BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Bu politikanın amacı; Quick Sigorta bünyesindeki bilgi varlıklarının korunmasını, güvenliğini ve sürdürülebilirliğini sağlamaktır. Kurumumuz, faaliyetlerini sürdürürken bilgi güvenliği prensiplerini benimser, çalışanlarının ve iş ortaklarının farkındalığını artırır ve yasal yükümlülüklere eksiksiz uyum sağlar.

2. Kapsam

Bu politika Quick Sigorta'nın tüm çalışanlarını, yöneticilerini, üçüncü taraf hizmet sağlayıcılarını ve diğer ilgili paydaşları kapsar. Bilgi teknolojileri altyapısı, yazılım ve donanım varlıkları, dijital ve fiziksel bilgi kaynakları, veri merkezleri, bulut hizmetleri ve tüm iş süreçleri bu politikanın kapsamındadır.

3. Temel İlkelerimiz

- **Gizlilik:** Bilgiler yalnızca yetkili kişiler tarafından erişilebilir olmalıdır.
- **Bütünlük:** Verilerin doğruluğu ve güvenilirliği korunmalıdır.
- **Erişilebilirlik:** İş süreçlerinin sürekliliği için gerekli bilgilere yetkili kişilerin zamanında ve kesintisiz erişimi sağlanmalıdır.
- **Uyumluluk:** Bilgi güvenliği uygulamaları, ulusal ve uluslararası mevzuatlar ile sektör standartlarıyla uyumlu olarak yürütülür.
- **Sürekli İyileştirme:** Risklerin etkin yönetimi ve teknolojik gelişmeler ışığında bilgi güvenliği sürekli olarak gözden geçirilir ve geliştirilir.

4. Bilgi Güvenliği Hedeflerimiz

- İş süreçlerimizin kesintisiz, güvenli ve etkin olarak yürütülmesi
- Kurumsal ve müşteri bilgilerinin korunması ve güvence altına alınması
- İç ve dış kaynaklı tehditlerin ve risklerin yönetilmesi
- Bilgi güvenliği konusunda farkındalığın ve bilinç düzeyinin yükseltilmesi
- Bilgi güvenliği sistemini, iç ve dış mevzuata uygun olarak oluşturmak, sürdürmek ve bilgi güvenliğinin hedeflerinin belirlenmesi için çerçeve sağlamak
- Bilgi güvenliği, siber güvenlik ve kişisel verilerin gizliliğini, bütünlüğünü ve sürekli erişilebilirliğini sağlamak
- Elektronik, yazılı, basılı, sözlü, görsel ve benzeri platformlarda bulunan verilerin güvenliğini sağlamak
- Bilgi güvenlik sistemini periyodik olarak gözden geçirmek, etkinliğini ve performansını sürekli iyileştirmek

5. Üst Yönetim Taahhüdü

Quick Sigorta üst yönetimi, bilgi güvenliği yönetim sisteminin etkin biçimde işlemesi ve sürekli iyileştirilmesi için gerekli kaynakları sağlar ve desteğini ifade eder. Bilgi güvenliği yönetiminin tüm çalışanlar tarafından benimsenmesi ve gerekli sorumlulukların yerine getirilmesi için liderlik eder.

6. Bilgi Güvenliği Yönetimi

- Bilgi güvenliği ile ilgili tüm süreçler üst yönetimin gözetiminde yürütülür.
- Bilgi güvenliği hedefleri belirlenir, duyurulur ve düzenli olarak ölçülür.
- Bilgi güvenliği süreçleri, şirketin stratejik hedefleri ile bütünleştirilir ve iş süreçlerine entegre edilir.

HAZIRLAYAN	KONTROL EDEN	ONAY
Bilgi Güvenliği Yönetim Sistemi Yönetim Temsilcisi	BT Genel Müdür Yardımcısı	Genel Müdür

7. Roller ve Sorumluluklar

- **Üst Yönetim:** Bilgi güvenliği stratejisinin belirlenmesi ve gerekli kaynakların sağlanması konusunda sorumludur.
- **Bilgi Güvenliği Yönetim Temsilcisi:** Bilgi güvenliği süreçlerinin koordinasyonu, kontrolü ve uygulanmasından sorumludur.
- **İş Birimi Yöneticileri:** Kendi faaliyet alanlarındaki bilgi güvenliği uygulamalarından, risklerin yönetilmesinden ve çalışanların farkındalığından sorumludur.
- **Tüm Çalışanlar:** Görevleri kapsamındaki bilgi güvenliği ilkelerine uyar ve uygunsuzlukları bildirir.
- **Dış Hizmet Sağlayıcıları:** Sözleşmelerde belirtilen bilgi güvenliği yükümlülüklerine uygun hareket eder ve kontroller ile takip edilir.

8. Bilgi Güvenliği Yönetim Uygulamaları

- **Varlık Yönetimi:** Bilgi varlıklarının tamamı kayıt altına alınır ve kritikliği doğrultusunda korunur. Kullanım dışı kalan varlıklar güvenli şekilde imha edilir.
- **Erişim Kontrolü:** Erişim yetkileri, yalnızca görev ihtiyaçları doğrultusunda verilir, düzenli olarak gözden geçirilir ve denetlenir.
- **Risk Yönetimi:** Tüm bilgi varlıkları periyodik olarak risk değerlendirmesine tabi tutulur. Risklerin yönetilmesi için gerekli önlemler alınır.
- **Ağ ve Sistem Güvenliği:** Kurumsal ağın ve sistemlerin güvenliği sürekli olarak izlenir ve güncel tehditlere karşı korunur.
- **Fiziksel Güvenlik:** Kritik bilgi işlem alanları yetkisiz erişime, doğal afetlere ve çevresel tehditlere karşı korunur.
- **Bilgi Güvenliği Olayları:** Olaylara karşı hızlı müdahale edebilmek için süreçler tanımlanmıştır. Yaşanan olaylardan ders çıkarılır ve tekrarlanmaması için önlemler alınır.
- **Yedekleme ve İş Sürekliliği:** Bilgiler düzenli olarak yedeklenir ve acil durumlar için iş sürekliliği planları hazırlanır, periyodik olarak test edilir.
- **Üçüncü Taraf Yönetimi:** Dış hizmet sağlayıcılarla yapılan sözleşmeler bilgi güvenliği kriterleri gözetilerek hazırlanır ve uyumu düzenli olarak izlenir.
- **Olay Yönetimi:** Bilgi güvenliği ihlal olaylarına etkin ve zamanında müdahale edilir, bu olaylardan ders çıkarılarak süreçler iyileştirilir.

9. Farkındalık ve Eğitim

- Quick Sigorta çalışanları, düzenli olarak bilgi güvenliği farkındalık eğitimlerine tabi tutulur.
- İş ortakları ve dış kaynak sağlayıcılar için gerekli bilgilendirme ve eğitim faaliyetleri yürütülür.
- Eğitimlerin etkinliği periyodik olarak değerlendirilir ve sonuçları yönetime raporlanır.

10. İhlal ve Olay Yönetimi

- Herhangi bir bilgi güvenliği ihlali durumunda hızlı müdahale edilir ve olay kayıt altına alınır.
- Meydana gelen olaylar değerlendirilir, sebepleri analiz edilir ve benzer durumların önlenmesi için gerekli iyileştirici tedbirler alınır

11. İzleme ve Denetim

- Bilgi güvenliği politikalarına uyum düzenli iç denetimlerle kontrol edilir.
- Dış denetimler düzenli aralıklarla gerçekleştirilir ve bulgular raporlanarak üst yönetimle paylaşılır.
- Gerekli iyileştirme faaliyetleri planlanır, uygulanır ve sonuçları takip edilir.

HAZIRLAYAN	KONTROL EDEN	ONAY
Bilgi Güvenliği Yönetim Sistemi Yönetim Temsilcisi	BT Genel Müdür Yardımcısı	Genel Müdür