Zurich Sigorta

Bilgi Güvenliği Politikası

Amaç 2

Kapsam 2

Taahhütler 2

Roller ve Sorumluluklar 4

Yürürlük ve Gözden Geçirme 4

Amaç

Zurich Sigorta Bilgi Güvenliği Politikası, Zurich Grup bilgilerini, bilgi işleme olanaklarını ve bilgi işleme olanaklarını destekleyen varlıkların tasarlanması ve işletilmesi sırasında uyulması gereken bilgi güvenliği kurallarını belirleyerek Zurich bilgilerinin gizlilik, bütünlük ve erişilebilirliğini sağlamayı amaçlar.

Kapsam

Bilgi Güvenliği Yönetim Sistemi (BGYS) çerçevesinde, bilgi güvenliği politikaları ve bunları destekleyici tüm düzenlemeler, Zurich personeli (sözleşmeli veya geçici), Kurum tarafından işe alınmış tüm çalışanları, tedarikçileri ve bu tedarikçilerin ilgili personelini ve Zurich ağına ve/veya verilerine doğrudan veya dolaylı etkisi olabilecek üçüncü şahısları ve bunlara bağlı diğer kişiler için geçerlidir.

Kurum, önceden ihbara gerek olmadan, zaman zaman, takdiri tamamen kendisine ait olmak üzere bu politikanın herhangi bir kısmını değiştirme, üzerinde değişiklik yapma veya durdurma hakkını saklı tutar.

Zurich Bilgi Güvenliği Yönetim Sistemi aşağıdaki varlık kategorilerini kapsamaktadır:

• Zurich bünyesinde üretilen, işlenen ve iletilen tüm veri dosyaları, sözleşmeler vb. den oluşan bilgi varlıkları,

• Zurich bünyesinde geliştirilen veya tedarik edilen uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları,

• Zurich bünyesinde barındırılan ve/veya işletilen yönlendirici cihazları, güvenlik cihazları, sistem yönetim sunucuları, yasal yükümlülükler kapsamında kurulmuş sunucu sistemleri, bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıklar,

• Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,

• Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıkları,

• Zurich bünyesinde bir probleme çözüm bulma ya da beliren bir fırsatı değerlendirmeye yönelik projeler,

• Bilgi Güvenliği dokümanları ve kayıtları,

Taahhütler

Zurich Sigorta (Kurum), amaçları, değerleri, misyon ve vizyonuna uygun olarak bilgi güvenliğine gereken önemi atfeder ve aşağıda belirtilen prensipler çerçevesinde bilgi güvenliğini yönetir:

1. Bilgi varlıklarımız ve sistemlerimizden tümüyle sorumluyuz
2. Tüm kanun ve yasal düzenlemelere uyumlu çalışacağız
3. Çıkar çatışmalarını önlemek için sorumlulukları kesin sınırlarla ayrıştıracağız
4. Veri ve bilgiye erişimi, "iş için kesin bilme gerekliliği" temeline göre kontrol edeceğiz
5. İş süreçlerimiz ve aktivitelerimizde, müşterilerimizin ve Kurum personelinin gizlilik ve kişisel özel hayatlarına (privacy) saygı göstereceğiz
6. Güvenlik uygulamalarımız işimize değer katacaktır
7. Güvenliğin değişen iş gereksinimlerini karşılayacak şekilde sürekli gelişmesini sağlayacağız
8. Güvenlik uygulamalarımız dünyada kabul görmüş güvenlik standartlarına ve bankacılık endüstri güvenlik uygulamalarına uyumlu olacaktır

Kurum, bilgi güvenliği politikası ile ilgili olarak aşağıdaki konuları garanti altına almak üzere gerekli kaynakları ayıracağını taahhüt eder:

1. Politika, standartlar, prosedürler ve diğer bağlantılı düzenlemeler bu politikayı destekleyecek şekilde oluşturulacaktır.
2. Tüm operasyonların bilinen ve kabul edilebilir risk seviyeleri ile gerçekleştirildiği bir bilgi teknolojisi ortamı kurulacak ve sürdürülecektir.
3. Tüm bilgi varlıklarımız gizlilik, hassaslık ve kritiklik derecesine uygun güvenlik kontrolleri ve işletim süreçleri ile dahili ve harici, kasıtlı yada kasıtsız tüm tehditlerden korunacak ve yönetilecektir. Bu çerçevede Zurich Grubu Bilgi Güvenlik Politikaları ve destekleyici dokümanlarına paralel olarak şirket sunucu, bilgisayar ve diğer cihazlara yönelik ilgili cihazların teknik özelliklerine uygun olarak antivirus, firewall, DLP ve diğer güvenlik önlemleri uygulanacak ve düzenli taramaların yapılması sağlanacaktır.
4. Bilgi güvenliği riskleri kurumun risk yönetimi metodolojisine uygun bir şekilde tespit edilir, değerlendirilir ve işlenir. Bu bağlamda bilgi güvenlik riskleri ve öncelikleri tanımlanacak; uygun, etkin ve uygulanabilir tedbirler ivedilikle alınacaktır. Bu çerçevede uyum ve risk yönetimi ile çalışılarak bilgi güvenliğinin hedeflediği çıktılara ulaşabilmek, risk iştahı dışındaki etkilerin kabul edilebilir seviyelere çekilmesi ve sürekli iyileştirmeye yönelik önlemler alınacaktır.
5. Değerli ve hassas bilgiler yetkisiz kişilerin erişiminden veya kesintilerden korunarak gizlilik sağlanacaktır.
6. Bilgi Teknolojileri grubunda hata veya normal dışı işlem risklerini azaltmak, sorunları tanımlayabilmek ve önlem alabilmek üzere görev ayrılığı prensibi uygulanır. Bu kapsamda yapılan işlerin herhangi birinin tüm aşamalarının bir personel tarafından tek başına yürütülmemesi esastır. Bu çerçevede:
    i. Görev ayrımı yapılmasının zor veya mümkün olmadığı durumlarda, faaliyetlerin bir üst yönetim kademesince izlenmesi ve kayıtların denetimi kontrolleri uygulanır
    ii. Yüksek riskli ve yüksek etkili işlemlerin başlatılması süreci ile sonuçlandırma onayları farklı kişilere görev ve sorumluluk atanır
    iii. İşler en az iki kişinin sorumluluğunda tamamlanmalı ve gerekiyorsa ilave kontroller uygulanır
    iv. Çalışanlar sadece görev tanımlarında belirtilen işleri yerine getirir. Bunun dışında yapılan işlerin görev ayrılığı prensibini ihlal etmemesi konusunda gerekli ek kontroller uygulanır
    v. Sistem geliştirme, yazılım, sistem yönetimi, veritabanı yönetimi, test, operasyon, güvenlik gibi fonksiyonlar birbirinden ayrı olarak tanımlanır
    vi. Hiç bir çalışan, açıkça yetki verilmeden tek başına bilgi varlıklarına erişemez, değiştiremez veya kullanamaz
    vii. Güvenlik denetimleri bağımsız olarak gerçekleştirilir
7. Şifreleme (Kriptografi), Zurich Grubu Risk Politikası yasal ve düzenleyici gereklilikler, ayrıca veri sınıflandırmasına uygun olarak verinin bütünlüğünü ve kritik veri transferlerinde inkar edilemezlik ve veri bütünlüğü kontrolünü sağlamak için kullanılabilecektir. Bu konuda gerekli görülen hususlarda düzenlemeler yapılacaktır.
8. Bilginin doğruluğu ve bütünlüğü, yetkisiz veya hatalı değiştirmelerden korunarak sağlanacaktır.
9. Bilgi ve bilgi sistemlerinin kullanılabilirliği iş gereksinimlerini karşılayacaktır.
10. Kullanım kolaylığı ve güvenlik arasında uygun bir denge kurulacaktır.
11. İş sürekliliği planları üretilecek, güncel tutulacak ve test edilecektir.
12. Bilgi güvenliği eğitimi tüm personel için sağlanacaktır.
13. Tüm gerçekleşmiş veya şüphelenilen güvenlik uyumsuzlukları en kısa zamanda Bilgi Güvenliği Yönetimine raporlanacaktır.
14. Belirgin güvenlik denetim konularının çözülmesi için Denetim, IK, Hukuk gibi uzman ekiplerle işbirliği yapılacaktır.
15. Bilgi güvenliği politikası ile uyum ve güvenlik uygulamaları düzenli olarak izlenecektir.
16. Kurum'un tüm üyeleri hareketlerinin ve çalışmalarının bilgi güvenliğini etkilediği noktalarda sorumlu olacaklardır.

Roller ve Sorumluluklar

- **Genel Müdür veya Genel Müdür Baş Yardımcısı**, Zurich Sigorta Bilgi Güvenliği Politikası ve bu politikada yapılan güncellemeleri onaylar,
- **Risk Komitesi**, mevcut bilgi güvenliği ve ilişkili riskleri sorgular ve uygun gördüğü konularda risk değerlendirmesini günceller, risk profili, kontroller ve güvenlik seviyesine bağlı olarak Genel Müdür / Genel Müdür Baş Yardımcısı'na gerekli güncellemeler ve eylemler konusunda tavsiyede bulunur.
- **Genel Müdür Baş Yardımcısı veya Bilgi Teknolojileri Genel Müdür Yardımcısı,** Zurich Sigorta Bilgi Güvenliği Politikası'na bağlı diğer politika, prosedür ve diğer düzenlemeleri onaylar
- **Bilgi Teknolojileri Genel Müdür Yardımcısı,** bilgi güvenliği altyapısının işletilmesi, desteklenmesinden ve muhafaza edilmesinden sorumludur. Bu çerçevede kendisine bağlı personelin sevk ve idaresini sağlar
- **Risk Yönetimi, İç Kontrol, Hukuk ve Uyum**, bu politika ve ilişkili diğer düzenlemlerin yerel mevzuat, Zurich Grup düzenlemeleri ve mevcut risklere bağlı olarak yapılması gereken değişiklikler konusunda Risk Komitesi'ne tavsiyede bulunur
- **Bilgi Güvenliği Yönetim Temsilcisi,** BGYS'nin oluşturulması, güncellenmesi, mevcut sistem çerçevesinde gerekli önlemlerin alınmasına yönelik olarak Bilgi Teknolojileri Genel Müdür Yardımcısı'na tavsiyede bulunur

- **Zurich personeli, Zurich bilgi varlıklarına erişmi olan üçüncü şahıslar ve bu şahıslara bağlı çalışanlar,** Zurich Sigorta BGYS düzenlemelerine uygun hareket etmekle yükümlüdür. Bilgi Güvenliği politika, prosedür, talimat ve diğer düzenlemelere uymamak uyarı, kınama, iş akdinin feshi vb. disiplin cezalarına neden olabilir.

Yürürlük ve Gözden Geçirme

Politika, en az yılda bir kez gözden geçirilir ve politikadaki değişiklikler "revizyon" şeklinde ilgili departmanlarca eş güdümlü olarak hazırlanır ve onaylandıktan sonra yayınlanır. Yayın tarihinde yürürlüğe girer