- **Kriptografi:** Okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerdir.

3. AMAÇ

Bu politikanın amacı; yasal mevzuatlar çerçevesinde ve ISO/IEC 27001 Bilgi Güvenliği ve Yönetim Sistemi standardına uygun olarak, Türkiye Kızılay Derneği tarafından kayıt altına alınan basılı, elektronik, fiziksel, görsel ve işitsel ortamdaki her türlü bilgi ve veriye dair güvenlik ve korunmanın sağlanmasıdır.

4. KAPSAM

Bu politika, Türkiye Kızılay Derneğinin üyelerini, yöneticilerini, çalışanlarını, gönüllülerini, bağışçılarını, yararlanıcılarını, araştırmacılarını, tedarikçilerini, etkileşimde olduğu iş ortaklarını ve

diğer tüm üçüncü kişileri kapsamaktadır. Türkiye Kızılay Derneği, bu politikaya uygun hareket eden kişi, kurum ve kuruluşlarla iş birliği yapar.

5. POLİTİKA METNİ

Bilgi varlıklarına yönelik riskleri sistematik olarak yönetmek ve kurumsal güvenilirlik ve itibarı korumak için Türkiye Kızılay Derneği;

- Kurumsal faaliyetlerini gerçekleştirirken kullandığı bilişim hizmetlerini istenilen seviyede, kesintisiz ve sürekli bir şekilde yürütür.
- Yetkisiz erişim, fidye yazılımı ve virüsler gibi ağ tehditlerine karşı gelişmiş güvenlik sistemleri kullanır.
- Kişisel ve özel verileri, kriptografik algoritma ve şifreleme yöntemleri ile güvence altına alır.
- Bilgi güvenliği yönetim sistemini ISO/IEC 27001 standardının gereklerini yerine getirecek şekilde, gizlilik, bütünlük ve erişilebilirlik ilkesine uygun olarak ilgili mevzuatlar çerçevesinde yönetir.
- Yasalara, kurum mevzuatına, teknik güvenlik standartlarına uyum için gerekli süreçleri tasarlar, sürekli ve periyodik şekilde gözden geçirir, gözetim ve denetim faaliyetleri ile uyumluluğu güvence altına alır.
- Uzaktan çalışma ve mobil cihazların güvenliğini sağlamak amacıyla destekleyici güvenlik önlemlerini uygular.
- Kurum içi ve kurum dışı transfer edilen bilginin güvenliğini sağlar.
- Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygular.
- Yasal, meşru, düzenleyici veya sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önler.
- Bilgi güvenliği farkındalığını artırmak amacıyla teknik ve davranışsal yetkinlikleri geliştirecek eğitimleri gerçekleştirir.
- Kurumsal Bilişim sistemlerinin güvenliğinde herhangi bir aksamaya mahal verilmemesi için riskleri tanımlayarak genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında bütün kurum çalışanlarının alınan güvenlik kurallarına uymasını sağlar.
- Bilgi Güvenliği Politikasına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar ve 3. taraflar için gerekli yaptırımları uygular, hukuki süreçleri başlatır.