ÇELEBİ HAVA SERVİSİ A.Ş. BİLGİ GÜVENLİĞİ POLİTİKASI

- Şirketin tüm birimleri tarafından, süreçler göz önünde bulundurularak bilgi güvenliği riskleri değerlendirilir; risklerin önceliği belirlenir ve gereken önlemler alınır.
- Bilgi işlenirken, iletilirken, muhafaza edilirken, tüm aşamalarında gizlilik, bütünlük ve erişilebilirlik özelliklerinin işin ve ilgili bilginin gereklerine uygun seviyede korunması gerekir.
- Üst yönetim, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi için yeterli kaynağı tahsis eder ve güvenlik politikasıyla uyumlu olacak şekilde gerekli güvenlik kontrollerinin tesis edilmesini sağlar.
- Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır.
- Güvenlik alanındaki güncel gelişmeler, yeni tehditler ve zafiyetler takip edilir, gerekli yazılım güncellemelerinin ve yamaların uygulanması sağlanır.
- Bilgi güvenliği ihlaline ilişkin olaylar izlenir ve periyodik olarak değerlendirilir.
- Karar ve eylemlerde, güvenilir nesnel bilgiler ile teknolojinin tüm olanaklarının kullanılmasına önem ve öncelik verilir. Kullanılan bilgi teknolojileri sistemlerindeki verinin güncel ve doğru olması sağlanır.
- Kurumsal değerlerin gereği olarak gizliliğe önem verilir; her türlü müşteri bilgisi, kuruma rekabet avantajı sağlayan organizasyon, alt yapı, süreç ve teknoloji bilgisi, her tür kişisel bilginin gizliliği politikalar, süreçler ve ileri teknoloji başta olmak üzere gereken güvenlik önlemleri ile sağlanır.
- Bilgi güvenliği hususunda hem kurum içinde hem de kullanıcılar ve üye işyerleri nezdinde farkındalığı artıracak çalışmalar gerçekleştirilir.
- Bilgi sistemleri ve bilgi sistemleri üzerinde işlenen, saklanan ve iletilen veriler, güvenlik hassasiyet derecelerine göre sınıflandırılır ve her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir.
- Bilginin sahibi istemedikçe, yetki verilmedikçe veya yasal gereklilikler oluşmadıkça bilgi paylaşılmaz.
- Çalışanlar gizli bilgi içeren ortamları etiketlemeli ve gözetimsiz bırakmamalıdır.
- Çalışanların yetkilerinin olmadığı bilgi varlıklarına erişimi engellenir.
- Ağa karşı yapılacak saldırılardan korunmak için uygun güvenlik önlemleri alınır.
- Şirket bilgileri sadece yönetimin onayladığı amaçlar için kullanılabilir.
- Çözümlerin müşteri ihtiyaçlarına ve uluslararası standartlara uygunluğunu garanti edebilmek için, kendi alt yapımızın sürekliliği sağlanır.
- İlgili yasal gereklilikler takip edilir ve uygulanır.
- Bilgi güvenliği gereklilikleri politikalar ile tanımlanır, tüm çalışanlara duyurulur ve tüm çalışanların bu politikalara uyması sağlanır.
- Bilgi güvenliği politikası tüm çalışanlara ve ilgili üçüncü taraflara duyurulur.
- Tüm çalışanlar ve ilgili üçüncü taraflar bilgi güvenliği politikasının gereklerini yerine getirmekten bizzat sorumludur.
- Bilgi güvenliği politikasının uygulanmaması veya ihmal edilmesi durumunda disiplin prosedürü ve ilgili sözleşmelerin yasal gerekleri uygulanır.
- Şirketimizin bilgi sistemlerine yılda en az bir kez sızma testi dış kaynak tarafından yapılır. Saptanan bulgular için aksiyonlar planlanır.
- Her yıl çalışanlarımıza en az bir kez bilgi güvenliği farkındalık eğitimi verilir. Çalışanlarımız, bilgi güvenliği politika ve prosedürlerine erişim yetkileri olan ortak alan üzerinden erişir.
- Bilgi güvenliği politika ve prosedürleri ilgili sorumlular tarafından yılda bir kez gözden geçirilerek içeriğin güncelliği sağlanır. Güncellenen dokümanlar çalışanlara ve ilgili üçüncü taraflara duyurulur.