GSD VARLIK YÖNETİM ŞİRKETİ A.Ş
BİLGİ GÜVENLİĞİ POLİTİKASI

BİLGİ SİSTEMLERİ
(18.07.2024)

İÇİNDEKİLER

AMAÇ *1*
KAPSAM *1*
TANIMLAR VE KISALTMALAR *1*
I. ORGANİZASYONEL YAPI *2*
1. BİLGİ SİSTEMLERİNİN BAĞLI OLDUĞU MAKAM: **2**
II. GÖREV VE SORUMLULUKLAR *2*
III. RAPORLAMALAR *6*
IV. YÜRÜRLÜK *8*

AMAÇ

Bu politikanın amacı, bilgiyi yaşam döngüsünün her safhasında ve her bilgi saklama ortamında, yetkisiz erişimden, kasıtlı veya kasıtsız hatalı kullanım ve değişiklikten, bozulmaktan ve yok edilmekten korumaktır. Bu şekilde bilginin kullanılabilirliğinin, gizliliğinin ve bütünlüğünün sağlanması hedeflenmektedir.

1. Bilgi Güvenliğinin Sağlanması:

Şirketin bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak.

2. Risk Yönetimi:

Bilgi güvenliği risklerini tanımlamak, değerlendirmek ve yönetmek.

3. Uyum Sağlama:

Yasal düzenlemelere, ulusal ve uluslararası standartlara ve iç politikalara uyumu sağlamak.

4. Güvenlik Bilinci Oluşturma:

Çalışanların bilgi güvenliği konusundaki farkındalığını artırmak ve güvenlik politikalarına uyum sağlamalarını teşvik etmek.

KAPSAM

Bu politika, bilgi saklama ortamlarında var olan, Şirket'e ve müşterilere ait tüm bilgileri kapsamaktadır. Bu politikada bilgi saklama ortamlarında, Şirket'in sahip olduğu tüm Bilgi İşlem uygulamaları ve sistemleri ile bunlarla ortak çalışan her tür bilgi saklama, yedekleme, arşivleme birimleri ve ekipmanları tanımlanmıştır.

Bilginin güvenliği ve güncellenmesine ilişkin hususlar, kimlerin bilgiye erişeceği vb. konular ile ilgili kararlar, Bilgi İşlem Merkezi'nin önerisi ve bilginin sahibi olan birimlerin onayı ile yürürlüğe konulur.

1. Bilgi Varlıkları:

Şirketin sahip olduğu tüm bilgi varlıkları (veri tabanları, dokümanlar, yazılımlar, donanımlar, iletişim ağları vb.).

2. Çalışanlar ve Kullanıcılar:

Şirket çalışanları, taşeronlar, iş ortakları ve bilgi sistemlerini kullanan diğer yetkili kişiler.

3. Bilgi Sistemleri:

Şirketin bilgi işlem altyapısı, yazılım uygulamaları ve iletişim sistemleri.

4. Bilgi Güvenliği Prosedürleri:

Bilgi güvenliği ile ilgili politikalar, prosedürler, rehberler ve standartlar.

TANIMLAR ve KISALTMALAR

Şirket: GSD VYŞ.'yi
Bilgi Güvenliği: Bilginin yetkisiz erişime, kullanıma, ifşaya, bozulmaya, değiştirilmesine veya yok edilmesine karşı korunması.
Gizlilik: Bilginin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlama durumu.
Bütünlük: Bilginin doğruluğunun ve eksiksizliğinin korunması.
Erişilebilirlik: Bilgiye ihtiyaç duyulduğu anda erişilebilmesini sağlama.
Bilgi Varlıkları: Şirketin iş süreçlerini destekleyen bilgi ve bilgi işlem kaynakları.
Risk Yönetimi: Bilgi güvenliği risklerinin tanımlanması, değerlendirilmesi ve kontrol altına alınması süreci.

Saldırı: Bilgi varlıklarına zarar vermeyi, yetkisiz erişim sağlamayı veya işleyişini bozmayı amaçlayan eylem.

BGYS (ISMS): Bilgi Güvenliği Yönetim Sistemi (Information Security Management System)
GDPR: General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)
ISO/IEC 27001: Bilgi Güvenliği Yönetim Sistemi için Uluslararası Standart
KYC: Know Your Customer (Müşterini Tanı)
IT: Information Technology (Bilgi Teknolojisi)
DLP: Data Loss Prevention (Veri Kaybı Önleme)
VPN: Virtual Private Network (Sanal Özel Ağ)
MFA: Multi-Factor Authentication (Çok Faktörlü Kimlik Doğrulama)
APT: Advanced Persistent Threat (Gelişmiş Sürekli Tehdit)
CISO: Chief Information Security Officer (Bilgi Güvenliği Yöneticisi)
ifade eder.

I. ORGANİZASYONEL YAPI

Şirket yönetimi, bir bilgi güvenlik sorumlusu atayıp, bilgi güvenliği meselelerini koordine edecek ve yönetecek rol ve sorumlulukları dağıtır.

Şirket'in faaliyetleri sonucu üretilen tüm bilgiler, Şirket'in mülkiyetindedir. Çalışanların bireysel olarak yürüttükleri çalışmalar sonucu üretilen bilgi de bu kapsam içinde yer alır.

Tüm personelin Bilgi Güvenliği Politikası'nı okuması sağlanır. Ayrıca tüm çalışanlar Bilgi Güvenliği Politikası'nı okuduğu ve kabul ettiğine dair taahhütname imzalar ve bu taahhütnameler personel dosyalarında saklanır.

Müşteri bilgileri ile Şirket'e ait özel bilgiler sadece; müşterinin yazılı izni olduğu, yasal olarak yetkili birimlerin talebi ya da kanuni zorunlulukların gerektirdiği durumlarda üçüncü şahıslara açıklanabilir.

1. BİLGİ SİSTEMLERİNİN BAĞLI OLDUĞU MAKAM:

Bilgi sistemleri yönetimi Genel Müdür'e bağlı olarak çalışan Bilgi Sistemleri sorumlusu tarafından yerine getirebileceği gibi, Yönetim Kurulu onayı ile tamamen dış hizmet alımına konu edilebilir.

II. GÖREV VE SORUMLULUKLAR

Yönetim Kurulu
Yönetim Kurulu, Bilgi Güvenliği Politikasının onaylanması, Şirket'in tüm personeline dağıtımının sağlanması ve bilgi güvenliği raporlarını değerlendirmekten sorumludur.
Yönetim Kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı gösterir, bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder ve aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

- Bilgi güvenliği politikalarının ve tüm sorumlulukların belirli periyotlarla gözden geçirilmesi ve onay mekanizmasına tabi tutulması
- Bilgi kaynaklarına yönelik risklerin ve bilgi güvenliği ihlaline ilişkin olayların periyodik olarak değerlendirilmesi

İç Kontrol Yönetmeni
İç Kontrol Yönetmeni; Şirket çapında bilgi güvenliği yönetim çevresinin uygulanmasının takibinden; bilgi güvenliği bilincinin oluşturulmasından; bilgi güvenliği stratejilerine yön vermekten; bilgi güvenliğine yönelik politika, prosedür, standart ve talimatları önermekten ve gözden geçirmekten; bilgi güvenliğini tehdit eden riskleri tanımlamaktan; kendisine düzenli sunulan bilgi güvenliği raporlarını değerlendirmekten; bilgi güvenliğine yönelik tüm yasal yükümlülüklerin teknik detaylarının hayata geçirilmesi için yönlendirmekten; güvenlik denetimleri sonucu ortaya çıkan bulgu ve açıklıkların takibini koordine etmekten; Bilgi Güvenliği Politikası'ndaki güncellemeleri Yönetim Kurulu'na sunulacak şekilde onaylamaktan sorumludur.

Bilgi İşlem Merkezi
Politika çerçevesinde ele alınan konuların ve stratejilerin hayata geçirilmesi ve uygulamasından; iş yapış şekillerini Yönetim Kurulu ve İç Kontrol Müdürlüğü'nün aldığı kararlar ve stratejiler doğrultusunda Şirket'te oluşturulan politika, prosedür ve standartlara adapte etmekten ve uygulamaktan; Bilgi Güvenliği Politikası'nın ve eklerinin uygulanıp uygulanmadığını belirli aralıklarla kontrol etmekten; güvenlik olayları ile ilgili araştırma yapmaktan; hazırlanan güvenlik farkındalık eğitimlerinin içeriğini ve şeklini oluşturmaktan ve Şirket içindeki güvenlik kontrollerinin durumunu İç Kontrol Yönetmeni'ne düzenli olarak raporlamaktan sorumludur.

Personel/Kullanıcı
Tüm Şirket personeli gerek bu politikada gerekse destekleyici diğer prosedürler ile standartlarda belirtilen bilgi güvenliğine yönelik Şirket yaklaşımına uygun bir şekilde hareket etmekten ve çalışmalarında bunları uygulamaktan sorumludur.

Prosedürler ve Standartlar

Bilgi Varlıklarının Sınıflandırılması
Şirket, işlenen veya saklanan verinin ve bu veriyle ilgili tüm varlıkların gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayarak kazara veya kasti biçimde hasar görmesi, değişmesi, ifşa olması veya kaybolmasını önler. Bunun için varlık değerlendirmelerini yaparak bilgilerini sınıflandırır. Bilgi varlıkları, mümkün olduğu durumlarda, bilgi sınıflandırmasını yansıtacak şekilde etiketlenir. Her varlığa bir sahip atanır.

Bilgi İşlem Risk Yönetimi
Varlıklarla ilgili oluşabilecek riskler değerlendirilir ve bu riskler izlenir. Kontrol uygulayarak azaltılabilecek veya transfer edilebilecek risklerle ilgili kontroller oluşturulur, geri kalan riskler de Üst Yönetim tarafından değerlendirilerek kabul edilir. Şirket'te bilgi güvenliği kontrollerinin etkin bir şekilde hayata geçirilmesi için bilgi teknolojileri varlıklarının risk değerlendirmelerinin ve maruz kaldıkları riskler için kontrol oluşturma çalışmalarının yapılması ve Bilgi İşlem risklerinin kontrol altına alınması için ilgili tüm personel tarafından Bilgi İşlem Politikası'na uyumlu davranılır.

Şifre Yönetimi
Bilgi sistemleri ortamlarına erişirken kullanılan şifrelerin standartlara uygun biçimde oluşturulması, korunması, kullanılması ve değiştirilmesi, kullanıcılara tanımlanan şifreler konusunda çalışanların bilgilendirilmesi ve şifre işlemlerinin riski en aza indirecek en güvenli şekilde yapılmasını sağlamak amacıyla gerekli süreçler oluşturulur ve uygulanır. Bu süreç çerçevesinde, şifre oluştururken ve kullanırken uygulanacak genel kurallar, ana uygulama ve diğer sistemler için şifre parametrelerinin tanımlandığı genel kurallara tüm personel tarafından uyumlu davranılır.

Fiziksel ve Çevresel Koşullar
Şirket faaliyetlerinin gerçekleştirildiği yerlerde, işlenmekte olan bilginin değerine uygun şekilde fiziksel güvenlik önlemleri Şirket tarafından alınır. Başta kritik yazılımlar ve donanımlar olmak üzere Şirket bilgi

sistemlerinin fiziksel ve çevresel güvenliğinin korunması/arttırılması amacıyla oluşturulan genel kurallara tüm personel tarafından uyumlu davranılır.

Sistemlere Erişim ve Yetkilendirme
Şirket'in bilgi sistemlerine erişimde kullanılan kullanıcı hesaplarının yaratılması, izlenmesi ve silinmesi standartlarını tanımlamak, kullanıcıların erişmeye yetkili olacağı uygulamaları ve sistemleri belirleyerek, diğer sistem ve uygulamaları yetkisiz erişimlere karşı korumak amacıyla oluşturulan genel kurallara tüm personel tarafından uyumlu davranılır.

Internet Kullanımı ve E-posta Güvenliği
İnternet'in uygun olmayan kullanımı, Şirket'in yasal yükümlülükleri, kapasite kullanımı ve profesyonel imajı açısından istenmeyen sonuçlara neden olur. Bilerek ya da bilmeden, bu türden olumsuzluklara neden olunmaması amacıyla İnternet'in kurallara, etik ve yasalara uygun kullanımı sağlanır. Kabul edilebilir ve edilmez İnternet kullanımı ile yasaklı web alanlarının tanımı ve açıklaması yapılır.
E-posta, en önemli iletişim kanallarından biridir. E-postalar gönderilirken bilgi gizliliğine dikkat edilir. Üst Yönetim tarafından e-posta gönderimine ilişkin alınan karalar tüm personele iletilerek uyum konusunda gerekli özenin gösterilmesi sağlanır. Ek olarak, e-posta güvenliğine ilişkin gerekli teknolojik kontrollerin oluşturulması Yönetim Kurulu sorumluluğundadır.

Veri Güvenliği
Bilginin, Bilgi İşlem sistemlerine yetkilendirilen kişilerce kontrollü biçimde kaydedilmesi, gizlilik, bütünlük ve kullanılabilirlik ilkeleri doğrultusunda Bilgi İşlem sistemlerinde tutulması ve kullanılması, belirlenen ortamlarda belirlenen süre boyunca yedeklenmesi ve arşivlenmesi, süre bitiminde de imha edilmesi sağlanır. Kamuya açık bilgilerin dışında kalan her türlü bilgiye ve veri işleme kaynaklarına sadece kimliği tanımlanmış, kimliği doğrulanmış ve yetkilendirilmiş kişiler, yetkileri dâhilinde erişir. Bu süreçlerin tanımlandığı genel kurallara tüm personel tarafından uyumlu davranılır.

Zararlı Yazılımlardan Korunma
Hiçbir istisna olmadan, tüm kullanıcı PC'leri, sunucular ve taşınabilir bilgisayarlara anti-virüs yazılımı kurulur; düzenli güncellemelerinin ve taramaların yapılması sistem tarafından sağlanır.
Anti-virüs yazılımı, konusunda uzman ve lider olan bir sağlayıcıdan alınır.
Dışarıdan gelen e-postalar oluşturdukları bilgi güvenliği riskleri göze önünde tutularak özenle ele alınır. Kurum e-posta sunucusuna gelen mesajlar ile ekleri yalnızca virüs taramasından geçtikten ve onaylandıktan sonra iç ağa indirilir.
Yanıltıcı virüs uyarılarına karşı kurum çalışanları bilgilendirilir ve gerekli önlemler alınır.

Lisanslı Yazılım Kurulum ve Kullanımı
Şirket, bünyesinde yer alan bilgisayarlarda lisanssız yazılımların kurulumunu ve kullanımını engeller. Bilgi İşlem Merkezi izinsiz kurulan ve kontrolsüz kullanılan yazılımları tespit eder ve bilgi sistemleri üzerinden siler.

Güvenlik Olaylarının Bildirimi
Şirket bünyesinde, güvenlik olaylarının bildirimi bizzat personelin kendisi tarafından mümkün olan en kısa sürede direk Bilgi İşlem Merkezi'ne telefon ya da e-posta aracılığıyla yapılır. Şirket'in bilgisayar ağında oluşabilecek güvenlik ihlalleri karşısında nasıl davranılacağının belirlenmesi, güvenlik olaylarının sebeplerini analiz edebilmek için gerekli ve yeterli sayıda verinin toplanması ve güvenlik olaylarından sonra sistemin en kısa sürede tekrar çalışır duruma getirilmesi Bilgi İşlem Merkezi'nin sorumluluğundadır. Tüm çalışanlar, şahit oldukları güvenlik ihlallerini sorumlu birimlere iletmekle yükümlüdür.

Şirket Dışına Veri Transferi
Şirket dışına gönderilen tüm veriler için verilerin gizliliği, bütünlüğü ve veri transferine konu olan tarafların kimliklerinin doğrulanması için yeterli kontroller oluşturulur. Transfer edilecek veri için alınacak güvenlik önlemlerine ilişkin kontroller, verinin belirlenen sınıfına göre Bilgi İşlem Merkezi tarafından belirlenir.

Fiziksel olarak yapılan veri transferlerinde sadece yetkili ve güvenli kuryeler kullanılır. Yetkisiz erişimleri engellemek amacıyla parçalara bölerek ya da şifreleyerek gönderme yapılır.

Denetim İzlerinin Yönetilmesi
Şirket'in tüm kritik sistem ve uygulamalarının denetim izleri Bilgi İşlem Merkezi sorumluluğunda saklanır, takip ve analiz edilir. Böylece gerekli görüldüğünde kullanıcı faaliyetleri hakkında detaylı bilgi toplanabilir. Denetim izlerin yönetilmesi için oluşturulan genel kurallara ilgili tüm personel tarafından uyumlu davranılır.

Bilgi Sistemleri Yazılımlarının Alınması, Geliştirilmesi ve Bakımı
Yeni bir yazılım temin edilirken veya mevcut yazılımlarda değişiklik yapılırken; ilgili güvenlik ihtiyaçları, analiz safhasında ele alınır ve güvenlik ihtiyaçları göz önünde bulundurulur. Şirket, yazılımlar için değişiklik kontrol süreci uygular ve sistemleri buna uygun şekilde günceller.
Şirket politikası gereği dışarıdan tedarik edilen hizmetlere ilişkin tedarikçi çalışanları Şirketin belirlediği tüm kurallara uymakla zorunludur.

İş Sürekliliği Yönetimi
Faaliyetlerin devamını sağlamak ve kritik iş faaliyetlerini çeşitli arızalardan ve felaketlerden koruyarak kısa sürede yeniden başlatabilmek için iş sürekliliği ana çatısı oluşturulur ve uygulanır. Bu plan, düzenli olarak test edilir ve değişikliklere karşı gözden geçirilir. Kritik faaliyetlerde kullanılan verilerin yedeği alınır. Şirket'in karşılaşması muhtemel olağandışı olaylar ve felaketler karşısında hazırlıklı olması ve iş sürekliliğini sağlamak amacıyla hazırlanacak genel kurallara tüm personel tarafından uyumlu davranılır.

Güvenlik Farkındalık Eğitimleri
İnsan Kaynakları ve Eğitim Birimi, Şirket personelinin bilgi güvenliğine yönelik farkındalıklarını arttırabilmek amacıyla, çeşitli dönemlerde eğitimler düzenler. Bu eğitimlerin içeriği ve formatı, Bilgi İşlem Merkezi tarafından oluşturulur ve güncellenir.

Bu eğitimler çerçevesinde Şirket Bilgi Güvenliği Politikası ve ilgili prosedürler ile standartlar personele aktarılır ve personel tarafından rol tanımlarının bilinmesi/sahiplenilmesi sağlanır.

Personeli İlgilendiren Konular
Şirket'in tüm personeli Bilgi Güvenliği Politikası'nı okuyup kabul ettiğine dair taahhütname imzalar ve bu taahhütnameler İnsan Kaynakları ve Eğitim Birimi tarafından saklanır. Bilgi Güvenliği Politikası güncellemeleri Bilgi Güvenliği Sorumlusu tarafından tüm personele e-posta ile duyurulur.

Aşağıdaki durumlardan en az birinin gerçekleşmesi durumunda Bilgi Güvenliği Politikası'nın ihlal edildiği sonucuna varılır:
Şirket bilgilerini ve bilgi güvenlik sistemini tehlikeye atarak Şirket'i fiili ve olası iş kaybına maruz bırakmak,
Şirket'in itibarını riske atmak,
Şirket bilgilerini yetkisiz bir şekilde kullanmak, ifşa etmek, değiştirmek, tahrip etmek ve/veya bu bilgileri izinsiz bir şekilde üçüncü kişilerle yazılı/elektronik olarak herhangi ortamda paylaşmak

Şirket, Bilgi Güvenliği Politikası'nın ihlali durumunda bu ihlalin ciddiyetine göre hareket etme hakkını saklı tutar; ancak Politika'ya uymama veya kasıtlı Politika ihlalleri, disiplin cezası, yazılı kınama, işten çıkarma, hukuk muameleleri ve/veya cezai kovuşturmalar dahil olmak üzere bunlarla sınırlı olmayan eylemlerle sonuçlanabilir. Şirket, ihlalin ciddiyetine göre, çalışanın sistemlere erişim haklarını ve ilgili sorumluluklarını askıya alabilir.

Yasal Yükümlülükler
Şirket'in tabi olduğu sektörel kanun, yönetmelik ve düzenlemelerde belirtilen şartların yerine getirilmesinden Yönetim Kurulu ve İç Kontrol Yönetmeni sorumludur. Bilgi güvenliğine yönelik tüm yasal yükümlülüklerin teknik detaylarının hayata geçirilmesinden ise Bilgi İşlem Merkezi sorumludur.

Güvenlik Denetimi ve Uyum
Tüm çalışanlar ilgili yasalara, yönetmeliklere, fikri mülkiyet haklarına, lisans anlaşmalarına, Şirket politika ve prosedürlerine uymakla yükümlüdürler. Tüm çalışanlar, kurum verilerinin saklanması ve gizlilik derecelerine uygun şekilde ele alınması konusunda sorumludurlar.

Şirket, gerek bağlı bulunduğu sektörel düzenlemeler sebebiyle gerekse bilgi güvenliğine yönelik kontrollerin arttırılması amacıyla İç Kontrol Yönetmeni aracılığıyla denetim faaliyetleri gerçekleştirir.

III. RAPORLAMALAR

Yönetim Kurulu, Genel Müdür ya da diğer iş birimleri tarafından ihtiyaç duyulan bilgileri İç Kontrol yönetmeni tarafından yılda iki kez hazırlanacak raporlarla tüm tarafların dikkatine sunulur.

GSD VYŞ dışındaki tüm makamlara ilgili mevzuat gereği hazırlanması ve sunulması gereken raporrın tamamı İç Kontrol yönetmeni tarafından gerçekleştirilir.

IV. BİLGİ SİSTEMLERİ YÖNETİMİNE İLİŞKİN TEMEL İLKELER

- Bilgi teknolojilerinin yapısının, Şirket'in ölçeği, faaliyetlerin ve sunulan ürünlerin niteliği, çeşitliliği ve stratejik hedefleri ile uyumlu olması; Bilgi teknolojileri ile içerdiği verinin güvenilir, doğru, eksiksiz, izlenebilir, tutarlı, erişilebilir ve ihtiyaçları karşılayacak nitelikte oluşturulması esastır. Bilgi teknolojileri asgari olarak;
  - Şirket'le ilgili tüm bilgilerin yurt içinde elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanılmasına veya yedeklenmesine ve kullanılmasına,
  - Sızma ve stres testi yapılabilmesine,
  - Muhasebe kayıtlarının Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurulu tarafından belirlenen usul ve esaslara uygun şekilde muhasebeleştirilmesini imkân verecek yapıda tesis edilir.

- Bilgi teknolojilerinin sürekli biçimde işlerliğini sağlamak üzere BS Süreklilik Planı oluşturulur. Söz konusu planın işlerliği ve yeterliliği düzenli olarak test edilir; ihtiyaç duyulması halinde gerekli tedbirler alınır. İş sürekliliğinin planlanmasında, kritik bilgi teknolojileri varlıkları ile süreçleri belirlenir; bunlara ilişkin iş etki analizi ile risk değerlendirmesi yapılır.

- Bilgi teknolojileri ile içerdiği verinin güvenli biçimde saklanması esastır. Bu çerçevede, veriler, güvenlik hassasiyet derecelerine göre sınıflandırılır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir ve buna göre yedeklenir. Bilgi teknolojilerinin güvenliği ve yedekleme sistemlerinin işleyişi düzenli olarak test edilir ve test sonuçlarına göre ihtiyaç duyulması halinde gerekli değişiklikler yapılır.

- Bilgi güvenliğinin temininde ve Şirket'in Bilgi teknolojilerine erişimde, kimlik doğrulama ve yetkilendirme mekanizmaları ile inkâr edilemezlik ve sorumluluk atama imkânlarını içeren teknikler kullanılır.

-

- Bilgi teknolojilerinin geliştirilmesi, test edilmesi ve işletilmesi süreçlerinde görevler ayrılığı ilkesi uygulanır. Bilgi teknolojileri yönetim sürecinde görev alan bölüm ve çalışanların görev, yetki ve sorumlulukları görevler ayrılığı ilkesine uygun belirlenir.

- Faaliyetlerin yürütülmesi sırasında Bilgi teknolojileri aracılığıyla edinilen ve saklanan müşteri ve Şirket bilgilerinin gizliliğini sağlamak esastır. Müşteri bilgilerinin, yasalarla yetkili kılınmış merciler dışındaki taraflarla paylaşımına ilişkin personele taahhütnameler belirlenir, imzalatılır.

- Bilgi teknolojileri kullanılarak gerçekleştirilen ve şirket faaliyetlerine ait kayıtlarda değişikliğe neden olan işlemlere ilişkin olarak yeterli detayda ve açıklıkta denetim izleri oluşturulur. Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli tedbirler alınır.

Uygulamaya konulan Bilgi teknolojilerinin işleyişi, stratejik hedeflere uygunluğu, kontrollerin etkinliği ve yeterliliği, bilgi teknolojilerindeki gelişmeler de göz önüne alınarak düzenli olarak izlenir. Yeni Bilgi teknolojilerinin Şirket'te uygulanmasının, Şirket'in risk profili üzerinde yaratacağı etki değerlendirilir. Bu çerçevede, gerek duyulması halinde, Bilgi teknolojileri işleyişi revize edilir.

V. BİLGİ GÜVENLİĞİ POLİTİKASI

Şirket *Bilgi Güvenliği Politikası* ile

- Kişisel bilginin mahremiyetinin korunmasını sağlamak amacıyla müşteri ve personel bilgilerinin gizliliğini korur.
- Bilginin bütünlüğünü koruyacak ve sürekli erişilebilirliğini garanti altına alacak altyapıyı ve kontrolleri hayata geçirir.
- Tasarım, geliştirme, test ve uygulama süreçlerinde görevler ayrılığı prensibine uygun yetkilendirmeyi sağlar ve kritik işlemlerde onay mekanizması tesis eder.
- Geliştirme, Test ve Üretim ortamlarının fiziksel ve mantıksal olarak ayrılmasını sağlar.
- Kullanıcıların yetkilendirilmesinde gerekli olan minimum yetkilendirme prensibinin sağlanması ve yetkilerin düzenli olarak kontrol edilmesini sağlar.
- Dış ağlardan gelebilecek tehditlere karşı ağ güvenliğini tesis eder.
- Katmanlı güvenlik mimarisini tesis eder ve sürekli gözetimini sağlar.
- Risk Merkezi verilerinin ve kişisel bilgilerin iletilmesinde ve saklanmasında şifreleme, maskeleme gibi güvenliği sağlayacak tedbirlerin alınmasını sağlar.
- Kullanılan şifreleme anahtarlarının güvenilirliğini sağlar.

- Bilgi güvenliği faaliyetlerinin yönetilmesini ve koordinasyonunu sağlamak amacıyla bir bilgi güvenliği organizasyonu oluşturur.
- Bilgi varlıkları envanterini çıkarır, sahiplikleri belirler ve bilgi varlıkları üzerindeki riskleri yönetir.
- Bilgi güvenliği olaylarının tespit edilmesi, raporlanması ve tekrarının önlenmesi adımlarını içeren bilgi güvenliği olay yönetimi faaliyetleri gerçekleştirir.
- Tüm personele yeterli seviyede farkındalık programı uygular ve bilgi güvenliği gerekliliklerinin karşılanması için tüm çalışanların katılımını sağlar.
- Bilginin işlendiği alanlarda bilginin güvenliğinin sağlanabilmesi amacıyla gerekli fiziksel ve çevresel güvenlik önlemlerini alır.
- Bilgi teknolojileri edinim, geliştirme ve bakımında güvenlik gerekliliklerinin neler olduğunu belirler ve hayata geçirir.
- Belirlenen bilgi güvenliği politikalarına, süreçlerine, yasal ve düzenleyici zorunluluklara çalışanların uymalarını yazılı taahhütlerini alarak zorunlu tutar.
- Bilgiye erişimi kontrol etmek ve yetkisiz erişimleri önlemek için ilgili tüm alanlarda gerekli güvenlik kontrollerini hayata geçirir.

Bilgi teknolojileri faaliyetlerinin işletilmesinde gerekli güvenlik kontrolleri uygular, buna yönelik rol ve sorumlulukları tanımlar.

VI. YÜRÜRLÜK

Bu Politika, Yönetim Kurulu'nun 18/07/2024 tarihli kararı ile yürürlüğe girmiştir.

ONAY

YÖNETİM KURULU ÜYESİ / GENEL MÜDÜR

CANAN SÜMER