Doğan Şirketler Grubu Holding A.Ş.
Bilgi Güvenliği Politikası

Doğan Şirketler Grubu Holding A.Ş. (Şirket) *"Bilgi Güvenliği Politikası"*; bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin olarak; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik genel usul ve esasları düzenlemektedir.

Şirket *"Bilgi Güvenliği Politikası"*; bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin, sorumlulukların belirlenmesini ve görev tanımlarının yapılmasını, hedeflerin belirlenmesini, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini, değerlendirilmesini ve gözetimini kapsamaktadır.

A) Bilgi Sistemlerine İlişkin Temel Rol ve Sorumluluklar ile Görev Tanımları

1. Yönetim Kurulu

Şirket Yönetim Kurulu; Üst Yönetim tarafından hazırlanan *"Bilgi Güvenliği Politikası"*nı; bilgi sistemlerine yönelik genel usul ve esaslar ile hedefler doğrultusunda değerlendirerek nihai onayını yapar.

"Bilgi Güvenliği Politikası" kapsamında; bilgi sistemleri kontrollerinin; etkin, yeterli ve uyumlu bir şekilde tesis edilmesi, değerlendirilmesi ve üst gözetimi Şirket Yönetim Kurulu'nun sorumluluğundadır.

2. Üst Yönetim

Şirket Üst Yönetimi; *"Bilgi Güvenliği Politikası"* ve bilgi sistemleri stratejisi uygulamalarının üst gözetimini yapar.

Bilgi güvenliğine yönelik hedeflerin belirlenmesi, *"görevler ayrılığı ilkesi"* çerçevesinde gerekli görevlendirmelerin yapılması, bilgi sistemlerinin etkin ve uyumlu yönetimine ilişkin gerekli kaynak tahsislerinin yapılması ve görev alanı kapsamındaki politika, prosedür, süreç veya projelerin nihai onayının yapılması Şirket Üst Yönetimi'nin sorumluluğundadır.

3. Bilgi Sistemleri Birimi

Şirket Bilgi Sistemleri Birimi; *"Bilgi Güvenliği Politikası"* ve bilgi sistemleri stratejisinin uygulanmasını yönetir.

Şirket Bilgi Sistemleri Birimi;

- Bilgi sistemleri yönetimine ilişkin süreç ve kontrollerin tesis edilmesi ve geliştirilmesi,
- Bilgi sistemlerinden kaynaklanan güvenlik risklerinin değerlendirilmesi,
- Bilgi güvenliği önlemlerinin uygun düzeye getirilmesine yönelik gerekli mekanizmaların kurulması ve
- Bilgi güvenliği süreçlerinin ISO/IEC 27001 standardına uyumunun sağlanması amaçlarıyla gerekli çalışmaları yapar.

4. Çalışanlar ve Diğer Paydaşlar

Şirket'in tüm çalışanları ile Şirket'in bilgi ve iş sistemlerini kullanan tedarikçiler, müşteriler, iş ortakları, hizmet sağlayıcıları ve danışmanlar gibi diğer tüm paydaşlar; Şirket'in *"Bilgi Güvenliği Politikası"* ve bilgi sistemleri stratejisine uyarlar; bilgi güvenliği gereksinimleri, riskler ve güncel tehditler konusunda bilgi düzeyini artırmaya yönelik eğitimlere katılırlar ve bilgi güvenliğine ilişkin şüpheli durumları bildirirler.

B) Bilgi Sistemlerine Yönelik Hedefler

Bilgi sistemleri, kurumsal yönetim uygulamalarının ve yönetim yapısının önemli bir parçası olarak ele alınmakta olup **ilke olarak**;

- Şirket operasyonlarının istikrarlı, rekabetçi, gelişen ve güvenli bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejilerin, iş hedefleri ile uyumunun sağlanması,
- Bilgi sistemlerinin; güvenlik, performans, etkinlik, doğruluk ve sürekliliğinin sağlanması suretiyle doğru yönetimi,
- Bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanması,
- Mevzuata, standartlara ve sözleşmelere uyumun en üst düzeye çıkarılması,
- En etkin ve güncel bilgi güvenliği kontrollerinin uygulanarak bilgi güvenliği ihlallerinin ve tehditlerinin en aza indirilmesi,
- Çalışanlar ve paydaşların; bilgi sistemlerine yönelik bilinç, farkındalık ve uyum düzeyinin en üst düzeye çıkarılması

hedeflenmektedir.

C) Bilgi Sistemlerine İlişkin Risklerin Yönetilmesine Dair Süreçler ve Kontroller

Şirket *"Bilgi Güvenliği Politikası"*; bilgi sistemleri yönetimine ilişkin genel usul ve esasları düzenlemekte olup bilgi sistemlerine ilişkin risklerin yönetilmesine dair detaylı süreçler ve kontroller ilgili prosedürlerde düzenlenmektedir.

Mevzuat değişikliklerine bağlı olarak yasal şartlara uyumun sağlanması, yeni gelişen risk ve tehditlere hazırlıklı olunması, iş modelleri ve organizasyon yapısındaki değişikliklerin süreç ve kontrollere yansıtılması gibi amaçlarla Şirket *"Bilgi Güvenliği Politikası"* ve bu Politika'ya bağlı prosedürler periyodik olarak gözden geçirilir ve ihtiyaç halinde gerekli güncellemeler yapılır.