Durak Fındık

Bilgi Güvenliği Risk Değerlendirme Politikası

Durak Fındık olarak; tüm bilgi varlıklarımızın gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı, dijital ve fiziksel bilgi akışlarımızı güvenli şekilde yönetmeyi ve iş sürekliliğimizi kesintisiz sürdürebilmeyi temel sorumluluklarımız arasında görmekteyiz. Bilgi güvenliği; yalnızca teknik bir gereklilik değil, aynı zamanda şirketimizin itibarı, sürdürülebilirliği, yasal uyumu ve paydaşlarımıza karşı güvenilirliğimizin ayrılmaz bir parçasıdır.

Bu doğrultuda; bilgi güvenliği risklerinin tanımlanması, analiz edilmesi, önceliklendirilmesi, gerekli önlemlerin alınması ve tüm bu süreçlerin şeffaf bir şekilde yönetilmesi, Durak Fındık'ın sürdürülebilir büyüme ve kurumsal yönetim anlayışının temel unsurlarındandır.

Bu kapsamda Durak Fındık olarak, bilgi güvenliğini güçlendirmek, riskleri kontrol altına almak, veri gizliliğini sağlamak ve tüm bilgi varlıklarımızı korumak amacıyla:

- Tüm dijital ve fiziksel bilgi varlıklarımız için sistematik bir risk değerlendirme süreci yürütmeyi,
- Bilgi varlıklarını sınıflandırmayı, önem seviyelerine göre değerlendirmeyi ve düzenli olarak güncellemeyi,
- Yetkisiz erişim, veri kaybı, veri sızıntısı, siber saldırı, donanım arızası ve insan kaynaklı hatalar gibi tüm tehditleri belirlemeyi ve analiz etmeyi,
- Riskleri olasılık ve etki kriterlerine göre derecelendirerek yüksek riskleri öncelikli olarak yönetmeyi,
- Teknik ve idari kontrol mekanizmalarını (güçlü parola politikası, antivirüs, güvenlik duvarı, erişim yetkilendirme, çok faktörlü doğrulama, yedekleme, log izleme vb.) etkin şekilde uygulamayı,
- Kritik bilgiler için erişim kısıtlaması ve "bilmesi gereken" prensibini zorunlu kılmayı,
- Çalışanların bilgi güvenliği farkındalığını artırmak amacıyla düzenli eğitimler gerçekleştirmeyi ve tüm personelin bu politikaya tam uyumunu sağlamayı,
- Şirket e-posta sistemi, bulut hizmetleri, mobil cihazlar ve ağ altyapısında güvenlik standartlarını sürekli olarak geliştirmeyi,
- Üçüncü taraf hizmet sağlayıcılar ve iş ortaklarının bilgi güvenliği standartlarına uymasını zorunlu tutmayı; uyumsuzluk halinde düzeltici faaliyet süreçlerini işletmeyi,
- KVKK ve ilgili tüm ulusal/uluslararası bilgi güvenliği düzenlemelerine tam uyum sağlamayı,
- Risk değerlendirme süreçlerini yılda en az bir kez gözden geçirerek güncellemeyi ve yeni sistem, yazılım, proje veya platform devreye alındığında ek risk analizi yapmayı,

- Bilgi güvenliği ihlali, şüpheli durum veya zafiyet tespit edildiğinde hızlı, güvenli ve gizlilik esaslı bir inceleme süreci yürütmeyi,
- Bilgi güvenliği politikamızın; Etik Kurallar, Gizlilik Politikası, Çıkar Çatışması Politikası ve diğer ilgili prosedürlerle bütünsel bir yapıda uygulanmasını sağlamayı,
- Mevzuat değişiklikleri, sektörel riskler, teknolojik gelişmeler ve şirket ihtiyaçları doğrultusunda politikayı sürekli olarak iyileştirmeyi taahhüt ederiz.