Gelecek Varlık

POL01 BİLGİ GÜVENLİĞİ POLİTİKASI

İÇİNDEKİLER

1. AMAÇ

Bilgi Güvenliğinin ve bu politikanın amacı, bilgilerin ve tüm destek iş sistemlerinin, süreçlerinin ve uygulamalarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek, yönetmek ve verilen hizmetlerde müşteri ihtiyaç ve beklentilerini tam olarak karşılanmaktır. Bunun anlamı; bilgilerin yetkili ellerde kalması; bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması ve bilgilerin,

sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır. Bu nedenle Gelecek Varlık ve ilgili tüm taraflar, konumları veya görevleri ne olursa olsun işlerini, bilgilerin Gelecek Varlık bünyesinde korunmasını gözetecek biçimde yapmayı amaçlamaktadır.

2. SORUMLULUK

Yönetim Kurulu ve Üst Yönetim:

Yönetim Kurulu etkili bir bilgi güvenliği yönetim yapısının tesis edilmesi amacıyla, bilgi güvenliği stratejisi ve yol haritasının belirlendiği Bilgi Güvenliği Politikasını onaylar ve uygulanmasını zorunlu tutar. Politika kapsamında hazırlanması gereken tüm standart, prosedür ve talimatların onaylanması için Yönetim Kurulu tarafından, Yönetim Temsilcisi yetkilendirilmiştir. Yönetim Temsilcisi,, Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesi için gerekli kaynak ve yetki / sorumluluk tahsislerini gerçekleştirir. Yönetim Temsilcisi, Yönetim Kurulunu temsilen, periyodik olarak bilgi güvenliği sisteminin gözden geçirmelerinin yapıldığı BGYS Ekibine katılım sağlar

Tüm Çalışanlar:

Bilgi Güvenliği Yönetim Sistemi kategorisinde yayınlanmış tüm politika ve prosedürlere uymakla, gerçekleşmiş ya da olası güvenlik ihlallerini ve zafiyetlerini bildirmek ve BGYS Ekibi tarafından talep edilen tüm faaliyetleri gerçekleştirmekle yükümlüdür.

Üçüncü Partiler:

Gelecek Varlık'ta mal ve hizmet sağlayan üçüncü kişilerin ve bunların çalışanlarının uyması gereken bilgi güvenliğine ilişkin düzenlemeler ilgili sözleşmeler ve güvenlik protokolleri ile belirlenir. Bunlar asgari aşağıdaki hususları kapsar:

• Sözleşmeler veya protokoller ile bildirilen bilgi güvenliği kuralları başta olmak üzere üçüncü taraflarla ilişkileri düzenleyen Gelecek Varlık Politika ve Prosedürleri 'ne uygun hareket etmek.

• Gelecek Varlık'a ait bilgi ve varlıkları Gelecek Varlık onayı ve izni olmadan başkaları ile paylaşmamak.

• Gelecek Varlık tarafından kendilerine verilen kimlikleri mukavelelere ve talimatlara uygun şekilde kullanmak

• Üçüncü partinin Gelecek Varlık ile çalışmakta olan çalışanlarının kendi firmasından ayrılması/görev değiştirmesi söz konusu ise, bu durumu aynı gün içerisinde Gelecek Varlık'a bildirmek ve yetkilerinin iptal edilmesini sağlamak.

• Gelecek Varlık'ın onay ve izni olmadan, Gelecek Varlık'ın cihazlarındaki hiçbir veri ve yazılımı kopyalamamak, ortamın ses kaydını almamak, resmini, videosunu çekmemek, veri güvenliğini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak.

Gelecek Varlık lokasyonlarında yapılacak sistem erişimlerini Bilgi Teknolojileri ekiplerinin gözetiminde gerçekleştirmek.

3. UYGULAMA ESASLARI

Bu politikanın uygulanması hizmet sunulan birimlerle olan ilişkilerde uygunluğu göstermek ve sürdürmek için önemlidir. BGYS, kapsanan bilgi varlıklarıyla herhangi bir ilişkisi olan tüm Gelecek Varlık Yönetimi A.Ş. çalışanları bu politikayı uygulamakla yükümlüdürler ve politikayı onaylamış olan yönetimin desteğine sahiptir. **Politikamız;**

- Kendisinin ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi,

- Tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamayı,
- İş / Hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmayı ve işin sürekliliğini ve sürdürülebilirliğini sağlamayı,
- Bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygulamayı,
- Kurumsal ve müşteri bilgi varlıklarının gizlilik, bütünlük, erişilebilirlik haklarını korumayı,
- Bilgi Güvenliği Yönetim Sisteminin şartlarına uymayı ve etkinliğinin sürekli iyileştirilmesini sağlamayı,
- Risk Merkezi verilerinin ve kişisel bilgilerin iletilmesinde ve saklanmasında şifreleme, maskeleme gibi güvenliği ve sürekliliğini sağlayacak tedbirlerin alınmasını sağlamayı,
- Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi,
- Bilgi Güvenliği Yönetim Sisteminin işletilmesinde istisnai ve kapsam dışı faaliyetleri de göz önünde bulundurmayı,
- Gerekli bilgi güvenliği görev ve sorumluluklarını belirlemeyi, gerekli kaynağı sağlamayı ve ilgili atamaları yapmayı,
- 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve ilgili diğer mevzuat kapsamında çalışanlara, stajyerlere, ziyaretçilere, tedarikçilere ve ilgili diğer 3.taraflara ait kişisel bilgilerin işlenmesi, korunması ve imhası konusunda tüm sorumlulukları karşılamayı, taahhüt eder.

İLGİLİ DOKÜMANLAR

P00 BGYS El Kitabı

Yönetim Kurulu Temsilcisi

Zehra Sezin ÜNLÜDOĞAN