Bilgi Güvenliği Politikası

Firmamız "VERİ MERKEZİ, BİLİŞİM GÜVENLİĞİ, VERİ DEPOLAMA, SANALLAŞTIRMA, AĞ ÇÖZÜMLERİ VE YENİ NESİL BİLİŞİM TEKNOLOJİLERİ ALANINDA YAZILIM GELİŞTİRME VE UYGULAMA, DONANIM (VERİ DEPOLAMA, IP TELEFON, ACCESS POİNT, SWİTCH,SERVER VB) SATIŞI VE KURULUM FAALİYETLERİ alanında hizmet vermektedir. Firmamız gizlilik, bütünlük ve tüm fiziksel ve elektronik bilgi varlıklarını korumayı taahhüt etmektedir. Bilgi ve bilgi güvenliği gereksinimleri kurumsal hedeflerimiz ile aynı doğrultuda olacaktır. Firmamız yönetimi değişime açık, iyi eğitim almış, konusunda yetkin personel istihdamı sağlayacak ve sektör içerisinde rakiplerimizle rekabeti sağlayacak finansmanı sağlamak, yeterli donanım ve altyapıyı bulunduracaktır. Bu altyapı ve personel ile birlikte gerekli finansmanda sağlanacaktır. İş sürekliliği ve acil durum planları, veri yedekleme prosedürleri, virüslerden ve bilgisayar korsanlarından sakınma, erişim kontrol sistemleri ve bilgi güvenliği ihlal bildirimi temel faaliyetlerimizin temel taşlarını oluşturacaktır. Yapılan risk değerlendirmeleri sonucunda elde edilen açıklıklar ve tehditler bertaraf edilerek müşteri ve personelimizin bilgilerine güvenli erişim sağlanacaktır.

Ayrıca risk değerlendirmeleri sonucunda amaçlarımızı belirleyip bu amaçlarım başarılması için gerekli olan kaynaklar ve şartlar sağlanacaktır.

Bu politikayı gerçekleştirmek için başta çalışanlarımızın Bilgi Güvenliği Yönetim Sistemi şartlarını çalışma biçimi haline getirmelerini beklemekteyiz. Tüm personel ve belirli üçüncü tarafların Bilgi Güvenliği Yönetim Sistemi ile ilgili uygun eğitimleri alması sağlanacaktır.

Bilgi güvenliği ile ilgili uygulanabilir şartlar ve bu şartların getirdiği fırsatlar ve gereklilikler yerine getirilecek ve bu şartlar sürekli iyileştirilecektir. Ayrıca firmamızın, personelimizin ve tüm ilgili tarafların bu sisteme adaptasyonu sağlanacaktır.

Bilgi Güvenliği Politikamız yılda bir kez ya da firmamızla ilgili önemli değişikliklerin olması durumunda uygunluğunu, doğruluğunu ve etkinliğini sağlamak için yönetim ve birim sorumlularının katılımıyla gözden geçirilmekte ve güncelliği sağlanmaktadır.

Erişim Kontrolü Politikası

Müşterilerimizin taleplerine zamanında ve doğru çözümler bulabilmemiz için yasal mevzuata uygun şekilde verinin bütünlüğünün sağlanması için:

- Oryantasyon aşamasında personele gerekli bilgiler aktarılmıştır,
- Gerekli altyapı ve donanım belirlenmiştir,
- Gerekli altyapı ve donanımın kesintisiz olarak sağlanması için, gerekli kaynaklar ayrılmıştır,
- Müşteri bilgilerinin korunması açısından yapılması gerekenler personelimize eğitimlerle aktarılmış, personel sözleşmeleri ile sorumlulukları yazılı hale getirilmiştir,
- Tüm verilerin yedeklenmesi amacıyla gerekli alt yapı belirlenip, sorumlular tanımlanmıştır,

- Network üzerinde gerekli erişim işlemleri sınırlandırılmıştır,
- Şirketimizin bilgi güvenliği konusundaki 3 temel prensibi gizlilik, bütünlük ve yetkililerce erişilebilirliktir.

Temiz Masa Temiz Ekran Politikası

Personel kendisine tahsis edilen bilgisayarlarda, üzerinde çalıştığı proje dosyaları, firma dokümanları vb. bilgi ve belge içeren her türlü evrak ile çalışırken ortak depo alanı kullanmakla yükümlüdür. Bu dokümanları bilgisayarında depolayamayacağı, şirket dışına çıkaramayacağı düzenlenen eğitimlerle Yönetim Temsilcisi tarafından bütün personele bildirilir. Bu dokümanları işleme-düzenleme uygulamalarını bilgisayarın masaüstünde ilgili şekillerde klasörler oluşturarak, masaüstünü düzenli bir biçimde kullanması gerektiği konusunda da bilgilendirilmiştir.

Basılı dokümanla çalışmak durumunda olan personel, bu dokümanları işi tamamlandığında gerekli alanlara yerleştirmek zorundadır ve aynı dokümanları masasında açık bir şekilde bırakamayacağı konusunda da bilgilendirilmiştir.

Güvenli Geliştirme Politikası

Güvenli geliştirme güvenli hizmet için bir gerekliliktir. Bunun için öncelikle güvenli geliştirme ortamları kullanılacaktır. Hizmetlerimiz yaşam döngüsü dâhilinde tasarım aşamasında güvenlik gereksinimleri belirlenerek sonrasında bu güvenlik gereksinimlerinin uygulanması sağlanacaktır. Projelerde güvenlik kontrol noktaları oluşturularak yapılan testlerde bu güvenlik kontrollerine uyulması sağlanacaktır. Tüm geliştiriciler açıklıklardan kaçınma, açıklıkları bulma ve düzeltme konusunda kendilerini geliştireceklerdir.

Tedarikçi İlişkileri Politikası

Firmamız gizlilik, bütünlük ve tüm fiziksel ve elektronik bilgi varlıklarını korumayı taahhüt etmektedir. Bilgi ve bilgi güvenliği gereksinimleri kurumsal hedeflerimiz ile aynı doğrultuda olacaktır. Firmamız yönetimi değişime açık, iyi eğitim almış, konusunda yetkin personel istihdamı sağlayacak ve sektör içerisinde rakiplerimizle rekabeti sağlayacak finansmanı sağlamak, yeterli donanım ve altyapıyı bulunduracaktır. Bu altyapı ve personel ile birlikte gerekli finansmanda sağlanacaktır.

Firmamız tedarikçilerinin firmamızda uygulanan Bilgi Güvenliği Yönetim Sistemi Şartlarına uygun olarak faaliyet göstermesini beklemekteyiz. Özellikle bilgi sistemlerimize erişim sağlayan bakım hizmetleri gerçekleştiren ya da sistemi temini sağlayan tedarikçilerin bu konulara uyumu büyük önem göstermektedir. Uyumun sağlanmaması yasal yaptırımları beraberinde getirecektir.

Tedarikçilerimizin özellikle yapılacak tedarikçi sözleşmelerine uyum sağlaması önemlidir. Bu sözleşmeler verilerini korumakla yükümlü olduğumuz müşterilerimiz ve personelimiz için ayrı bir önem taşımaktadır.

Kriptoloji Politikası

Kripto servis bilgileri ve dışardan temin edilen kriptolu kullanılan anahtarları firma tarafından güvenlik verilerine erişim yetkisi bulunan kişiler tarafından saklanmakta ve yönetilmekte olduğunu beyan ederiz.

Kötücül Yazılımlardan Korunma Politikası

Firmamızın bütün PC (Kişisel Bilgisayar) tabanlı bilgisayarları anti-virüs yazılımlarına sahiptir ve bu bilgisayarlar belli aralıklarda düzenli olarak güncellenmektedir. Buna ek olarak anti-virüs yazılımı ve virüs patternleri otomatik olarak güncellenmektedir. Virüs bulaşan makineler tam olarak temizleninceye kadar kurumsal ağdan çıkarılmaktadır. Sistem yöneticileri anti-virüs yazılımının sürekli, düzenli çalışması ve bilgisayarların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur. Zararlı programları (solucan, truva atı vs.) kurum bünyesinde oluşturmak ve dağıtmak yasaktır. Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virüs programını bilgisayarından ve sistemden kaldıramaz.

Teknik Açıklıkların Yönetimi Politikası

Güvenlik açıklarına karşı taranması hususunda politika belirlemektir.

Denetim Sebepleri:

- Bilgi kaynaklarının bütünlüğü ve gizliliğini sağlamak

• Kurumun güvenlik politikalarına uyumunun kontrolü için güvenlik açıklarının tespit edilmesi

• Gerektiği zaman kullanıcıların veya sistemin aktivitelerini kontrol etmek

Bu politika şirketimiz bünyesinde sahip olunan bütün bilgisayar ve haberleşme cihazlarını kapsamaktadır. Bu politika kurumun bünyesinde bulunan fakat kurumun sahip olmadığı herhangi bir sistemi de kapsamaktadır. Denetim yapan kişi veya kurum hizmetlerin durdurulması aktivitesi yapmayacaktır.

İstenildiğinde denetim yapan firmanın bireylerine erişim izni verilecektir. Kurumun birimleri denetim yapan firmaya ağ taraması yapması için protokol, adres bilgileri, ağ bağlantıları hakkında bilgi verecektir.

Kurum denetimi yapan firmaya oluşabilecek sorunlar hakkında danışabileceği bir kişiyi yazılı olarak verecektir.

Kurum ve denetimi yapan firma denetim yapılacak zamanı yazılı olarak bildirecektir.

Kurum ile güvenlik taraması yapacak firma, tarama sonucunda elde edilecek bilgilerin hiçbir şekilde üçüncü şahıslara aktarılmayacağına dair gizlilik anlaşması yapacaktır.

Haberleşme Güvenliği Politikası

5809 Sayılı Elektronik Haberleşme Kanunu temel alınarak; ”bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi” ilkesinin göz önüne alınması gerektiği ifade edilmektedir. Kanunla verilen düzenleme ve denetleme görevleri Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilmektedir.

Bu politika TECH DATA Bilgisayar Sistemleri AŞ yönetimi tarafından gözden geçirilmiş ve onaylanmıştır.

Kişi Tespit Bilgisinin Mahremiyeti ve Korunması Politikası

“A.18 Uyum” “A.18.1 Yasal ve sözleşmeye tabi gereksinimlere uyum” kontrolünün “A.18.1.4 Kişi tespit bilgisinin gizliliği ve korunması” detaylı teknik kontrolü altında “Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde yasa ve düzenlemeler ile sağlanmalıdır.” olarak ifade etmiştir. Buna göre ISO 27001:2013 EK-A’da Bulunan Uygulanabilir Teknik Kontroller temel alınarak;

- Veri sorumlusu;
    a. Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
    b. Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
    c. Kişisel verilerin muhafazasını sağlamak

Amacı ile uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

- Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

- Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

- Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.