



BİLGİ GÜVENLİĞİ POLİTİKASI

1. Bilgi Güvenliğinin Amacı, Kapsamı ve Konunun Yönetim Tarafından Benimsenmesi

Kplus kurumsal bilgiyi son derece değerli bir varlık olarak kabul etmektedir. Bilgi; iş faaliyetlerimizin sürdürülebilmesi açısından kritik önem taşır ve uygun bir şekilde korunması gerekir. Kplus, Bilgi Güvenliği Yönetim Sistemi (BGYS) ISO 27001 standardını uygulayarak kurumsal bilginin Gizlilik, Bütünlük, Kullanılabilirlik ile ilgili ortaya çıkabilecek riskleri ve bu risklerin etkilerini en aza indirmeyi amaçlar.

Bu politika Kplus üst yönetimi tarafından onaylanmıştır.

Kplus üst yönetimi özellikle aşağıda belirtilen konuların yerine getirilmesini benimsemiştir:

- Kplus bilgilerinin ve bilgi sistemlerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanmasını
- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetilmesini,
- Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmeyi,
- Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamayı,
- Bilgi Güvenliği Yönetim Sistemi'nin yaşatılması için sürekli iyileştirme fırsatlarının değerlendirmeyi ve çalışmalarını gerçekleştirmeyi,
- Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmeyi,
- Bu politikaya bağlı diğer alt prosedürlerin Bilgi ve İletişim Teknolojileri sorumluları tarafından hazırlanmasını ve yayınlanmasını.

Kplus, Bilgi Güvenliği Politikaları ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, kurum bilgilerini veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve kurum bilgilerine erişim gereği olan üçüncü şahıs hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır.

2. Tüm Çalışanların Sorumlulukları

Bilgi Güvenliğinin ve bu politikanın amacı, bilgilerin ve tüm destek iş sistemlerinin, süreçlerinin ve uygulamalarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek ve yönetmektir. Bunun anlamı; Kplus' a ait bilgilerin yetkili ellerde kalması; bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması; ve bilgilerin ve sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır. Bu nedenle tüm kurum ve dış kaynaklı personel ile stajyerleri, konumları veya görevleri ne olursa olsun işlerini, bilgilerin kurum bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur.



BİLGİ GÜVENLİĞİ POLİTİKASI

Kplus' a ait bilgilerin eksiksiz, doğru ve kullanılabilir durumda hazır olmasının sağlanmasının yanı sıra tüm personel, Personel sözleşmelerinde belirtilen gizli bilgilerin korunması ve kurum iş ahlakı ilkelerine de uymak zorundadır.

Kplus; Kişisel Verilerin Korunması Yasasında belirtilen önlemleri almayı ve Kişisel Verilerin Korunması Politikasına tam uyumlu çalışmayı taahhüt eder.

3.Politika Sahipliği ve Bilgi Güvenliğinde Rehberlik Sağlanması

Bu politikanın ve tüm standartların ve diğer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliği Bilgi Güvenliği Yöneticileri tarafından yürütülecek ve bu yöneticilik, aynı zamanda politikanın tüm kurum bünyesinde uygulanmasıyla ilgili olarak tavsiye kaynağı ve rehber olacaktır.

Bilgi Güvenliği Yöneticileri tüm çalışanların, Bilgi Güvenliği konularıyla ilgili uygun bilinçlenme düzeyinin oluşmasını sağlayacak uygun eğitimleri almalarını temin edecek ve genel olarak bilgi güvenliği olaylarının ele alınmasında rehberlik edecektir. Gerekli olduğunda bu politikanın ayrıntılı standartlar, prosedürler ve süreçlerle desteklenmesini ve bunların gerek doğrudan kullanıma hazır olmasını sağlayacaktır. Ayrıca bu politika gereklerinin tüm çalışanlara (daimi veya dönemsel) ve tüm yüklenici personeline aktarılmasını sağlamaktan sorumlu olacaktır.

Bilgi Teknolojileri Yöneticisi, Bilgi Güvenliği ile ilgili genel yönetim çerçevesinin oluşturulmasından ve sürekliliğinin sağlanmasından ve bu politikanın, güncel olarak yaşamasını ve kurum iştiraklerinin işle ilgili gerekliliklerini veya bilgilerinin ve bilgi sistemlerinin karşı karşıya olduğu risk ortamındaki ya da tehditlerdeki değişimleri yansıtmaya devam etmesini temin edecek şekilde devamlı gözden geçirilmesinden sorumlu olacaktır.

Bilgi Güvenliği politikaları Kplus bilgi varlıklarının karşı karşıya olduğu güncel riskleri yansıtmaları amacıyla yapılan varlık ve risk güncellemelerine paralel olarak yılda en az bir defa gözden geçirilirler. Yeni riskleri ve risklerde meydana gelen değişiklikleri kontrol altında tutmak için Bilgi Güvenliği Politikaları yeni gerekli eklemeler yapılarak güncellenir. Ayrıca herhangi bir kurum çalışanı Bilgi Güvenliği Politikaların gelişmesi ve kurumun ihtiyaç duyduğu kontrolleri daha iyi yansıtmaları amacıyla politikaların değiştirilmesi konusunda Bilgi Güvenliği Yöneticiliğine talepte bulunabilir. Yapılan talepler Bilgi Güvenliği Yöneticiliği tarafından ele alınır ve değerlendirilir.

Bilgi Güvenliği Politikası ilkeleri, Kplus insan Kaynaklarının personel kurallarına paralel uygulanmalıdır. Çalışanlar ayrıca Bilgi Güvenliği Politikasının farkında olmaktan ve bu ilkelere uymaktan sorumludur.

4.Denetleme ve Politikalara Uyulması ve Uyulmama Durumlarının Çözülmesi

Her birim yöneticisi Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetlemekten birinci derece sorumludur.

Bilgi Güvenliği Yöneticiliği başta Bilgi Güvenliği Ana Politikası olmak üzere yayınlanmış olan tüm politika ve prosedürler ile ilgili standartlara uyumun periyodik olarak denetiminden ve ilgililere raporlanmasından sorumludur.

Bilgi Güvenliği Politikası ihlalleri, Kplus' ın risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca yeni Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Dolayısıyla söz konusu ihlal aynı zamanda kurum Personel Yönetmeliği ihlali olup disiplin cezası sonucunu doğurabilir. Gerek gözetim, gerek denetim, gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlalleri istihdama son verilmesine



BİLGİ GÜVENLİĞİ POLİTİKASI

hatta Adli ve Cezai yasal işlemler başlatılmasına varıncaya kadar gidebilecek şirket içi disiplin cezaları ile sonuçlanabilecektir.

Bu politikanın uygulanması konusunda hep birlikte çalışılması, bilgilerimizin ve itibarımızın sürekli olarak korunmasına ve işimizin başarısının devamlılığının sağlanmasına yardımcı olacaktır.

5.Bilgi Güvenliği Politikası

Kplus Bilgi Güvenliği, kurum itibarının, güvenilirliğinin, bilgi varlıklarının korunması, temel ve destekleyici iş faaliyetlerinin mümkün olan en az kesinti ile devam etmesi amacıyla,

- Kurumun, işlediği, muhafaza ettiği ve diğer kuruluşlar ile paylaştığı bilgi varlıklarını gizlilik, bütünlük ve erişebilirlik ilkelerine göre korumak,
- Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri uygulamak için kurulmuş yönetim sistemini geliştirmek ve sürekli iyileştirmeyi sağlamak,
- Kurum vizyon ve misyonuna uygun olarak faaliyetlerden kaynaklanan risklerin değerlendirilmesi ile sürekli iyileşme ihtiyaçlarını ve fırsatları tayin etmek,
- Hizmet verilen kapsam bağlamında teknolojik gelişim ve değişimlere ayak uydurarak takip etmek,
- Bilgi güvenliği risklerinin etkisini azaltarak iş sürekliliğini sağlamak,
- Tâbi olduğu ulusal ve uluslararası düzenlemelere, yasal ve ilgili mevzuat gereklerine, anlaşmalardan doğan yükümlülüklerle, iç ve dış paydaşlara yönelik kurumsal sorumluluklara uyum sağlamak
- Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak
- Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek
- Kurum itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak,
- Kişisel Verilerin Korunması Kanunu kapsamında kişi bilgilerini muhafaza etmek,
- Çalışanların bilgi güvenliği farkındalığı ve yetkinliklerini geliştirecek eğitimleri gerçekleştirmek, gerekli desteği sağlayarak diğer yönetim sistemleriyle bütünleşik olarak sektörde örnek bir kuruluş olmak,

Her bir Kplus çalışanı bu hedeflere katkı sağlamaktan sorumludur.

Genel Müdür