TÜRK KIZILAY	**BİLGİ GÜVENLİĞİ VE İŞ SÜREKLİLİĞİ POLİTİKASI**	Doküman No	PLT.001
		İlk Yürürlük Tarihi	03.07.2019
		Revizyon No	03
		Revizyon Tarihi	19.07.2023
		Sahibi	Yönetişim Ofisi Başkanlığı

1. GİRİŞ

Bu politika, Bilgi Güvenliği Yönetim Sistemi ve İş Sürekliliği Yönetim Sistemi için yönetsel bir çerçeve çizme amacı ile oluşturulmuştur. 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.

İş sürekliliğinin konusu, servis ve hizmetlerin sürekliliğinin sağlanması için her türlü kesinti kaynağını değerlendirmek ve gerekli önlemleri almaktan ibarettir. İş sürekliliğinin sağlanması; kesinti tehdidini bertaraf etmek adına risk tabanlı bir yaklaşım ile hizmet ve servislerin süreklilik seviyesinin korunmasını hedeflemektedir.

Türkiye Kızılay Derneği; tüzel kişiliğe sahip, özel hukuk hükümlerine tâbi, kâr amacı gütmeyen, yardım ve hizmetleri karşılıksız olan ve kamu yararına çalışan bir gönüllü sosyal hizmet kuruluşudur. Proaktif bir kurum olarak afetlerde ve olağan dönemde ihtiyaç sahipleri ve korunmasızlara yönelik yardım sağlamak, toplumda yardımlaşmayı geliştirmek, güvenli kan teminini gerçekleştirmek ve zarar görebilirliği azaltmak için hizmet kalitesini ve süreklilik yönetimi anlayışını her zaman ön planda tutar.

Bu nedenle, Bilgi Teknolojileri Hizmet Sürekliliği Yönetimi ile iş sürekliliğini tehdit eden durumların potansiyel sonuçlarını teşhis etmeyi, iş sürekliliği kesintisi yaratabilecek bilgi teknolojileri olayları ve etkilerini önlemeyi ve kontrol dışı durumlarda; kesinti olasılığını ve kesinti süresini kısaltan, kesinti etkilerini sınırlandıran kurtarma faaliyetlerini etkin olarak yürütmeyi hedefler.

2. TANIMLAR

Bu politikada geçen;

- **BT:** Bilgi Teknolojilerini,
- **BT Hizmet Sürekliliği Yönetimi:** Kuruluşun BT ürün ve servislerinin kesinti olayı sonrasında önceden tanımlanmış kabul edilebilir seviyede sürdürebilme kapasitesini,

- **ISO-22301 Standardı:** Kuruluşların iş sürekliliğini sağlamaları için gerekli planları oluşturmaları, uygulamaları, işletmeleri, izlemeleri, incelemeleri, sürdürmeleri, korumaları ve riskleri azaltmak için hazırlanmaları, yıkıcı olaylardan kurtarmak için belgelenmiş bir yönetim sistemini geliştirmek amacıyla gereksinimlerini tanımlayan ISO standardını,
- **İş Sürekliliği Yönetimi:** Kuruluşların değer yaratan faaliyetlerini, herhangi bir felaket, kriz ve afet durumunda önceden belirlenen seviyede yürütebilme becerisini,
- **Bilgi:** Kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken süreç ve varlıklarını,
- **Bütünlük:** Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini, kazara veya kasıtlı olarak bilginin bozulmamasını temin etmeyi,
- **Erişilebilirlik:** Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmeyi,
- **Gizlilik:** Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmeyi,
- **Kriptografi:** Okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan teknikleri,

İfade eder.

3. AMAÇ

Bu politikanın amacı; yasal mevzuatlar çerçevesinde ve ilgili standartlara (ISO/IEC 27001 Bilgi Güvenliği ve Yönetim Sistemi, ISO 22301 İş Sürekliliği Yönetim Sistemi) uygun olarak, Dernek tarafından kayıt altına alınan basılı, elektronik, fiziksel, görsel ve işitsel ortamdaki her türlü bilgi ve veriye dair korunmanın sağlanması ile hizmet kesintisine sebebiyet verebilecek başlıca risklerin tespiti, değerlendirilmesi, gerekli kontrollerin uygulanması, kesintiye sebebiyet verebilecek konulara yönelik yaklaşımın ortaya konulmasıdır.

4. KAPSAM

Bu politika Türkiye Kızılay Derneğinin temel aktivitelerini destekleyen öncelikli BT süreçlerini ve bu BT süreçlerinde rol alan personelini, bilgi varlıklarını, bilgi teknolojileri ve haberleşme altyapısını, çalışma ofisleri, ürün ve servislerini kapsamaktadır.

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

5.1. Bilgi Güvenliği

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.

5.2. İş Sürekliliği

Türkiye Kızılay Derneği;

- Yasal gereksinimler, ulusal ve uluslararası standartlar ve paydaş beklentileri doğrultusunda etkili bir BT Hizmet Sürekliliği Yönetimini kurma, uygulama ve entegre bir yönetim süreci olmasını sağlamak amacıyla zaman, sermaye ve BT teknolojilerini dikkate alarak planlamalarını yapar.
- Öngörülmeyen kesintiler oluştuğunda, vermiş olduğu hizmetleri, tüm bağlayıcı unsurların (yasa, yönetmelik, müşteri sözleşmesi vb.) mecbur kıldığı süreler içerisinde kabul edilebilir seviyelerde yeniden verilebilir hale getirilebileceği bir yapıyı kurmak için gerekli yatırım, planlama ve eğitim altyapısını oluşturur.
- Bir afet, acil durum ve kriz anında, kritik iş süreçlerinin ve servislerin devamlılığı için başarılı bir kurumsal yönetişimin kritik bileşeni olarak, yasal ve uluslararası standartlar çerçevesinde etkin bir BT Hizmet Sürekliliği Yönetimi programını uygulamaya alır.

- Üyelerin, yöneticilerin, çalışanların, gönüllülerin, bağışçıların, yararlanıcıların, araştırmacıların, tedarikçilerin, etkileşimde olduğu iş ortaklarının ve diğer tüm üçüncü kişilerin Dernek lokasyonlarındaki güvenliğini sağlar ve işbu politika ve gereklilikleri konusunda bilgilendirir.

- En öncelikli hedef olarak; bir iş kesintisinin başından sonuna kadar yasal mevzuata uygun olarak iş sürekliliğini sağlar.

- Faaliyetleri çerçevesinde ilişkili otoritelerin beklentilerini karşılar.

- Uluslararası düzeyde kabul gören ISO-22301 standardı ve diğer iyi uygulamaları baz alarak, yasal ve hukuki zorunlulukları da göz önünde bulundurarak, Derneğin mevcut stratejileri doğrultusunda hizmetlerin devamlılığını sağlar ve BT Hizmet Sürekliliği Yönetim yapısını sürekli iyileştirir.

- İş kesintisi durumunda elektronik işlemlerin bütünlüğünü korur.

- Tanımlı bir zaman ölçeği dahilinde kullanıcılarına en etkin hizmet veren kanalların faaliyetini kabul edilebilir düzeylerde sürdürmek sureti ile potansiyel bir iş kesintisinin etkilerini sınırlar.

- Derneğin itibarını zedeleyebilecek ve kurumsal varlığını tehdit edebilecek riskleri yönetmek için gerekli aksiyonları alır.

- İş Sürekliliği Yönetimine ilişkin eğitim programları ve farkındalık uygulamaları ile çalışan farkındalığını arttırarak iç ve dış iletişimini sağlar.

- Potansiyel bir kesinti etkilerinin minimize edilmesi ve işlerin kabul edilebilir düzeyde devamlılığının sağlanması amacıyla önceden belirlenmiş kritik faaliyetlerin iş sürekliliği planları uyarınca sürekliliğini sağlayarak iş kesintilerinin Derneğe olan finansal, operasyonel, itibari vb. etkilerini azaltır.

- Bir kesinti sonrası normale dönüş plan ve prosedürleri oluşturarak, normal çalışma düzenine dönüşü en etkin şekilde gerçekleştirir.

- Süreçlerinde yaşanabilecek değişikliklerde iş sürekliliği dinamiklerinin göz önüne alınmasını sağlar.

- İş Sürekliliği Yönetim stratejilerinin, felaket kurtarma ve kriz yönetimi kültürünün sürekli geliştirilmesindeki ilerlemeyi düzenli olarak izler ve gözden geçirir.