ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

İLGİLİ FORMLAR

•

REFERANS DOKÜMANLAR

- **6698 Sayılı Kişisel Verilerin Korunması Kanunu**
- **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik**
- **Kişisel Verilerin İşlenmesi ve Korunması Politikası**
- **Kişisel Veri Saklama ve İmha Politikası**
- **Veri İhlali Müdahale Planı**

REVİZYON TARİHÇESİ

Revizyon No	Tarih	Hazırlayan	Açıklama
00	10.07.2020	Rabia İrtan	İlk yayın

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Rabia İRTAN İç Denetim ve Uyum Uzmanı	Aykut SANCAK İç Denetim ve Uyum Müdürü	Banu HIZLI CEO

1. AMAÇ

- CMC İletişim ve Çağrı Merkezi Hizmetleri A.Ş. (Bundan sonra "Şirket" olarak anılacaktır) veri sorumlusu olarak 6698 sayılı Kişisel Verilerin Korunması Kanunu ("Kanun") uyarınca özel nitelikli kişisel verilerin hukuka uygun olarak işlenmesi ve korunmasına azami önem veriyor ve tüm planlama ve faaliyetlerimizde bu özenle hareket ediyoruz. Bu bilinçle, işbu Politika, Kanun'un 6. maddesi uyarınca oluşturulan "Özel Nitelikli Kişisel Verilerin İşlenme Şartları" Sorumlu olan gerçek veya tüzel kişiler hakkında uygulanacak ve Şirket, Şirket çalışanları ile Şirket'in sözleşmesel olarak sorumlu kıldığı üçüncü kişiler tarafından uyulması gereken esasları belirleyecektir.

- 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 6 ncı maddesinin (4) numaralı fıkrasında, "*Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.*" hükmü yer almaktadır. Buna istinaden Kişisel Verileri Koruma Kurulu'nun 07.03.2018 tarihli Resmî Gazete 'de yayımlanan, 31.01.2018 tarihli Kararı uyarınca Şirket, veri sorumlusu olarak, uhdesinde bulunan özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedür belirlemekle ile yükümlüdür. Buna istinaden Şirket, işbu Politika ile özel nitelikli kişisel verilerin güvenliğine yönelik yönetimini sağlayacağı tüm faaliyetleri kapsayacak şekilde kuralları tanımlamakta, bu verileri kişisel veri işleme envanterine uygun bir şekilde saklamakta ve bunu sürdürmek için gerekli adımları atmaktadır.

2. KAPSAM

- İşbu Politika, Şirket bünyesinde özel nitelikli kişisel verileri işleyen herhangi bir sürece dahil olan tüm departmanları çalışanları ve üçüncü kişileri kapsamaktadır. Politika; Şirket'in özel nitelikli kişisel verilerin güvenliğine yönelik kuralları tanımlayacak ve bu alandaki yönetimi sağlayacak tüm faaliyetleri kapsayacak ve sürdürmek için her adımda uygulanacaktır.

- İşbu Politika özel nitelikli kişisel veri olmayan veriler hakkında uygulanmayacaktır.

3. TANIMLAR

İşbu Politika 'da yer verilen kavramlar aşağıda belirtilen anlamları ifade eder:

Şirket/ Şirketimiz	**:**	CMC İletişim ve Çağrı Merkezi Hizmetleri A.Ş. 'dir.
Kişisel Veri/Veriler	**:**	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
Özel Nitelikli Kişisel Veri/Veriler	**:**	Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik verilerdir.
Kişisel Verilerin İşlenmesi	**:**	Kişisel Verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemdir.
Kişisel Veri Sahibi/İlgili Kişi	**:**	Şirket Paydaşları, Şirket Yetkilileri, İş Ortağı/Tedarikçiler, iştirakçıları, Çalışan, Çalışan

		Adayları'mız, Ziyaretçiler'imiz, Şirket ve Grup Şirket Müşterileri, Potansiyel Müşteriler şirketin işbirliği içinde olduğu kurum/firmalar tarafından şirket ile paylaşılan ve/veya bu kurum/firmalar adına şirket tarafından elde edilen üçüncü kişiler
Veri Kayıt Sistemi	**:**	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt istemini ifade eder.
Kayıt Ortamı	**:**	Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortama verilen addır.
Sicil	**:**	Başkanlık tarafından tutulan Veri Sorumluları Sicilidir.(VERBİS)
Kişisel Veri İşleme Envanteri	**:**	Veri sorumluluarının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerinin; kişisel verileri işleme amaçlarını, veri kategorisini, aktarılan alıcı grubunu ve veri konusunu kişi grubuyla ilişkilendirerek oluşturulan ve detaylandırılan envanterdir.
Veri Sorumlusu	**:**	Kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.
Veri İşleyen	**:**	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişidir.
Açık Rıza	**:**	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.
Kanun	**:**	6698 sayılı Kişisel Verilerin Korunması Kanunu'nu ifade eder.
Yönetmelik	**:**	Kişisel Verilerin Silinmesi,Yok Edilmesi veya Anonim Haline Getirilmesi Hakkında Yönetmelik'tir.
İlgili Karar	**:**	"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" İle ilgili Kişisel Verileri Koruma Kurulu'nun 31.01.2018 tarihli, 2018/10 sayılı kararıdır.
KVK Kurulu	**:**	Kişisel Verileri Koruma Kurulu'dur.

4. KAYIT ORTAMLARI

Şirket nezdinde saklanan özel nitelikli kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.
Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle matbu ortamlar, yerel dijital ortamlardır:

Matbu ortamlar	**:**	1. Verilerin kâğıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlar 2. Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) 3. Yazılı, basılı, görsel ortamlardır.
Yerel dijital ortamlar	**:**	1. Şirket bünyesinde yer alan sunucular 2. Yazılımlar (ofis yazılımları, İK, muhasebe yazılımları e posta sistemleri) 3. Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, ağ cihazları günlük kayıt dosyası, anti- virüs,

		anti-spam vb.) 4. Bilgisayarlar (Masaüstü, dizüstü) 5. Mobil cihazlar (telefon, tablet vb.) 6. Yazıcı, parmak izi okuyucu, tarayıcı, fotokopi makinesi sair dijital ortamlardır.

5. ÖZEL NİTELİKLİ KİŞİSEL VERİ

5.1. Şirket Tarafından İşlenen Özel Nitelikli Kişisel Veriler

Özel nitelikli kişisel veriler Şirket bünyesinde alınan açık rıza aracılığı ile veya Politika'nın 5.2. numaralı bölümündeki ilkeler çerçevesinde işlenmektedir. Şirket ile veri sahibi arasındaki ilişkinin türüne ve niteliğine, kullanılan iletişim kanallarına ve bahsi geçen amaca bağlı olarak çeşitlenmekte ve farklılaşmaktadır. Bu veriler Kişisel Veri İşleme Envanteri içerisinde belirtilmiştir.

5.2. Özel Nitelikli Kişisel Verilerin İşlenmesinde Genel İlkeler

- Şirket özel nitelikli kişisel verilerin işlenmesinde Kurul tarafından belirlenen yeterli önlemlerin alınması konusunda gerekli işlemleri yürütür, bu verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile ilgili gerekli her türlü teknik ve idari tedbirleri alır.

- Şirket, özel nitelikli kişisel verileri Kanun'da belirtildiği şekle uygun olarak işlemektedir.

- Şirket, Kanun'un 6.maddesi 3.fıkrasındaki özel nitelikli kişisel verilerin işlenmesi şartlarındaki istisnalar mevcut olmadığı sürece; açık rızasını almadığı kişilerin özel nitelikli kişisel verilerini işlemez ve saklamaz.

- Özel nitelikli kişisel veriler toplanıp işlenecek ise, alınacak açık rıza sırasında toplanma ve işlenme sebepleri açık olarak belirtilir.

- Sağlık ve cinsel hayat dışındaki kişisel veriler (Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleri) kanunlarda öngörülen hallerde ilgili kişinin açık rıza aranmaksızın işlenebilecektir. Sağlık ve cinsel hayata ilişkin kişisel veriler, Şirket tarafından ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbı teşhis ve tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunduğu koşullarda ilgili kişinin açık rızası aranmaksızın işlenir.

5.3. Özel Nitelikli Kişisel Verilerin İşlenme Amaçları

- Özel nitelikli kişisel veriler, Kanun'a uygun şekilde, kişisel veri işleme envanteri içerisinde, Şirket'in "Kişisel Verilerin işlenmesi ve Korunması Politikası"'nda ve açık rıza sırasında ilgili kişiye belirtilen amaçlar kapsamında işlenmekte olup, bu amaçların ve ilgili yasal sürelerin öngördüğü müddetçe saklanabilmektedir.

- Şirketin, **Kişisel Veri Saklama ve İmha Politikası**'na http://www.cmcturkey.com/adresinden ulaşabilirsiniz.

5.4. Özel Nitelikli Kişisel Verilerin Aktarılması

- Şirket, özel nitelikli kişisel verilerin işlenme amaçları çerçevesinde ve Kanun'un 8 inci ve 9 uncu maddeleri uyarınca yurt içi veri aktarımı yapmaktadır. Özel nitelikli kişisel veriler bu kapsamda

kullanılan sunucu ve elektronik ortamlarda işlenerek saklanabilmektedir. Şirket tarafından hazırlanmış "Kişisel Veri İşleme Envanteri"nde ve "Kişisel Verilerin İşlenmesi ve Korunması Politikası"ında veri aktarımı gerçekleşen taraflar ve veri aktarım amaçları detaylı bir şekilde belirtilmiştir. Yapılan bu aktarımların niteliği ve paylaşım yapılan taraflar, ilgili kişi ile Şirket arasındaki ilişki türüne ve niteliğine, aktarımın amacına ve ilgili yasal dayanağa bağlı olarak değişmektedir. Bu kapsamda Şirket tarafından "**Kişisel Verilerin İşlenmesi ve Korunması Politikası**" içerisinde tanımlanmış olan tedbirler ve uygulama esasları geçerlidir.

- Kişisel Verileri Koruma Kurulu'nun 07.03.2018 tarihli Resmî Gazete 'de yayımlanan, 31.01.2018 tarihli Karar uyarınca Şirket, özel nitelikli kişisel verileri aşağıdaki şekilde aktarır:

I. Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılır.
II. Taşınabilir Bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kripto grafik yöntemlerle şifrelenir ve kripto grafik anahtar farklı ortamda tutulur.
III. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımı gerçekleştirilir.
IV. Verilerin kâğıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınır ve evrak "gizlilik dereceli belgeler" formatında gönderilir.

5.5. Özel Nitelikli Kişisel Verileri İşleme Şartlarının Ortadan Kalkması

- Şirket, özel nitelikli kişisel verilerin işlenme şartlarının ortadan kalktığı durumlarda veri işlemeye devam edemez. Şirket, şartların ortadan kalktığı ortamları ilgili iş birimlerinin ya da BGK/KVK Komitesi'nin talebi üzerine Politika 'ya uygun bir şekilde ortadan kaldırmakla yükümlüdür. Bu kapsamda Şirket tarafından "**Kişisel Veri Saklama ve İmha Politikası**" içerisinde tanımlı olan tedbirler, uygulama usul ve esasları geçerlidir.

- Şirket aşağıdaki örnek olarak listelenen ve Yönetmelik içinde de belirtilen ilgili durumlarda özel nitelikli kişisel veri işleme şartlarının ortadan kalktığını kabul eder:

I. Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması.
II. Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması.
III. Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştirildiği hallerde, ilgili kişinin rızasını geri alması.

5.6. Özel Nitelikli Kişisel Verilerin Güvenliği

Özel nitelikli kişisel verilerin işlenmesinde, Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır. Bu önlemler; Kişisel Verileri Koruma Kurulu'nun 07.03.2018 tarihli Resmî Gazete 'de yayımlanan, 31.01.2018 tarihli Kararı uyarınca aşağıdaki şekilde belirlenmiştir.

I. Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik;

a) Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi,
b) Gizlilik sözleşmelerinin yapılması,

c) Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması,
d) Periyodik olarak yetki kontrollerinin gerçekleştirilmesi,
e) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkilerinin derhal kaldırılması. Bu kapsamda, veri sorumlusu tarafından kendisine tahsis edilen envanterin iade alınması,

II. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise;

a) Verilerin kripto grafik yöntemler kullanılarak muhafaza edilmesi,
b) Kripto grafik anahtarların güvenli ve farklı ortamlarda tutulması,
c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
d) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
e) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
f) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması,

III. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise;

a) Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemlerinin (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alındığından emin olunması,
b) Bu ortamların fiziksel güvenliğinin sağlanarak yetkisiz giriş çıkışların engellenmesi,

Şirket ayrıca Kişisel Verileri Koruma Kurumu'nun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberi'nde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirleri de dikkate almaktadır. Yukarıda Kurul kararına uygun olarak belirlenen önlemlere ek olarak Kişisel Veri Güvenliği Rehberi dikkate alınarak, alınan teknik ve idari tedbirler aşağıdaki gibidir:

5.6.1. İdari Tedbirler

I. Mevcut Risk ve Tedbirlerin Belirlenmesi

Veri güvenliğinin sağlanması için öncelikle Şirket tarafından işlenen kişisel verilerin neler olduğu, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığı ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirler alınır. Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilir ve gerekli teknik ve idari tedbirler planlanarak uygulamaya konulur.

II. Kişisel Veri Güvenliği Politikalarının ve Prosedürlerinin Belirlenmesi

Politika ve prosedürler kapsamında; düzenli olarak kontroller yapılmakta, yapılan kontroller belgelenmekte, geliştirilmesi gereken hususlar belirlenmekte ve gerekli güncellemeler yerine

getirildikten sonra da düzenli olarak kontrollere devam edilmektedir. Ayrıca, her kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenmiştir. Özel nitelikli kişisel verilerin güvenliğinin sağlanması için hazırlanan ve uygulanan Politika ve Prosedürler aşağıdaki gibidir:

- ✓ **Özel Nitelikli Kişisel Verilerin Korunması Politikası (işbu Politika)**
- ✓ **Kişisel Verilerin İşlenmesi ve Korunması Politikası**
- ✓ **Veri İhlali Müdahale Planı**

III. Kişisel Verilerin Mümkün Olduğunca Azaltılması

Kanunun 4 üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri uyarınca kişisel veriler, doğru ve gerektiğinde güncel olarak tutulur, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilir. Şirket, işleme amaçları bakımından özel nitelikli kişisel verilere hala ihtiyaç olup olmadığını değerlendirir ve kişisel verilerin doğru yerde muhafaza edildiğinden emin olur. İhtiyaç duyulmayan özel nitelikli kişisel veriler, "**Kişisel Veri Saklama ve İmha Politikası**" ve **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yönetmeliği**'ne uygun ve güvenli bir şekilde imha edilir.

IV. Veri İşleyen ile İlişkilerin Yönetimi

Şirket, hizmet aldığı veri işleyenden, tüm kişisel veriler konusunda en az kendileri tarafından sağlanan güvenlik seviyesinin sağlandığından emin olur. Veri işleyen ile imzalanan sözleşme veya alınan taahhüt, veri işleyenin sadece Şirket talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin korunması mevzuatı ile uyumlu şekilde hareket edeceğine ilişkin hükümler içerir. Bu hükümler Şirket'in "**Kişisel Veri Saklama ve İmha Politikası**" ile de uyumludur. Şirket'in hizmet aldığı veri işleyen, işlediği tüm kişisel verilere ilişkin olarak süresiz sır saklama yükümlülüğüne tabidir. Veri işleyen herhangi bir veri ihlali olması durumunda, bu durumu derhal Şirket'e bildirmekle yükümlüdür.

5.6.2. Teknik Tedbirler

I. Siber Güvenliğin Sağlanması ve Takibi

Şirket'in iyi yapılandırılmış bir güvenlik duvarı ve ağ geçidi bulunmaktadır. Kullanılmayan yazılım ve servisler güncel tutulmak yerine, silinerek cihazlardan kaldırılmaktadır. Yazılım güncellemeleri ile yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi sağlanmaktadır. Özel nitelikli kişisel veri içeren sistemlere erişim sınırlıdır. Bu kapsamda Şirket çalışanlarına, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmıştır. Çalışanlar, kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlamaktadırlar. Söz konusu şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonlar tercih edilmektedir. Güçlü şifre ve parola kullanımının yanı sıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve Şirket ile ilişikleri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle erişimin sınırlandırılmaktadır. Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden anti-virüs, anti-spam gibi ürünler

kullanılmakta, bu ürünler güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmaktadır.
Bilişim ağlarında hangi yazılım ve servislerin çalıştığı kontrol edilmekte, sızma veya olmaması gereken bir hareket olup olmadığı belirlenmektedir. Tüm kullanıcıların işlem hareketleri kayıtları düzenli olarak tutulmaktadır (log kayıtları gibi). Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanmasının sağlanması için Çalışanların sistem ve servislerdeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulmuştur. (Bkz. Veri İhlali Müdahale Planı)

II. Bilgi Teknoloji Sistemleri Tedariği, Geliştirme ve Bakımı

Şirket tarafından yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmaktadır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmakta, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmektedir. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmıştır. Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamı sökülerek saklanmakta, sadece arızalı parçaların gönderilmesi gibi işlemler yapılmaktadır. Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemler alınmaktadır.

6. GÜNCELLEME, UYUM VE DEĞİŞİKLİKLER

- Şirket, Kanun'da veya ilgili mevzuatta yapılan değişiklikler nedeniyle, KVK Kurulu kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda işbu Politika ve bu Politika 'ya bağlı ve ilişkili diğer politikaları günceller ve bu değişikliği yapma hakkını saklı tutar.

- Şirket, Politika üzerinde yaptığı değişiklikler incelenebilir şekilde, Politika'yı www.cmcturkey.com internet sitesinde erişime sunacak ve değişikliği çalışanlara ve sürece dahil olan üçüncü kişilere bildirecektir.

- İşbu Politika 'da yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar Politika'nın sonunda açıklanır.