BİLGİ GÜVENLİK VE İHLAL POLİTİKASI

TYH A.Ş. Bilgi Güvenliği Politikası

TYH A.Ş. , ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi'nin şartlarını yerine getirmeyi, etkinliğini sürdürmeyi ve sürekli geliştirme faaliyetini devam ettirmeyi, yasal şartlar ve müşteri şartlarını da göz önünde bulundurarak, mevcut ve oluşabilecek riskleri de dikkate almak yoluyla bilgi güvenliği gereksinimlerini karşılamayı politikası olarak belirlemiş ve ilgili taraflara sunmuştur.

1. AMAÇ

Bu politikanın amacı, bilgi güvenlik ihlallerinin önlenmesi ve eğer ihlal gerçekleşirse alınacak önlemleri açıklamaktır.

2. KAPSAM

Bu politikanın ISO 27001:2013 standardı 4.2.1 maddesi gereklerine uygun olarak hazırlanmıştır.

3. SORUMLULUKLAR

3.1. BGYS Direktörü: Politikanın oluşturulmasından sorumludur.

3.2. Bütün Bölümler: Kendi faaliyet alanlarında politikanın uygulanmasından sorumludur.

4. UYGULAMA

- Kullanıcılar tarafından kullanılan bilgisayar yada bilişim cihazlarının hem fiziki hemde yazılımsal (veri) güvenliği kullanıcının kendisine aittir.Kullanıcının şifre güvenliği ise kullanıcı ilk kez sisteme giriş yapana kadar sistem yöneticisine,sisteme dahil olup şifresini değiştirdikten sonra kullanıcının kendisine aittir.

- Sisteme ilk defa giren kullanıcı,bilgi işlem güvenlik gereği şifresini uygun protokoller dahilinde değiştirmeli ve **kimseye söylememelidir.**

- Şifresi geçersiz olan (süresi dolan) yada şifresini unutan kullanıcı en kısa sürede sistem yöneticisi ile irtibata geçmeli ve durumu iletmelidir.

- Yanlış şifre üzerinde güvenlik ihlali oluşturacak gereksiz tekrarlamalardan kaçınılmalıdır.

- Kullanıcı bilgisayara giriş yaptıktan sonra,bilgisayarının başından kısa yada uzun süreli ayrıldığında güvenlik ihlaline sebep olmamak için **pc'yi kilitleme (lock) moduna** almalıdır.

- Şirket içi mail adresi yalnızca iş takibinde kullanılmalı,gereksiz olan mailler belirli zaman aralıklarında kullanıcılar tarafından silinmeli,kaynağı bilinmeyen email yada spam'lar anında imha edilmelidir.

- Standart bir bilgisayar kullanıcısı,ağ ortamında daha önce tanımlanan standart kullanıcıların belirli haklara sahip oldukları bilgilere ulaşabilirler. Bu dosya,doküman yada printer gibi çevresel cihazlara erişimde, kullanıcıların tanımlı olduğu gruptan gelen haklar

dışında hiçbir işlem yapamazlar.Eğer kullanıcının ilgili dosya yada dökümana erişim hakkı yok ise **"Kaynağa erişim yetkiniz yoktur… Lütfen sistem yöneticiniz ile görüşünüz…"** şeklinde bir bilgi mesajı verilmektedir.

- Kullanıcı yetkisi dışındaki klasörlere,dosyalara yada ağ paylaşımlarına erişebiliyorsa bunu en kısa sürede sistem yöneticisine bildirmekle sorumludur.Aksi takdirde güvenliği ihlal etmiş olur.

- Sistemde her bilgisayarın **birbirinden farklı bir fiziksel adresi (Mac Adress) ve network IP adresi (Internet Protocol)** vardır. Kullanıcılar,gerekli olan ağ kaynaklarına düzgün bir şekilde bağlanıp gerekli olan bilgi ve paylaşılan kaynaklara erişebilirler.

- Kullanıcıların internette yasaklanan sitelere girmeleri ve internette güvenliğinden kesin emin olmadıkları kaynakları kullanmalar, güvenlik ihlaline sebep olduğu için uygun değildir.

- Uygunsuz ya da yasadışı internet sitelerine giren kullanıcılar network izleme cihazları ile takip edilip tespit edilirler.Tespit edilen kullanıcılar öncelikle uyarılır.Tekrar eden güvenlik ihlallerinden sonra şirket içi disiplin yönetmeliği gereği uygulanır.

- Kullanıcı erişim hakkına sahip printer,dosya yada dökümana erişip gerekli işlemleri yaptıktan sonra o kaynakla bağlantısını kesmeli,gereksiz yere ağı (networku) meşgul etmemelidir.Böylece bilgi güvenliği ihlal edilmemiş olur.

- Sanal ortamda tanımadığı kimse yada kimselerden bilmediği doküman yada dosyaları almamalı,**şirket içindeki bilgileri de şirketin bilgi gizliliği kapsamında dışarıya çıkartmamalıdır**.

- Yetkisiz personel yada kullanıcıların program yükleme,güncelleme ve silme gibi genel güvenliğe ve talimata aykırı davranmaları kesinlikle yasaktır.

- Kullanıcılar ,mecbur kalmadıkça şirket içindeki diğer bilgisayarları ve başkasına ait veri taşıma disklerini (usb memory) kullanmamalıdır.

- Şirket içinde kullanılan usb yada harici diskler her kullanımda sistemde kullanılan antivirüs programı sayesinde otomatik olarak test edilmeli yada kullanıcı tarafından elle (manual olarak) yapılmalıdır.

- **Çalışanlar sistem ve bilgi işlem genel güvenliği kapsamında, mesai sonunda usb bellek,cd, dvd,disket,harici harddisk yada gizli bilgi içeren şirket dökümanlarını (dosya,klasör,gizlilik içeren yazılı doküman vb..) masada yada açıkta bulundurmamalıdır.**

- Yönetim, şirket içinde kullanılan bilgi işlem cihazlarından ve güvenliğinden,şirket içi bilgilerin gizliliğinden ve bilgi güvenliği ihlalinde yapılması gereken işlemlerden müştereken sorumludur.

4. REFERANSLAR

- ISO 27001:2013 Madde 4..2.1 BGYS'nin Kurulması

5. EKLER

--