# BİLGİ GÜVENLİĞİ POLİTİKASI

| | |
|---|---|
| Doküman No: | BT02 |
| Doküman Sahibi: | BT Müdürü |
| Dokümanı Onaylayan: | Yönetim Kurulu |
| İlk Yayın Tarihi: | 05.07.2023 |
| Gözden Geçirme Tarihi | 20.11.2025 |
| Revizyon No: | - |
| Revizyon Tarihi: | - |
| Hazırlayan Bölüm: | Bilgi Teknolojileri Müdürlüğü |

# İÇİNDEKİLER

# 1. GİRİŞ

## 1.1. Amaç

Politikanın amacı, Kuruluş çalışanlarının görevlerini ve kaynakları kullanırken uyması gereken bilgi güvenliği kurallarını belirleyerek bilginin gizliliğini, bütünlüğünü, erişilebilirliğini sağlamak, kontrol altyapısını geliştirmek ve düzenli olarak politika güncellenmesi çalışmalarını gözetim altında tutmak ve bu sayede Kuruluş' a ait tüm bilgiyi korumaktır.

Bilgi Güvenliği Politikası, aşağıdaki alanlarda Kuruluş genelinde sürekli ve en iyi seviyede bulunmak amacıyla oluşturulmuştur:

a) Bilginin güvenli bir ortamında kullanılmasını sağlamak
b) Programları, verileri, iletişim ağını ve ekipmanları (donanım) kayıplara, yanlış kullanıma ve suiistimallere karşı koruma altına almak
c) Tüm kullanıcıların Politika beyannamesine, ilgili destekleyici politikalara ve prosedürlere bütünüyle uymalarını ve farkında olmalarını sağlamak
d) Tüm kullanıcıların kendi sorumluluklarını, yönetimlerinde olan ve/veya erişebildikleri verinin bütünlüğü ve gizliliğinin önemini anlamalarını sağlamak
e) Kuruluşun genel ihtiyacı çerçevesinde bilgi güvenliğine genel bir bakış açısı ve standartlar bütünü tanımlamak
f) Kuruluşun bilgi güvenliğine olan bakışını vurgulamak ve detaylandırmak
g) Üst Yönetim'in Kurtuluş'ta bilgi güvenliğine verdiği önemi ve desteği ifade etmek
h) Bilgi güvenliğine yönelik sorumlulukların oluşturulmasını sağlamak
i) Kuruluş bilgi güvenliğini tehdit edebilecek olayların oluşmasını engellemek, yönetim ve çalışanların bu amaçla yeterli seviyede bilgilendirilmesini sağlamak

| **İLGİLİ STANDARTLAR** | |
|---|---|
| **Tebliğ** | **Alt Maddeleri** |
| ÖDEME KURULUŞLARI VE ELEKTRONİK PARA KURULUŞLARININ BİLGİ SİSTEMLERİNİN YÖNETİMİNE VE | **Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler**<br>**Bilgi güvenliği ve bilgi güvenliği yönetimi**<br>**MADDE 5**<br>(1) Kuruluş, genel kabul görmüş ilgili uluslararası standartları ve en iyi uygulama örneklerini de göz önünde bulundurarak, faaliyetlerine ilişkin bilgi sistemlerinin |

| | |
|---|---|
| DENETİMİNE İLİŞKİN TEBLİĞ | gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak amacıyla kural, ilke ve politikaları içeren bilgi güvenliği yönetim çerçevesi oluşturur.<br><br>(2) Kuruluş, birinci fıkra kapsamında oluşturduğu bilgi güvenliği yönetim çerçevesine uygun bir bilgi güvenliği yönetim sistemi oluşturur.<br><br>(3) Kuruluş, bilgi güvenliği yönetim sisteminin oluşturulmasına, yönetilmesine, yılda en az bir defa düzenli olarak gözden geçirilmesine ve gerekli hallerde güncellenmesine ilişkin görev, yetki ve sorumlulukları açıkça belirler. |

## 1.2. Kapsam

İşbu politika, Kuruluştaki tüm müşterileri, çalışanları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları, bilgi sistemlerine destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını ve ziyaretçileri kapsamaktadır.

Politika kapsamı aşağıdaki alanları içerecek şekilde oluşturulmuştur:

i. Kuruluşa ait tüm bilgi sistemleri varlıkları ve bileşenleri: Bu bileşenler aşağıdakilerle sınırlı olmaksızın ve saklandığı formata bakılmaksızın bütün bilgi ve verileri ihtiva eder:
   1. Bilgisayar dosyaları ve veri tabanları,
   2. Veri saklama ortamları (Disk, teyp, USB Disk, vb.),
   3. Bilgisayar sistemlerinde üretilen tüm raporlar,
   4. Bilgisayar uygulama ve yazılımları ile bunlara ait dokümanlar,
   5. Tüm e-posta mesajları,
   6. Veri iletim araçları.

ii. Kuruluşa ait iletişim ağları,

iii. Personel, çevresel ve fiziksel alanlar,

iv. Kuruluş süreçler/işleyiş ve yöntemler (iletişim ve işletim süreçleri, risk yönetim süreçleri, İş/BT devamlılık süreçleri vb.),

v. Dış Kuruluş ve şahıslarla ilişkiler ve sözleşmeler,

vi. Kanun ve yönetmeliklere uyum

Ayrıca, Kuruluş Yönetimi;

- Kuruluşun güvenilirliğini ve imajını korumayı,
- Yapılan sözleşmelerin, bilgi güvenliği gerekliliklerini yerine getirdiğinde emin olmayı,
- Kuruluşun temel ve destekleyici faaliyetlerinin en az kesinti ile devam etmesini sağlamayı hedefler.

## 2. TANIMLAMALAR VE KISALTMALAR

**Kuruluş/Şirket:** Hayhay Elektronik Para ve Ödeme Hizmetleri A.Ş.

**Bilgi Teknolojileri (BT):** Elektronik ortamda bilgilerin işlenmesi ve depolanması için kullanılan giriş, işleme, depolama, yedekleme, kopyalama ve yazdırma fonksiyonlarını kapsayan yazılım ve donanımların tümüdür.

**Kanun:** 20/6/2013 tarihli ve 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun

**Tebliğ:** İlgili yasal merci tarafından yayınlanan "Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine Ve Denetimine İlişkin Tebliğ"

**Hassas ödeme verisi:** Kullanıcıların sistemler üzerinde kimliklerini kanıtlamak amacı ile kullandıkları parola, PIN, şifreleme anahtarı, kart numarası, kişisel sertifika, akıllı kart, biometrik bilgi vb. yüksek seviyede gizli sınıfındaki verileri

**Politika:** Bilgi Güvenliği Politikası

**Kriptografi:** Kriptografi, açık ve anlamlı bilgilerin matematiksel algoritmalar ile korunmasıdır.

**Şifreleme (Encryption):** Bilgisayar güvenliğinde verilerin anlaşılmaz kılınacak bir şekilde dönüştürüldüğü ve ancak şifre çözme algoritmasıyla geri kazanılabildiği yöntemdir.

**Sızma testi:** Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amaçlı gerçekleştirilen ataklardır.

**SSH:** Verilerin güvenli bir kanal üzerinden aktarıldığı bir ağ protokolüdür.

**SSL (Secure Socket Layer):** İnternet üzerinde bilginin gizliliğini ve bütünlüğünü korumak için oluşturulmuş bir protokol katmanıdır. Bu protokol bütün yaygın web sunucuları ve tarayıcıları tarafından desteklenmektedir. Bu protokolle çalışan web siteleri 'http' yerine 'https' ile başlar. SSL, gönderilen bilginin sadece doğru adreste deşifre edilmesini sağlar; bilgi gönderilmeden önce şifrelenir ve sadece doğru alıcı tarafından deşifre edilir. Bilginin bütünlüğü de bu süreçte kontrol edilir.

**İz Kaydı (Log):** Bir veri kaynağı hakkında zaman içindeki durumlarının ya da değişikliklerinin kayıt altına alınması sırasında oluşan sistemsel kayıtlardır.

**Kullanıcı:** Şirket bünyesinde istihdam edilen personel

**Müşteri:** Şirket ürünlerinden faydalanan dış kullanıcı

**Üst Yönetim:** Kuruluş yönetim kurulu ile genel müdür ve genel müdür yardımcıları ve başka unvanlarla istihdam edilseler dahi, danışmanlık birimleri dışındaki birimlerin, yetki ve görevleri itibarıyla Genel Müdür Yardımcısına denk veya daha üst konumlarda görev yapan yöneticiler.

**Dış Hizmet Sağlayıcı:** Kuruluşun, Ödeme Sistemleri Yönetmeliğin 14. maddesi çerçevesinde münhasıran kendisi tarafından yapılması gerekenler dışında kalan faaliyetlerini kuruluş adına gerçekleştiren ya da gerçekleştirilmesinde kuruluşa yardımcı nitelikte hizmet veren tüzel kişiler

# 3. GÖREV VE SORUMLULUKLAR

Kuruluşta uygulanacak olan Bilgi Güvenliği Politikası kapsamında görev alan personelin rol ve sorumlulukları aşağıdaki alt başlıklar ile detaylandırılmıştır:

## 3.1. Bilgi Güvenliği Organizasyonu

Bilgi Güvenliği Komitesi, bilgi güvenliği altyapısını desteklemek ve işleyişini devam ettirmek ile sorumludur. Bilgi Güvenliği Komitesi, Genel Müdür, İç Kontrol Müdürü, Bilgi Teknolojileri Müdürü ve Sistem, Network ve Güvenlik Yöneticisi' nden (Bilgi Güvenliği Yöneticisi) oluşur.

## 3.2. Rol ve Sorumluluklar

### 3.2.1. Yönetim Kurulu

Yönetim Kurulu, Bilgi Güvenliği Politikasının onaylanması ve kendisine düzenli sunulan bilgi güvenliği raporlarını değerlendirmekten sorumludur.

### 3.2.2. Üst Yönetim

Kuruluş Üst Yönetimi, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder. Üst Yönetim, aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

a) Bilgi güvenliği politikaların ve tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması,
b) Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,
c) Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,
d) Tüm çalışanlara, hizmet alan kullanıcılara ve üye iş yerlerine bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerinin verilmesi

Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürler, Kuruluşun organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir ve işlerliğine ilişkin gözetim ve takipler gerçekleştirilir.

Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir Bilgi Güvenliği Yöneticisi belirlenir.
Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlanır. Planda kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı belirlenir.

#### 3.2.3. Bilgi Teknolojileri Departmanı

Bilgi Teknolojileri Müdürü ve tüm Bilgi Teknolojileri Departmanı personeli, Politika çerçevesinde ele alınan konuların ve stratejilerin hayata geçirilmesi ve uygulamasından; iş yapış şekillerini Yönetim Kurulu'nun aldığı kararlar ve stratejiler doğrultusunda Kuruluşta oluşturulan politika, prosedür, teknik prosedür ve standartlara adapte etmek ve uygulamaktan sorumludur.

#### 3.2.4. Bilgi Güvenliği Yöneticisi

Bilgi Güvenliği Yöneticisi politikadaki aktiviteleri gerçekleştirmekten sorumludur.

#### 3.2.5. Personel/Çalışan/Kullanıcı

Tüm Kuruluş personeli gerek bu Politikada gerekse destekleyici diğer politika ve prosedürlerde belirtilen bilgi güvenliğine yönelik Kuruluş yaklaşımına uygun bir şekilde hareket etmek ve çalışmalarında bunları uygulamaktan sorumludur.

#### 3.2.6. Diğer Sorumlular

- **Fiziksel Güvenlik Sorumlusu** (Sistem, Network ve Güvenlik Yöneticisi), Kuruluş içinde fiziksel güvenliğin sağlanmasından, kurumsal fiziksel güvenlik standartlarını belirlemek ve bu standartlardan tüm çalışan personeli bilgilendirmek ve uygulanması için gerekli mekanizmaların kurulmasını sağlanmasından, bilgi varlıkları için belirlenen fiziksel güvenlik önlemlerinin gerçekleştirilmesinden ve her seviyede kontrollerin yapılması ve uygulanması için güvenlik personelinin gerekli desteği vermesini sağlamaktan sorumludur.

- **Bilgi Güvenliği Yöneticisi** aynı zamanda Bilgi Varlığı Sahibidir ve bilgi varlığı envanterinin çıkarılması çalışmalarına destek verilmesinden, bu varlıkların korunmasından, risklerinin ve tehditlerinin belirlenmesinden ve söz konusu varlıklara yönelik yetkisiz erişimlerin engellenmesine yönelik kontrollerin belirlenmesinden sorumludur.

- **Altyapı Güvenlik Sorumlusu** (Sistem, Network ve Güvenlik Yöneticisi), tanımlanmış olan güvenlik standartlarının gereklerinin sistemler üzerinde uygulamaya koyulmasından, yeni başlayan veya devam eden tüm projelerin önceden belirlenmiş güvenlik gereksinimlerinin uygulamaya konulmasından, sorumluluğu altındaki güvenlik sistemleri üzerindeki operasyonları

gerçekleştirmekten, sistemler üzerindeki gerekli güncelleme ve yükseltme çalışmalarını yapmaktan, Kuruluşun kullanıcılara sunulan hizmetlerin güvenliğini sağlamaktan, tespit edilen güvenlik ihlallerini ve tehditlerini ilgili taraflara bildirmekten, tespit edilen ihlallerin tekrar edilmemesini sağlayacak çalışmalardan ve sorumluluğu altındaki güvenlik sistemlerinin güvenlik seviyesini arttıracak çalışmaları yapmaktan ve gerekliliklerini raporlamaktan sorumludur.

# 4. UYGULAMA

## 4.1. Bilgi Güvenliği Politikası Uygulama Adımları

### 4.1.1. Bilgi Tanımı

Bu bilgiler şirkete ve müşterilerine ait olan bilgilerdir. Tüm çalışanlar bu bilgiler üzerinde yetkisiz değişiklik yapılmasını, imha edilmesini ve ifşa edilmesini korumakla görevlidir.

### 4.1.2. Bilgi Kapsamı

Kuruluşa ait olan kâğıt üzerinde ve elektronik ortamda var olan bilgilerin tamamıdır.

### 4.1.3. Kullanıcının Bilgi Üzerinde Sorumluluğu

Kullanıcı, Kuruluşa ait tüm bilgileri, her ne amaç olursa olsun, Kuruluş dışına e-posta, internet, kâğıt ve taşınabilir hafıza birimleri vasıtası ile bu bilgileri yayınlayamayacağını kabul eder.

### 4.1.4. Kullanıcın Ayrılması Durumunda Bilgi Üzerinde Olan Hakkı

Kuruluş ile ilişkisi kesilen personel 4.1.1'de tanımı verilen bilgiyi çoğaltamaz, beraberinde götüremez, elektronik veya posta kanalı ile gönderemez. Farklı veya benzeri bir kuruluşta Kuruluşa ait herhangi bir bilgiyi kullanamaz

### 4.1.5. Personelin Bilgilendirilmesi

Kuruluşta yeni işe başlayan tüm personelin bu Politika dokümanını okuması sağlanır. Bu amaçla bu Politika İnsan Kaynakları oryantasyon eğitiminin bir parçası olabileceği gibi Kuruluşun tüm personeline açık olan ortak erişimli dosya paylaşım platformlarında yayımlanır. Bilgi Güvenliği Politikası tüm güncellemeleriyle birlikte ortak erişimli dosya paylaşım platformunda yayımlanır ve tüm Kuruluş çalışanlarının e-posta ile bilgilendirilmesi sağlanır.

Aşağıdaki durumlardan en az birinin gerçekleşmesi durumunda Bilgi Güvenliği Politikası'nın ihlal edildiği sonucuna varılır:

a) Kasten ya da ihmal sonucu Bilgi Güvenliği Politikası'nda ve/veya ilgili alt politikalar, prosedürler, talimatlar ve standartlarda açıkça belirtilmiş maddelere karşı hareket etmek,
b) Kuruluşun itibarını riske atmak,

c) Kuruluş bilgilerini ve bilgi güvenlik sistemini tehlikeye atarak Kuruluşu fiili ve olası iş kaybına maruz bırakmak,
d) Kuruluş 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,
e) Kuruluş bilgi varlıklarını yasal olmayan bir amaç için kasten ya da ihmal sonucu kullanmak

Kuruluş, 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 dâhil olmak üzere bunlarla sınırlı olmayan eylemlerle sonuçlanabilir. Kuruluş, ihlalin ciddiyetine göre, çalışanın sistemlere erişim haklarını ve ilgili sorumluluklarını askıya alabilir.
Kuruluş' bünyesinde personelin **Kabul Edilebilir Kullanım Prosedürü'ne** ve **Bilgi Güvenliği Politikası'na** uyumunu sağlamak adına tüm personel tarafından söz konusu standart ve **Bilgi Güvenliği Taahhütnamesi** imzalanması zorunluluğu bulunmaktadır.

#### 4.1.6.Temiz Masa ve Temiz Ekran İlkesi

**Temiz Masa İlkesi:**

Fiziksel güvenliğin önemli parçası, veri ve dokümanları yetkisiz kişilerin erişiminden korumaktır. Bu amaçla Kuruluşta tüm personelin uyması gereken "Temiz Masa İlkesi" benimsenmiştir.

Bu ilke çerçevesinde tüm Kuruluş personeli, herkese açık çalışma alanlarında ve masalarında Kuruluşa ve müşterilerine ait bilgi, belge, doküman ve bunları içeren her türlü elektronik/manyetik verileri bulundurmamalıdır. Tüm verilerin saklanması için özel koruma imkânları (kilitli dolap, kasa vb.) tercih edilmeli; tüm verileri ve dokümanları başka bir çalışanın masasına ya da çalışma alanına bırakırken yetkisiz erişimlere açık olup olmadığı kontrol edilmelidir.

**Temiz Ekran İlkesi:**

Kuruluşta veri gizliliğin sağlanması ve yetkisiz erişimlerin önlenmesi amacıyla "Temiz Ekran İlkesi" benimsenmiştir.
Bu ilke çerçevesinde Kuruluşta kullanılan tüm sistemler için, uzun süre aktivite olmadığında ilgili oturumun kapatılmasına ilişkin oturum zaman aşımı değerleri tanımlanmalıdır. Personel, bilgisayarında çalışırken gizli kalması gereken verilerin güvenliğini sağlayacak tedbirler alması için bilinçlendirilmelidir. Yıllık bilgi güvenliği eğitimlerinde, personelin masasından ayrıldığında bilgisayarını kilitlemesi gibi koruma tedbirlerine yönelik farkındalık sağlanmalıdır.

#### 4.1.7.Bilgi Varlıklarının Sınıflandırılması

Bilgi sistemleri ve bilgi sistemleri üzerinde işlenen, saklanan ve iletilen veriler ve bu verilerin tutulduğu varlıklar bilgi varlığı olarak adlandırılır. Bilgi varlıklarına gerektiği seviyede ve yeterli miktarda güvenlik önlemlerinin tanımlanması ve oluşturulması için bu varlıkların güvenlik seviyelerine göre sınıflandırılması gerekmektedir. Kuruluşta bu amaçla BT Varlık Yönetimi ve Veri Gizliliği Prosedürü oluşturulmuştur. Bu prosedür çerçevesinde bilgi varlıkları aşağıdaki detayda sınıflandırılır:

| | | | |
|---|---|---|---|
| a) | **Gizli** | Şirket içinde kalır, belirli kişiler tarafından gözlemlenebilir. | **G(1)** |
| b) | **Hizmete Özel** | Müşteri bilgileri ve/veya çalışan özlük içerir. | **G(2)** |
| c) | **Şirket İçi Kullanım** | Şirket içi politika, prosedür vb dokümanlar ve dahili mailler | **G(3)** |
| d) | **Açık** | Herkes ile paylaşılabilen veriler | **G(4)** |

#### 4.1.8.Sistemlere/Uygulamalara Erişim ve Yetkilendirme

Kuruluşun 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 korunmak amacıyla Kullanıcı Erişim ve Yetkilendirme Prosedürü oluşturulmuştur. Bu prosedür çerçevesinde aşağıdaki alanlar ele alınmaktadır:

a) Genel erişim yetkilendirme ve kontrolü,
b) Elektronik para ve Ödeme uygulamalarına erişim yetkilendirme (kullanıcı açma/değiştirme/kapatma),
c) Etki alanı (Domain) erişim yetkilendirme (kullanıcı açma/değiştirme/kapatma),
d) Uzaktan erişim (VPN) talepleri,
e) Destek kuruluşu personeli için erişim yetkilendirme,
f) Acil durum erişim yetkilendirme,
g) Düzenli erişim kontrolü

Bilgi Teknolojileri Departmanı personeli bu standart çerçevesinde son kullanıcı hizmetini sağlayacak ve verilen hizmetin kalitesinin ölçülmesi hedeflenecektir.

#### 4.1.9.Parola ve Kimlik Doğrulama Yönetimi

Kuruluşta bilgi sistemleri ortamlarına erişirken kullanılan şifrelerin standartlara uygun biçimde oluşturulması, korunması, kullanılması ve değiştirilmesi, kullanıcılara tanımlanan şifreler konusunda çalışanların bilgilendirilmesi ve şifre işlemlerinin Kuruluş riskini en aza indirecek en güvenli şekilde yapılmasını sağlamak amacıyla Parola Yönetimi ve Kimlik Doğrulama Prosedürü oluşturulmuştur. Bu

prosedür çerçevesinde şifre oluştururken ve kullanırken uygulanacak genel kurallar, Ödeme ve Elektronik para uygulamaları ile etki alanındaki şifre yönetim süreçleri ele alınmaktadır.

#### 4.1.10. Güvenlik Olaylarının Bildirimi

Kuruluşta Bilgi güvenliği ihlaline ilişkin olayların izlenmesini ve periyodik olarak değerlendirilmesini ve Kuruluşun bilgisayar ağında oluşabilecek güvenlik ihlalleri karşısında nasıl davranılması, güvenlik vakalarının sebeplerini analiz edebilmek için gerekli ve yeterli sayıda verinin toplanması, sistemin en kısa sürede en az zarar ile tekrar çalışır duruma getirilmesi, uygunsuzlukların nasıl raporlanması ve Bilgi Teknolojileri Bölümünün ulaştığı bulgulara karşı nasıl hareket edilmesi gerektiği konusundaki kuralları belirlemek amacıyla Bilgi Güvenliği Olay Yönetimi Prosedürü oluşturulmuştur. Bu prosedür çerçevesinde vakaların tanımlanması ve kategorize edilmesi, vakaların bildirilmesi, değerlendirilmesi ve vaka yönetim sürecinin yönetilmesine yönelik konular ele alınmıştır. İlgili prosedüre göre tüm Kuruluş çalışanları veya üçüncü taraf kullanıcıları, bir güvenlik açığıyla karşılaştıklarında olası güvenlik olaylarını engellemek amacıyla, durumu mümkün olduğu kadar kısa sürede rapor etmelidir. Tüm personel, kullandığı sistemlerin ve uygulamaların durum bilgilerine sahip olmalı ve tüm yetkisiz kullanım ve şüpheli durumları rapor etmek için hazır olmalıdır.

#### 4.1.11. Fiziksel ve Çevresel Güvenlik

Kuruluşun bilgisayar sistemlerinin ve bunların bulunduğu mekânların zarar görmesi ve bu alanların fiziksel ve çevresel tehditlere yönelik olarak yeterli seviyede korunmaması, Kuruluş verilerinin sağlaması gereken gizlilik, bütünlük ve erişilebilirlik kriterlerini yerine getirilememesine sebep olabilir. Bu nedenle kritik BT varlıklarının korunması bilgi güvenliği yönetiminin önemli bir parçasıdır. Kuruluş bu kapsamda aşağıdaki önlemler alır:

- Kuruluşun sistem odasına erişimler yetkili personel ile sınırlıdır ve güvenli alanlara iz kayıtları tutulacak şekilde erişim yapılmaktadır.
- Sistem odasına yetkili personel dışındaki erişimler, ziyaretçi defteri tutularak yetkili personel eşliğinde gerçekleştirilir. Sistem odasının güvenliğinin sağlanması amacıyla erişimler kayıt altına alınır ve kamera kayıtları geriye dönük 1 yıl olmak üzere tutulur.
- Sistem odasında oluşacak herhangi ısı veya nem dalgalanmaları anlık olarak bölüm yöneticilerine bildirilir ve acil durumlar için güvenlik görevlisinde sistem odası erişim yetkisi bulunur.
- Sistem odası, içerisinde bulunan ekipmanların çevresel ve fiziksel faktörlerden korunması maksadıyla gerekli olan cihazlar ile donatılır. Sistem odasında soğutucu klimalar yer almaktadır. Sistem odasında, yükseltilmiş taban kullanılmıştır. Yangın önlemi olarak, FM200 otomatik yangın söndürme sistemi yer alır. Isı ve nem sensörleri bulunur.

- Sistem odası olası elektrik kesintilerine ve arızalarına karşılık, UPS ve Jeneratör Sistemleri bulundurulur.
- Bu ekipmanlar için bakım sözleşmeleri yapılır ve düzenli olarak bakımları gerçekleştirilir.

#### 4.1.12. Değişiklik ve Problem Yönetimi

Kuruluş sunmakta ve kullanmakta olduğu sistem ve hizmetlerin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesi aşamalarında görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlar. Bu kapsamda, söz konusu ortamlara erişim ve söz konusu süreçler tek bir kişi tarafından başından sonuna kadar yetkilendirilmesi ve tamamlanmasına olanak tanımayacak şekilde tasarlanır ve işletilir. Kuruluş değişiklik yönetimi kapsamında son kullanıcılar tarafından bildirilen sorun veya talepleri JIRA Service Desk uygulamasında kayıt altın alır, projelendirilen değişiklikler Kuruluş test metodolojisine uygun olarak test edilir ve gerekli onaylar alındıktan sonra üretim ortamına aktarılır. Kuruluşta söz konusu süreç Değişiklik ve Problem Yönetimi Prosedürü üzerinde detaylandırılmıştır.

#### 4.1.13. Log Yönetimi

Kuruluşun tüm kritik sistem ve uygulamalarının iz kayıtları saklanmakta, izlenmekte ve analiz edilmektedir. Bu analizler neticesinde yatırım ya da çalışma planları oluşturulabildiği gibi bu sistemleri ve uygulamaları kullanan kullanıcılar hakkında da bilgi toplanabilmek için Log Yönetimi Prosedürü oluşturulmuştur.

#### 4.1.14. Ağ Güvenliği ve Yama Yönetimi

Kuruluş üst yönetimi, 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. Kuruluşun bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırılır Kuruluşta ağ seviyesi bilgi güvenliği stratejilerini gizlilik, bütünlük ve erişilebilirlik prensiplerini göz önünde bulundurarak ortaya koyan bir Ağ ve Yama Yönetimi Prosedürü oluşturulmuştur. Bu prosedür çerçevesinde ağ yönetimi ve ilgili sorumluluklar; ağ cihazlarının konfigürasyonu ve yönetimi ele alınmıştır.

Kuruluş bünyesinde kullanılan tüm sistemler ve sunulan tüm hizmetler için, güvenlik alanındaki güncel gelişmeler, yeni tehditler ve zafiyetler ışığında gerekli yazılım güncellemeleri ve yamaları uygulanır. Yama yönetimine ilişkin süreçler Ağ ve Yama Yönetimi Prosedürü içerisinde tanımlanmıştır.

#### 4.1.15. Süreklilik Yönetimi

Kuruluş bünyesinde kullanılan tüm sistemler ve sunulan tüm hizmetler için olası bir felaket veya kesinti durumunda, Kuruluşun faaliyetlerini ve önemli iş fonksiyonlarını destekleyen bilgi sistemleri servislerinin sürekliliğini sağlamak üzere bir süreklilik planı hazırlanır. Süreklilik planı ve süreklilik yönetimi süreçleri İş Sürekliliği Planı, BT Süreklilik Planı ve Acil Durum Yönetimi Prosedürü dokümanlarında detaylandırılmıştır.

#### 4.1.16. Zararlı Yazılımlardan Korunma

Kuruluş bünyesinde kullanılan tüm PC'ler, sunucular ve taşınabilir bilgisayarlar üzerine antivirüs yazılımı kurulur. Yazılımın düzenli güncellemeleri, virüs tanımları ve taramalar sistem tarafından sağlanır.
Antivirüs yazılımı, konusunda uzman ve lider olan sağlayıcılardan alınır.
Dışarıdan gelen e-postalar oluşturdukları bilgi güvenliği riskleri göze önünde tutularak özenle ele alınır. Kuruluş e-posta sunucusuna gelen mesajlar ile ekleri yalnızca virüs taramasından geçtikten ve onaylandıktan sonra iç ağa indirilir.
İnternet üzerinden dosya indirilirken hem art niyetli yazılımlara (virüs, trojan, spyware, adware) hem de uygunsuz içeriğe karşı korunmak için büyük özen gösterilir.
Yanıltıcı virüs uyarılarına (hoax) karşı Kuruluş çalışanları bilgilendirilmeli ve gerekli önlemler alınmalıdır. Sistemde herhangi bir bilgisayarda virüs enfeksiyonu ile karşılaşılması durumunda uygulanacak adımlar önceden belirlenmiş olan süreçler dahilinde gerçekleştirilir.

#### 4.1.17. Güvenlik Risk Değerlendirme Çalışmaları

Kuruluşta bilgi güvenliği kontrollerinin etkin bir şekilde hayata geçirilmesi için bilgi teknolojileri varlıklarının risk değerlendirmelerinin ve maruz kaldıkları riskler için kontrol oluşturma çalışmalarının yapılması kaçınılmazdır.

Bu amaçla Kuruluşun BT ve güvenlik risklerini kontrol altına alabilmek için BT Risk Yönetimi Prosedürü oluşturulmuştur. Bu çerçeve içinde BT varlıklarının sınıflandırılması, bu varlıklara yönelik tehditlerin ortaya çıkartılması, bu tehditlerin ve ilişkili risklerin azaltılması için güvenlik modellerinin oluşturulması ve bunların hayata geçirilmesine yönelik konular ele alınır.

Düzenli olarak risk değerlendirme çalışmalarının yapılması ve takip edilmesi konusunda sorumluluklar belirlenir ve hayata geçirilir.

BT Bilgi güvenliği risklerinin tanımlanması, değerlendirilmesi ve işlenmesi, Kuruluşun risk yönetimi kapsamında ele alınır. Risklerin yönetiminden Bilgi Teknolojileri Müdürü ve Bilgi Güvenliği Yöneticisi sorumludur.

#### 4.1.18. Bilgi Güvenliği Farkındalık Eğitimleri

Kuruluş çalışanlarının, hizmetlerden faydalanan kullanıcıların ve üye iş yerlerinin bilgi güvenliğine yönelik farkındalıklarını arttırabilmek bu politikanın temel amaçlarından biridir. Bu nedenle İnsan Kaynakları eğitim programlarına entegre bir şekilde, Kuruluş çalışanlarına yönelik işe girişte ve çeşitli dönemlerde bilgi güvenliği farkındalığı arttırma ve bilinçlendirme eğitimleri ve farkındalık arttırıcı çalışmalar düzenlenir. Bu eğitimler çerçevesinde Kuruluş, bilgi güvenliği çerçevesinin ve standartlarının çalışanlara aktarılması, güvenlik politika ve standartların farkında olunması ve politikalardaki rol ve tanımların bilinmesi ve sahiplenilmesini amaçlar.

Hizmetlerden faydalanan kullanıcıların ve üye iş yerlerinin bilgi güvenliği farkındalıklarını arttırmak için de sene içinde Kuruluş tarafından hazırlanan eğitimler ve çalışmalar gerçekleştirilir.
Bu eğitimlerin ve farkındalık çalışmalarının içeriği ve formatı Bilgi Güvenliği Yöneticisi tarafından oluşturulur ve güncellenir.

#### 4.1.19. Müşteriyi İlgilendiren Konular

##### 4.1.19.1. Müşteri Bilgilendirilmesi

- Kuruluş tarafından sunulan hizmetlerden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir. Kuruluş, sunmakta olduğu hizmetlere ilişkin riskler ve tehditler hakkında müşterilerini kendi kanalları aracılığı ile uyarır ve bu hususlarda müşteri farkındalığı oluşturulması için azami özen gösterir. Bu kapsamda;
  a) Kuruluş tarafından müşterilerinin hizmeti alabilmeleri için sunulan yazılımlar ya da mobil uygulamalar ile ödeme araçları ve hassas ödeme verilerinin güvenli bir şekilde kullanımına ilişkin yönergeler
  b) Kuruluş tarafından müşterilerine hizmet almaları için sunulan yazılımlar ya da mobil uygulamalar ile ödeme araçları ve hassas ödeme verilerinin kaybedilmesi, çalınması, silinmesi ya da değiştirilmesinin gerekmesi gibi durumlarda müşterilerin takip etmesi gereken adımlar,
  c) Sunulan hizmetlerin taşıdığı riskler ile bu hizmetlere ilişkin koşullar; müşterinin ve Kuruluşun hakları ve sorumlulukları,

d) Dolandırıcılık şüphesi ya da hizmetin alınması sırasında herhangi bir problemle karşılaşılması halinde nelerin yapılması gerektiğine ilişkin yönlendirici talimatlar, kullanıcıların takip etmesi gereken adımlar,

- Kuruluşun kendi kanalları ve iletişim araçları vasıtası ile müşterilerinin dikkatine sunulur.
- Kuruluş bünyesinde, müşterilerin aldıkları hizmetlerden dolayı yaşayabilecekleri sorunların iletilmesine olanak veren, bu sorunların veya şikayetlerin Kuruluş tarafından takip edilip, değerlendirip en kısa sürede çözüme ulaştıracağı imkanlar ve mekanizmalar oluşturulur.
- Kuruluş, müşteriye özel duyuru, uyarı gibi bilgilendirmelerini daha önceden müşteriye bildirdiği kendi kanalları aracılığı ile yapar. Söz konusu kanal üzerinden gelmeyen bilgilendirmelere itibar edilmemesi konusunda müşteriyi bilgilendirir
- Kuruluş, müşterinin işlem bilgilerini ve bakiye bilgilerini müşterinin bilgisine anlık olarak uygulama üzerinden sunar ve takip edebilmesini sağlar.
- Kuruluş internet sitesi aracılığı ile ticaret unvanını, genel müdürlük adresini, Kuruluş ve Kuruluş'un iletişim bilgilerini müşterilerinin bilgisine sunar. Müşterilerin bilgilendirilmesine yönelik her türlü açıklama, Kuruluş'un internet sitesi aracılığı ile müşterinin erişimine kesintisiz olarak sunulur.

#### 4.1.19.2. Müşteri Bilgilerinin Gizliliği

Kuruluş, faaliyetleri sırasında bilgi sistemleri araçlarıyla edindiği, işlediği, ilettiği veya sakladığı tüm müşteri bilgilerinin gizlilik ve güvenliklerini sağlamaya yönelik politika ve prosedürler oluşturur. **(BT Varlık Yönetimi ve Veri Gizliliği Prosedürü)**.

Kuruluş, hassas ödeme verilerini dış hizmet sağlayıcılar ve kanunlarla açıkça yetkili kılınan merciler dışındaki taraflarla paylaşmamayı taahhüt eder. Hassas ödeme verisi dışındaki diğer müşteri bilgileri, ancak müşterinin rızası olması ve paylaşım sınırları açıkça müşteriye bildirilmesi ve gerekli izinleri alması şartıyla, kanunla açıkça yetkili kılınan merciler dışındaki taraflara verilebilir. Söz konusu izinler sözleşme ya da diğer güvenli yöntemlerle alınır. Sözleşme elektronik ortamda alınacak ise, onay yalnızca ilk defa oturum açılırken ve müşterinin açıkça bilgilendirilmesi kaydıyla gerçekleştirilebilir.

### 4.1.20. Bilgi Sistemlerine İlişkin Sınırlamalar

- Kuruluşun hassas ödeme verilerinin ve diğer müşteri bilgilerinin tutulduğu birincil ve ikincil sistemleri yurt içinde bulunur.
- Kuruluşun kendi müşterileri ya da farklı Kuruluşların müşterileri arasındaki ödeme işlemlerinin yürütülmesi sürecinde kullanılan tüm bilgi sistemleri ve bu sistemlerin yedekleri de yurt içinde

bulunur. Benzer şekilde, dış hizmet alınan tüm tedarikçi firmaların, söz konusu hizmetleri yürütmesinde kullandığı bilgi sistemleri ve bu sistemlerin yedekleri de yurt içinde bulunur.

- Ödeme işlemi taraflarından birinin Kuruluş müşterisi olmadığı takdirde, Kuruluş işlemin kendi tarafında gerçekleşen kısımları için Tebliğ hükümlerine tabidir.

### 4.2. Bilgi Güvenliği Raporlaması

Bilgi Teknolojileri Departmanı hazırladığı düzenli raporlar doğrultusunda Kuruluşta bilgi güvenliği politikasına uyum durumunu yılda bir (1) kez Yönetim Kurulu'na raporlar. Bu raporlar doğrultusunda gerek Yönetim Kurulu gerekse Bilgi Güvenliği Komitesi tarafından alınan kararlar Bilgi Teknolojileri Bölümü tarafından hayata geçirilir.

### 4.3. YASAL YÜKÜMLÜLÜKLER

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, Kuruluş Personel Disiplin Yönetmeliği gereğince uyarma, kınama, sözleşme feshi gibi yaptırımlar uygulanır.

### 4.4. GÜVENLİK DENETİMİ VE UYUM

Kuruluş, gerek bağlı bulunduğu sektörel düzenlemeler sebebiyle gerekse bilgi güvenliğine yönelik kontrollerin arttırılması amacıyla denetim faaliyetleri gerçekleştirir. Bu amaçla hem Kuruluş içindeki denetimden sorumlu yetkili birimlerce hem de bağımsız denetçilerce düzenli olarak denetimler yapılır.

Ayrıca dışarıya açık ve kritik sistemler için yılda bir (1) kere olmak üzere bağımsız firmalara sızma testi ve teknik güvenlik denetimleri yaptırılır (**Ağ ve Yama Yönetimi Prosedürü**). Bu denetim ve çalışmalar sonucunda bilgi güvenliğine yönelik ortaya çıkan bulgu ve konuların takibini Bilgi Güvenliği Komitesi yapar; önerilen çözüm ve yöntemlerin hayata geçirilmesinden Bilgi Teknolojileri Departmanı sorumludur.

### 4.5. POLİTİKANIN GÖZDEN GEÇİRİLMESİ VE GÜNCELLENMESİ

Bu politika, Bilgi Güvenliği Yöneticisi tarafından yılda en az 1 (bir) kez gözden geçirilir. Kuruluş Yönetim Kurulu tarafından onaylanır ve Bilgi Güvenliği Yöneticisi tarafından duyurulur. Bilgi güvenliği süreçlerine etkisi büyük değişikliklerde de politikanın gözden geçirilmesi gerekir. İş bölümleri; Bilgi Güvenliği Politikası ve bu politikada belirtilen standartların uygulanması konusunda, değişiklik, ek ya da çıkartma taleplerini detaylı gerekçeleri ile Bilgi Teknolojileri Departmanı'na bildirebilirler.

Bilgi Güvenliği Politikası'nın güncellenmesi için yeter şartlar aşağıda sıralanmıştır:

a) Sistem bileşenlerinde büyük değişiklik olması,
b) Yeni tipte güvenlik ihlallerinin çıkması,

c) Mevzuatta, Kuruluşsal süreçlerde ya da işletim talimatlarında değişiklik yapılması,
d) Güvenlik gereksinimlerinde değişiklik olması,
e) Güvenlik ihlalleri,

Bilgi Teknolojileri Departmanı'nın ihtiyaç duyduğu diğer tüm haller

Bilgi Güvenliği Politikası gözden geçirilirken aşağıda listelenen hususlar özellikle değerlendirilmelidir:

a) Mevcut politikanın etkinliği ve yeterliliği,
b) Tercih edilen güvenlik önlemlerinin ve korunan varlıkların değerleri,
c) Teknolojideki değişiklikler

## 5. İSTİSNALAR

Bu politika kapsamında tüm kararlar Bilgi Güvenliği komitesi raporu ışığında Yönetim Kurulu kararı ile alınır. Hiçbir istisnai durum söz konusu değildir.