



KVKK
KİŞİSEL VERİ SAKLAMA VE
İMHA POLİTİKASI

KASPA DIŞ TİCARET A.Ş.

İÇİNDEKİLER

1. GİRİŞ	1
1.1. Amaç	1
1.2. Kapsam	1
1.3. Kısaltmalar ve Tanımlar	1
2. SORUMLULUK VE GÖREV DAĞILIMLARI	3
3. KAYIT ORTAMLARI	4
4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR	4
4.1. Saklamaya İlişkin Açıklamalar	4
4.2. Saklamayı Gerektiren Hukuki Sebepler	5
4.3. Saklamayı Gerektiren İşleme Amaçları	5
4.4. İmhayı Gerektiren Sebepler	6
5. TEKNİK VE İDARİ TEDBİRLER	6
5.1. Teknik Tedbirler	6
5.2. İdari Tedbirler	8
6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ	9
6.1. Kişisel Verilerin Silinmesi	9
6.2. Kişisel Verilerin Yok Edilmesi	10
6.3. Kişisel Verilerin Anonim Hale Getirilmesi	10
7. SAKLAMA VE İMHA SÜRELERİ	10
8. PERİYODİK İMHA SÜRESİ	12
9. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI	13
10. POLİTİKA'NIN GÜNCELLENME PERİYODU	13

TABLolar LİSTESİ

Tablo 1: Kısaltma ve Tanımlar Tablosu	1
Tablo 2: Saklama ve imha süreçlerinde görev dağılımı	3
Tablo 3: Kayıt Ortamları Tablosu	4
Tablo 4: Veri Silme Yöntemi Tablosu	9
Tablo 5: Veri Yok Etme Tablosu	10
Tablo 6: Süreç bazında saklama ve imha süreleri tablosu	11

1. GİRİŞ

1.1. Amaç

Kişisel verileri saklama ve imha politikası (“Politika”), KASPA Dış Ticaret A.Ş., tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin usul ve esasları belirlemek amacıyla hazırlanmıştır.

1.2. Kapsam

Bu politika, çalışanlarımızın, şirket yöneticilerinin, ziyaretçilerin, çalışan adaylarımızın, hizmet sağlayıcılarımızın, tedarikçilerin, müşterilerin, üçüncü kişilerin kanun kapsamında işlenen kişisel verileri için uygulanmaktadır.

1.3. Kısaltmalar ve Tanımlar

Tablo 1: Kısaltma ve Tanımlar Tablosu

Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiç bir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilmeyecek hale getirilmesi
Çalışan	KASPA Dış Ticaret A.Ş. personeli
Hizmet sağlayıcı	KasGrup firması ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi
İlgili kişi	Kişisel verisi işlenen gerçek kişi

İlgili kullanıcı	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişi
İmha	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi
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 ortam.
Kişisel Veri	Kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.
Periyodik İmha	Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalması durumunda kişisel verileri saklama ve imha politikasında belirlenen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi
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, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Kişisel veri işleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi gruplarıyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere

	aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanter.
Politika	Kişisel verileri saklama ve imha politikası
Veri işleyen	Veri sorumlusunun verdiği yetkiye dayanarak veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişi

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Tablo 2: Saklama ve imha süreçlerinde görev dağılımı

Unvan	Birim	Görev
İnsan Kaynakları Ve İdari İşler Sorumlusu	İnsan Kaynakları Ve İdari İşler	Görevlerine uygun olarak politikanın yürütülmesinden sorumludur
Bilişim Sistem Yöneticisi	Bilgi işlem departmanı	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellemesinden, politikanın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

3. KAYIT ORTAMLARI

Kişisel veriler, şirketimiz tarafından aşağıdaki tabloda gösterilen ortamlarda saklanır ve koruma altına alınır.

Tablo 3: Kayıt Ortamları Tablosu

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım vb.)	Kağıt ve dosyalar
Yazılımlar (Ofis yazılımları, portal)	Birim dolapları
Bilgi güvenliği cihazları (Güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb)	Arşiv
Kişisel bilgisayarlar (Masaüstü, dizüstü)	
Mobil cihazlar (telefon, tablet vb)	
Optik Diskler (CD,DVD, vb)	
Çıkartılabilir bellekler (USB, Hafıza kartı vb)	

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

4.1. Saklamaya İlişkin Açıklamalar

“Kişisel verinin işlenmesi kavramı”, Kanun’un 3. maddesinde tanımlanmıştır. 4’üncü maddesinde ise Kişisel verilerin hukuka uygun olarak işlenebilmesi için uyulması gereken genel ilkeler tanımlanmış 5 ve 6. maddelerde ise kişisel verilerin işlenme şartları sayılmıştır.

Buna göre, Kas Grup faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

4.2. Saklamayı Gerektiren Hukuki Sebepler

Kas Grup faaliyetleri çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 sayılı Kişisel verilerin korunması kanunu,
- 5510 sayılı sosyal sigortalar ve genel sağlık sigortası kanunu
- 5651 sayılı İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun,
- 6331 sayılı iş sağlığı ve güvenliği kanunu,
- 4857 sayılı iş kanunu

4.3. Saklamayı Gerektiren İşleme Amaçları

Kas Grup, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak kullanabilmek
- Yasal raporlar yapmak
- Çağrı merkezi süreçlerini yönetmek
- Kas Grup ile iş ilişkilerinde bulunan gerçek/tüzel kişilerle irtibat sağlamak
- İstatistiksel çalışmalar yapabilmek
- Kas Grup güvenliğini sağlamak
- Kurumsal iletişimi sağlamak
- Hukuki yükümlülüklerin yerine getirilmesini sağlamak
- İnsan kaynakları süreçlerini yürütmesi
- Ticari ilişkilerin yürütülebilmesi
- Sözleşmelerden kaynaklanan yükümlülüklerin ifası
- Müşteri memnuniyeti ve tüketici şikayetlerin giderilmesi
- İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu buna göre düzenlemek ve gerekmesi halinde güncellemek.

Bu dokümanın aslı sanal ortamdadır. Bu doküman gizlilik taşıyan bilgiler içermektedir. Sadece KAYALAR dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

- Yasal düzenlemek gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

4.4. İmhayı Gerektiren Sebepler

Kişisel Veriler;

- İşlenmesini veya saklanmasını gerektiren amacın ortadan kalması
- Kanunun 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Kas Grup tarafından kabul edilmesi,
- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,
- Kas Grubun, ilgili kişi tarafından kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içerisinde cevap vermemesi halinde; Kişisel verileri koruma kurumuna şikayette bulunması ve bu talebin kurul tarafından uygun bulunması,
- İşlenmesine esas teşkil eden ilgili mevzuatın değiştirilmesi veya iptal edilmesi.

5. TEKNİK VE İDARİ TEDBİRLER

Kanunun 12 nci maddesinin 1 inci fıkrasında, veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek ile verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik, her türlü teknik ve idari tedbirleri almakla yükümlü tutulmaktadır.

5.1. Teknik Tedbirler

Kas Grup tarafından işlenen kişisel verilere ilişkin olarak alınan teknik tedbirler aşağıda sıralanmıştır.

Bu dokümanın aslı sanal ortamdadır. Bu doküman gizlilik taşıyan bilgiler içermektedir. Sadece KAYALAR dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

- Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Çalışanlar için yetki matrisi oluşturulmuştur.
- Erişim logları düzenli olarak tutulmaktadır.
- Gizlilik taahhütnameleri yapılmaktadır.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Güncel anti-virüs sistemleri kullanılmaktadır.
- Güvenlik duvarları kullanılmaktadır.
- Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Mevcut risk ve tehditler belirlenmiştir.
- Sızma testi uygulanmaktadır.
- Şifreleme yapılmaktadır
- Veri kaybı önleme yazılımı (DLP) kullanılmaktadır.
- Temiz masa temiz ekran politikası uygulanmaktadır.
- Kas Grup internet sitesi ve web tabanlı uygulamalarına erişimlerde https protokolü kullanılmakta sha 256 bit rsa algoritması ile şifrelenmektedir.
- Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yangın söndürme, iklimlendirme sistemi) ve yazılımsal (güvenlik duvarı, atak önleme sistemi, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb) önlemler alınmaktadır.
- Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmıştır.

- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş ve çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle aktarılmaktadır. Taşınabilir bellek, cd, dvd gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmektedir. Farklı fiziksel ortamlarda ki sunucular arasında ki dosya transferleri vpn ile yapılmaktadır. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmaktadır.

5.2. İdari Tedbirler

Kas Grup tarafından işlenen kişisel verilere ilişkin olarak alınan idari tedbirler aşağıda sıralanmıştır.

- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- Kişisel veri işleme envanteri işlenmektedir.
- Kişisel veri işlenmeden önce aydınlatma yükümlülüğü yerine getirilmektedir.
- Güvenli politika ve prosedürlere uyumayanlara yönelik disiplin prosedürü hazırlanmıştır.
- Kurum tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Çalışanlara KVKK farkındalık eğitimi verilmektedir.
- Veri koruma ekibi oluşturulmuş ve yapmış oldukları toplantılar bir tutanağa bağlanarak saklanmaktadır.
- Sağlık dosyaları doktor odasında kapalı ve kilitli ortamda tutulmaktadır.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

Kişisel veriler, Kas Grup tarafından re'sen veya ilgili kişinin başvurusu üzerine veya mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda silinir, yok edilir veya anonim hale getirilir.

6.1. Kişisel Verilerin Silinmesi

Kişisel verileri aşağıdaki yöntemlerle silinir.

Tablo 4: Veri Silme Yöntemi Tablosu

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucuda yer alan kişisel veriler, saklama süresinin tamamlanmasını takiben, sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silinir.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda bulunan kişisel veriler, saklama süresinin dolmasını müteakiben veri tabanı yöneticisi tarafından kimsenin hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi sağlanır.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel veriler, saklama süresinin tamamlanmasına müteakiben evrak arşivinden sorumlu birim yöneticisi tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

6.2. Kişisel Verilerin Yok Edilmesi

Kişisel verileri aşağıdaki yöntemlerle yok edilir.

Tablo 5: Veri Yok Etme Tablosu

Veri Kayıt Ortamı	Açıklama
Manyetik Ortamda Bulunan Kişisel Veriler	Optik medya veya manyetik ortamlarda bulunan kişisel veriler, saklama süresinin dolması üzerine, kırma, yok etme, toz haline getirme gibi yollarla kullanılamaz hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Saklama süresi dolan fiziksel ortamdaki kişisel veriler, kağıt kırma makinesi kullanmak suretiyle yok edilir.

6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilmeyecek hale getirilmesidir.

7. SAKLAMA VE İMHA SÜRELERİ

Kas Grup tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Kişisel verilerle ilgili olan saklama süreleri, Kişisel Veri İşleme Envanteri Formunda
- Veri kategorileri bazında Verbiste
- Süreç bazında saklama süreleri Kişisel Verileri Saklama Ve İmha Politikasında yer alır.

Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanır.

Tablo 6: Süreç bazında saklama ve imha süreleri tablosu

İNSAN KAYNAKLARI VE HUKUK		
Süreç	Saklama Süresi	İmha Süresi
Sözleşmeler	Sözleşmenin sona ermesini takiben 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
İnsan Kaynakları Süreçlerinin Yürütülmesi (özlük)	Faaliyetin sona ermesini takiben 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
Dava dosyaları ve icra takipleri	Davanın veya icra takibinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
İş başvuru formu özgeçmiş	Başvurunun olumsuz sonuçlanmasından sonra 6 AY	Saklama süresinin bitimini takip eden 7 gün içinde
Mesleki Deneyim (Diploma Gidilen Kurslar, Meslek İçi Eğitimler Sertifikalar, Transkript Bilgileri)	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
Çalışan Giriş Çıkış Kayıt Bilgileri	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
Ziyaretçilerin Giriş Çıkış Kayıt Bilgileri	1 YIL	Saklama süresinin bitimini takip eden gün içinde
İş sağlığı ve güvenliği uygulamaları	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
Güvenlik kamera görüntüleri	2 AY	Saklama süresinin bitimini takip eden gün içinde
Çalışanlar ile ilgili Sağlık kayıtları	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
Sabıka Kaydı	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde

Bu dokümanın aslı sanal ortamdadır. Bu doküman gizlilik taşıyan bilgiler içermektedir. Sadece KAYALAR dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

Ücret ve maaş'a ait tüm belgeler	İş ilişkisinin sona ermesinden itibaren 10 Yıl	İş ilişkisinin sona ermesinden itibaren 10 Yıl
SATIŞ SONRASI DESTEK		
Süreç	Saklama Süresi	İmha Süresi
Çağrı merkezi ses kayıtları	2 YIL	Saklama süresinin bitimini takip eden 180 gün içinde
Servis kaydı oluşturan müşteri kayıtları	10 YIL	Saklama süresinin bitimini takip eden 180 gün içinde
FİNANS		
Süreç	Saklama Süresi	İmha Süresi
Ödeme işlemleri	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
Banka hesap bilgileri	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
Cari kart verileri	İş ilişkisinin sona ermesinden itibaren 10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
BİLİŞİM SİSTEMLERİ		
Süreç	Saklama Süresi	İmha Süresi
İnternet ve wifi logları	3 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde
ERP logları	10 Yıl	Saklama süresinin bitimini takip eden 180 gün içinde

8. PERİYODİK İMHA SÜRESİ

Yönetmeliğin 11. maddesi gereğince Kas Grup, periyodik imha süresini 6 ay olarak belirlemiştir.

Bu dokümanın aslı sanal ortamdadır. Bu doküman gizlilik taşıyan bilgiler içermektedir. Sadece KAYALAR dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

9. POLİTİKA’NIN YAYINLANMASI VE SAKLANMASI

Bu dokümanın aslı sanal ortamdadır. Bu doküman gizlilik taşıyan bilgiler içermektedir. Sadece KAYALAR dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

10. POLİTİKA’NIN GÜNCELLENME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.