BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİLER POLİTİKASI

1. TANIM

Bilgi güvenliği, Şirket'teki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve bilginin geniş çaplı tehditlerden korunmasını sağlar. Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

a. Gizlilik

b. Bütünlük

c. Kullanılabilirlik

a. Gizlilik

Bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

b. Bütünlük

Bütünlük, bilginin, kasten veya ihmal ile yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı, içeriğinin korunarak bozulmamış olma halidir.

c. Kullanılabilirlik

Bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim, kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesine göre, her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

2. KAPSAM

Bu politika, Şirket bilgi işlem altyapısını kullanmakta olan tüm birimleri kapsamaktadır.

3. AMAÇ

Şirket yönetimi, şirketin iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak için bilgi işlem hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziki ve dijital bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

a. E-Posta Kullanma Kuralları

I. Şirketin e-posta sistemi, kullanıcının şahsi sosyal medya (facebook, twitter, instagram vb.) hesapları için kesinlikle kullanılamaz.

II. Kötü amaçlı, spam, sahte vs. nitelikteki zararlı e-postalara yanıt yazılmamalı, bu maillere iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

III. Kişisel kullanım için internetteki uygulamalar aracılığıyla liste ve benzerlerine üye olunması durumunda şirket e-posta adresleri kullanılamaz.

IV. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

V. Çalışanlar, e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

VI. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Eposta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

VII. Şirket çalışanları kurumsal e-postaların firma dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

VIII. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

IX. Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren bilgi işlem departmanı ile temasa geçip onlara durumu haber vermekle yükümlüdürler.

X. Şirketten ayrılan personel, kurumsal e-posta sistemini kullanmaya devam edemez. Eposta adresine sahip kullanıcının birim değiştirme, işten ayrılma gibi herhangi bir sebeple şirketten ayırılması durumunda e-posta sisteminde gerekli değişiklikler yetkililer tarafından Bilgi İşlem Birimine en kısa zamanda bildirilir.

b. İnternet Kullanım Politikası

I. Hiçbir kullanıcı Şirketin tavsiye ettiği veri paylaşım yöntemi dışındaki bir veri paylaşım kanalını kullanamaz.

II. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde mesajlaşma ve sohbet programları gibi chat programları kullanılarak kişisel veri toplanamaz.

III. Hiçbir kullanıcı özel amaçlı olarak internet üzerinden Multimedia Streaming (Video, müzik ve iletişim vb. için) yapamayacaktır.

IV. İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek ve bilgisayarlarda saklamak yasaktır.

V. İnternet üzerinden Bilgi İşlem Birimi tarafından onaylanmamış yazılımlar indirilemez ve firma sistemleri üzerine bu yazılımlar kurulamaz, kullanılamaz.

VI. Şirket ağlarından ve bilgisayarlarından genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

VII. Bilgi İşlem Birimi, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir. Gerekli durumlarda internet üzerinde kısıtlamalar yapabilir.

VIII. Herhangi bir siyasi içerik ya da propaganda yapılamaz.

c. Genel Kullanım Politikası

I. Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3. şahısların bilgilere erişimi engellenmelidir.

II. Şirket verilerini içeren bir bilgisayarın veya taşıyıcının çalınması, kaybolması vs. durumlar en kısa sürede Bilgi İşlem Birimi'ne bildirilmelidir.

III. Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek Şirkete veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret veya siyasi içerikli mail, kullanıcı bilgileri vs.) kişi sorumludur.

IV. Şirketin bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.

V. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişilmemelidir.

VI. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.

VII. Şirket bilgileri üçüncü kişilere iletilmemelidir.

VIII. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

IX. Herhangi bir cihaz, yazılım ve veri izinsiz olarak şirket dışına çıkarılmamalıdır. Şirketin kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD'leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.

X. Personel, kendilerine tahsis edilen ve şirket çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliğinden sorumludur.

XI. Bilgi İşlem Birimi kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir, gereken teknik veya idari tedbirleri uygulayabilir.

XII. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

XIII. Bilgisayarlar üzerinde resmî belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

XIV. Şirkette Bilgi İşlem Birimi bilgisi olmadan Ağ Sisteminde (Web Hosting, E-Posta Servisi vb.) sunucu niteliğinde olan bilgisayar ve cihaz bulundurulmamalıdır.

XV. Bilgi İşlem Biriminin bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

XVI. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisanssız yazılımı bilgisayarında barındıran personel bu durumdan kendisi sorumludur.

XVII. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde mutlaka şifre kullanım kurallarına göre hareket edilmelidir.

XVIII. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir.

c. Acil Durum Politikası

I. Şirketimizde loglama yapılmaktadır. Acil durumlarda sistem logları incelenmek üzere saklanmalıdır.

II. Şirket faaliyetlerinin devamlılığını sağlamak esastır. Acil durumlarda bu esasa yönelik teknik tedbirler planlanmalı ve gerektiğinde uygulanmalıdır.

III. Acil durumlar için gerekli araç-gereç ihtiyaçları tespit edilerek, yedekleme ve bakım planlaması yapılarak uygulanmalıdır.

d. Antivirüs Politikası

I. Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem Birimine haber verilmelidir.

II. Zararlı programları (Örneğin, virüsler, solucanlar, truva atı, e-posta bombaları vb.) Şirket bünyesinde oluşturmak ve dağıtmak yasaktır.

III. Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını kuramaz.

4. ŞİFRELEME

Şifreleme, bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre, ağ güvenliğini tümüyle riske atabilir. Güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkındaki standartlar ve uyulması gereken kurallar aşağıda belirtilmiştir.

5. GENEL BİLGİLER

a) Şifre Kullanma Kuralları

I. Kullanılan şifrelerin tamamı kolayca kırılamayacak güce sahip olmalıdır.

II. Şifreler (E-posta, internet, PC vs.) en az altı ayda bir değiştirilmelidir.

III. Şifreler e-posta iletilerine veya herhangi bir elektronik forma yazılmamalı ve eklenmemeli, başkası ile paylaşılmamalı, fiziki ya da elektronik ortamlara yazılmamalıdır.

IV. Herhangi bir kişiye telefonda şifre verilmemelidir.

V. Şifreler, işten uzakta olunan zamanlarda dahi iş arkadaşlarıyla paylaşılmamalıdır.

VI. Kullanıcı, şifresini 3. kişilerle paylaşmamalı, kağıtlara ya da elektronik ortamlara yazmamalıdır.

VII. Şifre 5 defa üst üste yanlış girildiğinde bilgisayar kilitlenmektedir.

VIII. Çoklu giriş yapılan bilgisayarlara giren personellere uyarılar yapılmaktadır.

IX. Mutlaka ekran kilidi kullanılmalı ve ekran kilidi kısa aralıklara ayarlanmalıdır.

b) Genel Şifre Oluşturma Kuralları

I. Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs.). Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

II. Şifre, küçük ve büyük karakterlerle (a-z, A-Z), rakam ve sembollere (0-9, !'^+%&/()=?_;* gibi) sahip olmalıdır.

III. En az sekiz karakter olmalıdır.

IV. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıdan şifresini değiştirmesi talep edilecektir.

c) Şifre Koruma Standartları

I. Şirket bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanılmamalıdır. (Örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde).

II. Değişik sistemler için farklı şifreleme kullanılmalıdır. Örneğin, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanılmalıdır.

Aşağıdakiler yapılmayacakların listesidir:

- Herhangi bir kişiye telefonda şifre vermek.
- E-posta mesajlarında şifre belirtmek.
- Üst yöneticinizle şifreleri paylaşmak.
- Başkaları önünde şifreler hakkında konuşmak.
- Aile isimlerini şifre olarak kullanmak.
- Herhangi bir form üzerinde şifre belirtmek.
- Şifreleri aile bireyleri ile paylaşmak.
- Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmek.

Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem Birimi yetkilisini araması söylenmelidir. Uygulamalarda ve browserlardaki "şifre hatırlama" özellikleri seçilmemelidir. (Örnek: Chrome, Internet Explorer vs.)

d) Uygulama Geliştirme Standartları

I. Uygulama geliştiricileri programlarında aşağıda belirtilen güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

II. Bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.

III. Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

IV. Kural yönetim sistemi desteklenmelidir. (Örnek; bir kullanıcı diğer bir kimsenin şifresini bilmeden fonksiyonlarına devam edebilmelidir.)

e) Uzaktan Erişen Kullanıcılar için Şifre Kullanımı

I. Şirketin bilgisayar ağına uzaktan erişimi tek yönlü şifreleme algoritması veya güçlü şifrelerle yapılmalıdır.

f) Sunucu Güvenliği

Sunucuların güvenliğinin sağlanması için uyulması gereken kurallar ve standartlar şunlardır.

i. Sahip Olma ve Sorumluluklar

Şirket bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu grup tarafından yapılacaktır.

a. Bütün sunucular ve mobil cihazlar ilgili şirketin cihaz envanterinde kayıtlı olmalıdır. Envanter en az aşağıdaki bilgileri içermelidir:
   - Sunucuların yeri ve sorumlu kişi.
   - Donanım ve İşletim Sistemi.
   - Ana görevi ve üzerinde çalışan uygulamalar.
   - İşletim Sistemi versiyonları.

b. Kişisel veri güvenliğine ilişkin tedbirler alınmak kaydıyla Şirket bütün bilgilerin güncel olarak tutulmalıdır.

c. Şirkette izin verilen bilgi işlem sistemleri haricinde yabancı bir mobil cihaz ya da veri taşıyıcı takılamaz, kullanılamaz.

ii. Genel Konfigürasyon Kuralları

a. İşletim sistemi konfigürasyonları bilgi işlem biriminin talimatlarına göre yapılacaktır.

b. Kullanılmayan servisler ve uygulamalar kapatılacaktır.

c. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, yama ve anti

virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.

d. Uygulama erişimleri için standart güvenlik prensiplerini çalıştırılmamalı, gereksiz servisler açılmamalıdır.

e. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.

f. Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

g. Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar.

iii. Gözlemleme

a. Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır:

- Bütün güvenlikle ilgili loglar minimum 1 hafta saklanmalıdır ve online olarak erişilmelidir.
- Günlük tape backupları en az 1 ay saklanmalıdır.
- Logların haftalık tape backupı en az 1 ay tutulmalıdır.
- Aylık full backuplar en az 6 ay tutulmalıdır.
- Logloma kayıtları bina dışında olmalıdır.

b. Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikli ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.

- Port tarama atakları.
- Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.
- Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

iv. Uygunluk

a. Denetimler yetkili organizasyonlar tarafından şirket bünyesinde atanan Sorumlu tarafından altı ayda bir yapılacaktır.

b. Denetimler Bilgi İşlem Birimi tarafından yönetilecektir.

c. Denetimlerde organizasyonun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

v. İşletim

a. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.

b. Sunucuların yazılım ve donanım bakımları yılda bir yetkili uzmanlar tarafından yapılmalıdır.

c. Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

6. KİMLİK DOĞRULAMA VE YETKİLENDİRME

Bilgi sistemlerinde Kimlik Doğrulama ve Yetkilendirme, konusunda alınması gereken önlemler, uyulması gereken kurallar ve standartlar şunlardır:

a. Şirket sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.

b. Şirket sistemlerine erişmesi gereken kurum dışı ve extranet kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacaktır.

c. Şirket bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenmelidir.

d. Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve gereksinimler ve gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.

e. Erişim ve yetki seviyelerinin sürekli güncelliği temin edilmelidir. f. Kullanıcılar şirket adına kullanımları için tahsis edilmiş sistemlerin güvenliğinden sorumludurlar.

g. Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

h. Sistemlere log-in olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.

i. Kullanıcılara erişim hakları yazılı olarak beyan edilmeli ve erişim haklarını ihlal eden kullanıcılar için yaptırım uygulanmalıdır.

j. Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

k. Dışarıdan şirket wi-fi ağına bağlanacak kimselerin mutlaka kimlik tespiti yapılmalıdır. Toplantı odaları için tahsis edilen wi-fi şifre kullanımları da toplantıya katılanların kimliği ile eşleştirilmelidir.

KİŞİSEL VERİLERİN GÜVENLİĞİ

1. Kişisel Veri Tanımı

6698 Sayılı Kanun'a göre kişisel veri, belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgidir. Örneğin, kişinin adı, soyadı, doğum tarihi, doğum yeri, parmak izi, ses kaydı, aile bilgileri ve telefon numarası vb. Kişisel verilerin mahremiyeti hususunda uyulması gereken temel kurallar şunlardır.

2. Genel Kurallar

Bütün kişisel ve kurumsal bilgilerin güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

a. Şirkette kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin nitelikli verilere erişmesi mümkün olmamalıdır.

b. Kişisel veriler, kişiye aittir. Yetkilendirilmiş çalışanlar ancak görevleri ile ilgili kişisel verilere erişebilmelidirler. Ancak şirket bünyesinde atanmış bulunan ilgili sorumlunun yazılı onayı ile diğer yetki dışındaki kişiler verilere erişebilirler.

c. Müşterinin rızası olmadan hiçbir çalışan sözle de olsa müşteri bilgilerini kişinin yakınları ile ya da tanıdıkları gibi üçüncü şahıslara ve kurumlara iletemez.

d. Müşteri verileri, ticari amaçlı olarak da üçüncü şahıslara iletilemez.

e. Müşterinin talebi halinde bilgilerine ilişkin bir kopya müşteriye teslim edilmelidir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir müşteri kaydı, elektronik veya kâğıt ortamında üçüncü kişi ve kurumlara verilmemelidir.

f. Müşteri ve çalışanlara ait kişisel verilerin izlenmemesi için gerekli tedbirler alınmalıdır. (Kişisel veri içeren hiçbir kayıt gelişi güzel ortada bırakılmamalı, bilgisayar ekranı başkalarınca okunabilecek şekilde bırakılmamalıdır).

g. Telefon ile konuşurken kişisel verilere üçüncü şahısların vakıf olmasına engel olunmalıdır.

h. Bütün kişisel veriler fiziksel olarak korunmuş mekanlarda saklanmalıdır.

i. Şirketin elektronik kayıtlarına internet ortamından erişim mümkün olmamalıdır.

3. KİŞİNİN VERİSİNE HAKİM OLMA HAKKI

Veri sahibi, kendi verisi ile ilgili olarak verisinin nasıl işlendiğini bilme, bilgi talep etme, gerektiğinde güncelleme ve nihayet silinmesini talep etme hakkına sahiptir. Şirket, kullanıcılardan ya da müşterilerden gelecek bu talepleri karşılamak zorundadır.

4. VERİLERİN HUKUKA UYGUNLUĞU İLKESİ

Şirkette bulunan veya şirkete intikal eden ya da şirketten çıkan bütün veriler ve verilerle ilgili her türlü işlem, hukuka ve kişilik haklarına uygun yapılmalıdır. Şirketin bütün çalışanları, şirket müşterilerinin verilerinin gizliliğine saygı göstermek zorundadır.

5. BİLGİ EDİNME HAKKI

Şirket müşterileri, kendi verilerinin nerede ve nasıl kullanıldığını bilme hakkına sahiptir. Bu hakkı kolaylaştıran ve mümkün kılan önlemler şirket tarafından alınır.