Bilgi Güvenliği Politikası

Standard Risk Yönetimi ve Danışmanlık A.Ş. (“**Standard Risk**” veya “**Şirket**”), faaliyetleri kapsamında elde ettiği bilgi varlıklarının, kişisel verilerin, müşteri bilgilerinin, çağrı kayıtlarının, ticari verilerin ve şirket içi bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı temel kurumsal sorumluluklarından biri olarak kabul etmektedir.

Şirketimiz; çağrı merkezi hizmetleri, alacak yönetimi, müşteri iletişimi, veri işleme ve danışmanlık faaliyetleri kapsamında işlenen tüm bilgilerin korunması amacıyla uygun teknik, idari ve organizasyonel tedbirleri uygulamayı taahhüt eder.

1. Amaç

Bu politikanın amacı, Standard Risk’in sahip olduğu veya işlediği bilgi varlıklarının korunmasına ilişkin temel ilke ve yaklaşımları belirlemek; bilgi güvenliği risklerinin azaltılmasını, iş süreçlerinin güvenli şekilde yürütülmesini ve ilgili mevzuata uyumun desteklenmesini sağlamaktır.

2. Kapsam

Bu politika aşağıdaki unsurları kapsar:

- şirket çalışanları
- yöneticiler
- çağrı merkezi personeli
- danışmanlar
- tedarikçiler
- iş ortakları
- dış hizmet sağlayıcılar
- şirket adına bilgiye erişen veya bilgi işleyen tüm üçüncü taraflar

Bu politika ayrıca aşağıdaki bilgi varlıkları bakımından uygulanır:

- kişisel veriler
- müşteri ve iş ortağı bilgileri
- çağrı kayıtları
- sözleşmeler ve hukuki belgeler
- finansal ve operasyonel kayıtlar
- elektronik posta içerikleri
- bilgi sistemleri ve yazılımlar
- fiziksel ve dijital arşivler
- şirket içi raporlar, dokümanlar ve ticari sır niteliğindeki bilgiler

3. Temel İlkeler

Standard Risk'in bilgi güvenliği yaklaşımı aşağıdaki temel ilkeler üzerine kuruludur:

3.1 Gizlilik

Bilgilere yalnızca yetkili kişiler, görev ve yetki sınırları dahilinde erişebilir.

3.2 Bütünlük

Bilgilerin doğruluğu, tamlığı ve güvenilirliği korunur; yetkisiz değişikliklerin önlenmesi hedeflenir.

3.3 Erişilebilirlik

Bilgilerin, yetkili kullanıcılar tarafından ihtiyaç duyulduğunda erişilebilir olması sağlanır.

3.4 Yetkilendirme

Bilgiye erişim, görev tanımı ve iş ihtiyacı esasına göre sınırlandırılır.

3.5 İzlenebilirlik

Bilgi sistemleri ve kritik işlemler, mümkün olduğu ölçüde kayıt altına alınır ve izlenebilir şekilde yönetilir.

3.6 Mevzuata Uyum

Bilgi güvenliği süreçleri, yürürlükteki mevzuat, sözleşmesel yükümlülükler ve şirket içi politika ve prosedürler ile uyumlu şekilde yürütülür.

4. Korunan Bilgi Varlıkları

Şirketimiz tarafından korunan bilgi varlıkları arasında özellikle aşağıdakiler yer alır:

- kişisel veriler
- müşteri ve borçlu bilgileri
- çağrı kayıtları ve görüşme içerikleri
- ödeme ve operasyon verileri
- şirket içi raporlar ve analizler
- ticari teklifler, sözleşmeler ve yazışmalar
- kullanıcı hesapları, şifreler ve erişim bilgileri
- yedekleme verileri
- sistem altyapısı ve yazılım bileşenleri

5. Bilgiye Erişim ve Yetki Yönetimi

Bilgiye erişim, yalnızca işin gerektirdiği ölçüde ve yetki çerçevesinde sağlanır.

Bu kapsamda:

- erişim yetkileri rol ve görev esaslı belirlenir
- gereksiz veya aşırı yetkilendirmeden kaçınılır
- görev değişikliği veya iş ilişkisinin sona ermesi halinde yetkiler gözden geçirilir
- kullanıcı hesapları ve erişim hakları düzenli olarak kontrol edilir
- ortak kullanıcı kullanımı mümkün olduğunca sınırlandırılır

6. Kişisel Verilerin ve Hassas Bilgilerin Korunması

Standard Risk, kişisel verilerin ve hassas nitelikteki ticari bilgilerin korunmasına özel önem verir.

Bu kapsamda şirketimiz:

- verileri hukuka ve dürüstlük kurallarına uygun işler
- belirli, açık ve meşru amaçlarla hareket eder
- verileri amaçla bağlantılı, sınırlı ve ölçülü şekilde işler
- gerekli teknik ve idari güvenlik tedbirlerini uygular
- veri paylaşımını yetki ve ihtiyaç çerçevesinde sınırlandırır
- veri saklama ve imha süreçlerini belirlenmiş kurallara uygun yürütür

7. Teknik ve İdari Güvenlik Tedbirleri

Şirketimiz, bilgi güvenliğinin sağlanması amacıyla iş modeline ve risk seviyesine uygun teknik ve idari tedbirler uygular.

Bu tedbirler arasında, ihtiyaca göre aşağıdaki uygulamalar yer alabilir:

- erişim kontrol mekanizmaları
- parola ve kimlik doğrulama kuralları
- yetkilendirme ve kullanıcı yönetimi
- veri yedekleme süreçleri
- ağ ve sistem güvenliği önlemleri
- zararlı yazılım ve yetkisiz erişime karşı koruma
- cihaz ve uç nokta güvenliği
- fiziksel evrak ve arşiv güvenliği
- çalışan farkındalığı ve iç bilgilendirme uygulamaları

8. Çağrı Merkezi ve Operasyonel Süreçlerde Bilgi Güvenliği

Standard Risk'in faaliyet yapısı gereği çağrı merkezi, müşteri iletişimi ve alacak yönetimi süreçlerinde bilgi güvenliği kritik öneme sahiptir.

Bu kapsamda:

- çağrı kayıtları yetkisiz erişime karşı korunur
- müşteri ve borçlu bilgileri yalnızca yetkili personel tarafından görüntülenir
- görüşme sırasında paylaşılan bilgiler gizlilik kuralları çerçevesinde ele alınır
- operasyonel verilerin yetkisiz üçüncü kişilerle paylaşılmasına izin verilmez
- kayıt, raporlama ve doğrulama süreçlerinde güvenlik ve doğruluk gözetilir

9. Tedarikçi ve Üçüncü Taraf Güvenliği

Şirketimiz, bilgiye erişen veya şirket adına veri işleyen tedarikçi, danışman ve diğer üçüncü tarafların da bilgi güvenliği yükümlülüklerine uygun hareket etmesini bekler.

Bu kapsamda, gerekli görülen durumlarda:

- gizlilik yükümlülükleri sözleşmesel olarak düzenlenir
- veri işleme ve erişim sınırları belirlenir
- hizmet sağlayıcıların güvenlik yaklaşımı değerlendirilir
- gerekli hallerde düzeltici tedbirler talep edilir

10. Bilgi Güvenliği İhlalleri ve Olay Yönetimi

Bilgi güvenliğini etkileyebilecek her türlü olay, zafiyet veya ihlal şüphesi gecikmeksizin ilgili yetkililere bildirilmelidir.

Bu kapsamda:

- bilgi sızıntısı
- yetkisiz erişim
- hesap ele geçirilmesi
- veri kaybı
- zararlı yazılım bulaşması
- sistem kesintileri
- yanlış kişiye veri gönderimi

gibi olaylar bilgi güvenliği olayı olarak değerlendirilebilir.

Şirketimiz, bu tür olayların tespiti, değerlendirilmesi, sınırlandırılması ve gerekli aksiyonların alınması için uygun süreçleri işletir.

11. İş Sürekliliği ve Yedekleme

Bilgi güvenliği yaklaşımımız, iş sürekliliği ile birlikte ele alınır.

Bu çerçevede şirketimiz:

- kritik bilgi ve sistemleri belirlemeyi
- uygun yedekleme mekanizmaları kurmayı
- veri kaybı ve sistem kesintisi risklerini azaltmayı
- gerekli durumlarda geri dönüş ve toparlanma adımlarını uygulamayı

hedefler.

12. Çalışanların Sorumluluğu

Tüm çalışanlar, görevleri kapsamında eriştikleri bilgi varlıklarını korumakla yükümlüdür.

Çalışanlardan beklenen temel yükümlülükler şunlardır:

- bilgi güvenliği kurallarına uygun hareket etmek
- şifre ve erişim bilgilerini korumak
- yetkisiz paylaşım yapmamak
- şüpheli durumları bildirmek
- şirket cihazlarını ve sistemlerini güvenli kullanmak
- gizlilik yükümlülüklerine uymak

13. Eğitim, Farkındalık ve Gözden Geçirme

Standard Risk, bilgi güvenliği kültürünün yalnızca teknik önlemlerle değil, çalışan farkındalığı ile de güçlendirileceğine inanır.

Bu nedenle şirketimiz, gerekli gördüğü ölçüde:

- bilgilendirme çalışmaları
- iç duyurular
- farkındalık faaliyetleri
- politika ve süreç güncellemeleri

yürütür.

Bu politika, değişen iş koşulları, teknolojik gelişmeler, operasyonel ihtiyaçlar ve mevzuat dikkate alınarak düzenli olarak gözden geçirilir ve gerektiğinde güncellenir.

14. İletişim

Bu politika hakkında sorularınız veya bilgi güvenliğine ilişkin bildirimleriniz için bizimle iletişime geçebilirsiniz:

Standard Risk Yönetimi ve Danışmanlık A.Ş.
E-posta: uyum@standardrisk.com.tr