1. AMAÇ

Bilgi Güvenliği Yönetim Sistemleri ve Kişisel Veri Yönetim Sistemleri kapsamında organizasyonun hassas bilgilerinin korunmasına odaklanır. Bu prosedürün amacı, kuruluşun müşteri bilgileri, çalışan bilgileri, finansal belgeler ve diğer önemli bilgilerin ve veri saklanan bilişim sistemlerinin (harddisk, cd, usb, vb.) veri imha yöntemlerini belirlemeyerek güvenli şekilde imha edilmesini sağlar.

2. KAPSAM

Bu prosedür, bilişim sistemlerinin (harddisk, cd, usb, vb.), kayıtları tutulan tüm kişisel veri içeren bilgilerin imha edilmesi faaliyetlerini kapsamaktadır.

3. SORUMLULAR

Bu prosedürün düzenlenmesi ve kontrol edilmesinden Yönetim Temsilcisi, uygulanmasından tüm personeller sorumludur.

4. TANIMLAR

İmha: Veri saklanan bilişim sistemlerinin (harddisk, cd, usb, vb) içindeki bilgilerin erişilemez hale getirilmesidir.
KVK: Kişisel Verilerin Korunması
KVKK: Kişisel Verilerin Korunması Kanunu

5. UYGULAMA

5.1. Varlıkların İmhası

Bilgi kayıt özelliğine sahip her türlü cihazın üzerindeki bilgiler yetkisiz erişime karşı silinir ve cihaz üzerindeki disk ve kayıt mekanizması fiziksel olarak tahrip edilir.

5.2. Verilerin Silinmesi Yöntemleri

a) Kağıt ortamında bulunan Kişisel Veriler, kağıt öğütücüsü ile imha edilerek ya da gerekli durumlarda karartma yöntemi kullanılarak silinmektedir.
b) İşletim sistemindeki silme komutu ile silinir.
c) Kalıcı biçimlendirme ile veriler ulaşılamaz hale getirilir.
d) Veri Tabanları: Verilerin bulunduğu ilgili satırlar veri tabanı komutları ile silinir.
e) Sanal Sunucular: sıfır yazdırma işlemi yapılarak silinir.

5.3. Varlıkların ve Verinin Yok Edilmesi Yöntemleri

a) Yerel Sistemlerde: De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerinden uygun olanı kullanılarak yok edilir.
b) Çevresel Sistemler:
- Ağ Cihazları (switch, router vb.) : a maddesinde belirtilen uygun yöntemler ile yok edilir.
- Flash tabanlı ortamlar: İlgili üreticinin önerdiği yöntemler ya da a maddesinde belirtilen yöntemler ile yok edilir.
- Manyetik bant: De-manyetize edilerek ya da yakma, eritme gibi fiziksel yöntemlerle yok edilir.
- Sim Kart ve sabit hafıza kartları: a maddesinde de belirtilen uygun yöntemler ile yok edilir.
- Optik diskler: yakma, küçük parçalara ayırma, eritme gibi fiziksel yöntemlerle yok edilir.
- Veri Kayıt Ortamı sabit olan çevre birimleri: a maddesinde belirtilen uygun yöntemler ile yok edilir.

c) Basılı Ortamlar: Kağıt imha makinaları kullanılarak yok edilir. Orijinal kağıt formattan tarama yoluyla elektronik ortama aktarılan Kişisel veriler ise bulundukları ortama göre uygun yöntemlerle yok edilirler.

5.4. İmha İlkeleri:

Kayıt imha ilkeleri, organizasyonun bilgi güvenliği ve gizliliği ile uyumlu bir şekilde belirli kayıtları imha etmesini sağlayan temel prensiplerdir. Bu ilkeler, organizasyonun yasal düzenlemelere uymasını, bilgi güvenliğini korumasını ve kayıtları gereksiz yere uzun süre saklamamasını sağlar.

5.4.1. Yasal ve Düzenleyici Uyum:

Kayıt imha süreçleri, yasal düzenlemelere ve endüstri standartlarına tam uyum sağlamalıdır. Yasaların ve düzenleyici gerekliliklerin belirlediği süreç ve kriterlere uyum, organizasyonun hukuki ve etik sorumluluklarını yerine getirmesini sağlar.

5.4.2. İhtiyaca Dayalı İmha:

Kayıtların imha zamanı, ihtiyaçlar ve gereksinimlere dayalı olarak belirlenmelidir. Gereksiz yere uzun süre saklanan kayıtların azaltılması ve sadece gereken bilgilerin korunması, kaynak kullanımını optimize eder.

5.4.3. Gizlilik ve Güvenlik:

İmha süreci, kayıtların gizliliğini ve güvenliğini korumalıdır. Kayıtların imha edildiği süreçte yetkisiz erişimlere karşı önlemler alınmalıdır. Fiziksel kayıtlar parçalanmalı veya güvenli bir şekilde yok edilmelidir. Dijital kayıtların silinmesi, üzerine yazılması veya güvenli bir şekilde imha edilmesi gerekebilir.

5.4.4. Belirlenmiş İmha Süreçleri:

Belirli kayıtların imha süreçleri önceden belirlenmiş olmalıdır. İmha süreci adımları, hangi kayıtların ne zaman ve nasıl imha edileceğini net bir şekilde tanımlamalıdır.

5.5. İmha Yöntemleri:

Kayıt imha yöntemleri, organizasyonların bilgi güvenliği standartlarına uygun olarak belirli kayıtları güvenli bir şekilde imha etmelerini sağlayan çeşitli yöntemleri içerir. İmha yöntemleri, kayıtların fiziksel veya dijital formatta olup olmadığına bağlı olarak farklılık gösterebilir. İşte bu yöntemlere örnekler:

5.5.1. Fiziksel Kayıtlar için İmha Yöntemleri:

- **Parçalama (Shredding):**

Kâğıt belgelerin parçalanması, gizli bilgilerin korunması ve gizliliğin sağlanması için etkili bir yöntemdir. Parçalama işlemi, belgeleri küçük parçalara ayırarak gerçekleştirilir.

- **Yakma (Incineration):**

Belirli güvenlik standartlarına uygun olarak gerçekleştirilen yakma işlemi, kağıt belgelerin tamamen yok edilmesini sağlar. Ancak, çevresel etkileri nedeniyle dikkatlice ve uygun şekilde yapılmalıdır.

- **Öğütme (Pulping):**

Kağıt belgelerin öğütülerek hamur haline getirilmesi, kağıdın tekrar kullanılmasını engelleyerek güvenli bir imha yöntemi olabilir.

- **Manyetik Medya İmhası:**

Manyetik taşıyıcılar, özellikle eski disketler veya manyetik bantlar gibi, manyetik bir ortamı kullanarak bilgi depolar. Bu tür medyaların özel olarak imha edilmesi gerekebilir.

- **Fiziksel Yıkım:**

Özellikle sabit disk sürücüleri gibi fiziksel medya, parçalama veya delme gibi yöntemlerle fiziksel olarak yok edilebilir.

5.5.2. Dijital Kayıtlar için İmha Yöntemleri:

- **Dijital Silme (Digital Erasure):**

Dijital verilerin üzerine yazılarak veya silinerek imha edilmesi, bilgilerin tekrar kullanılmamasını sağlar. Ancak, bu yöntem, belirli güvenlik standartlarına uygun olarak yapılmalıdır.

- **Fiziksel Medya Yok Etme:**

Dijital verilerin depolandığı fiziksel medyaların (hard disk sürücüleri, USB bellekler) fiziksel olarak imha edilmesi, bilgilerin geri getirilmesini engeller.

- **Fabrika Sıfırlama (Factory Reset):**

Elektronik cihazlar, özellikle mobil cihazlar veya diğer veri depolama cihazları, fabrika sıfırlama işlemi ile bilgileri temizleyebilir. Ancak, bu işlem güvenli bir şekilde yapılmalıdır.

- **Manyetik Silme:**

Manyetik bir ortamı kullanarak bilgileri silme işlemi, manyetik medyaların güvenli bir şekilde imha edilmesini sağlar.

- **Veri Şifreleme Anahtarlarının İmhası:**

Şifrelenmiş verilerin erişimi için kullanılan şifreleme anahtarlarının güvenli bir şekilde imha edilmesi, şifrelenmiş bilgilerin güvenli bir şekilde erişimini engeller.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler re ‘sen (periyodik imha süreleri) veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.1. Kişisel Verilerin Silinmesi

Kişisel veriler Tablo-1’de verilen yöntemlerle silinir.

Tablo 1: Kişisel Verilerin Silinmesi

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
Elektronik Ortamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı saklama ortamlarında tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

6.2. Kişisel Verilerin Yok Edilmesi

Tablo 2 : Kişisel Verilerin Yok edilmesi

Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.
Optik / Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

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 ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

7. VERİ TÜRLERİNE GÖRE SAKLANMA VE İMHA SÜRELERİ

Aşağıdaki tabloda belirtilen verilerin ilgili muhafaza süreleri boyunca muhafaza edilmesinden, departman yöneticileri sorumludur.

Departman yöneticileri uygun olarak imhaların gerçekleştirilmesinden ve muhafaza süresi dolan kişisel verilerin imhasına ilişkin gerekli hatırlatmaları yapmak bakımından görevli ve yetkilidir.

Tablo 3 : Kişisel Veri Saklama ve İmha Süreleri

VERİ TÜRÜ	MUHAFAZA SÜRESİ	İMHA SÜRESİ
E-postalar ve şirket içi yazışmalar	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Sözleşmeler	Sözleşmenin sona ermesini takip eden 10 yıl boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri Kayıtları	Müşteri ile girilen son etkileşimi takip eden 10 yıl boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çerezler ve Log Kayıtları	6 ay en fazla 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çağrı merkezi Ses Kayıtları	3 yıl	
Çalışan Kayıtları	Çalıştıkları süre boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Eski Çalışan Kayıtları	İşten ayrılmalarını takip eden 10 yıl boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Adaylarına İlişkin Kayıtlar	Başvuruyu takip eden 2 yıl boyunca	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Memnuniyet Anketlerine İlişkin Veriler	Anketin doldurulduğu yılın sona ermesine müteakiben 1 Yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe ve Finans Kayıtları	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Şirket İçi Şikayetler ve İlgili Belgeler	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Hukuk Kayıtları	10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

Resmi Yazışmalar	Süresiz	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Satınalma Kayıtları	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Vergi Kayıtları	5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	30 gün	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi Kayıtları	2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

8. İLGİLİ DOKÜMANLAR

- PR-006 Taşınır Kayıt Prosedürü
- LST-003 Veri İmha Listesi
- LST-004 İmha Edilen Kayıt Listesi
- RPR-002 Medya İmha Raporu

9. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	23.08.2023	İlk yayın.
001	10.02.2025	Kişisel veri imha yöntemi eklenerek imha yöntemleri uygulamaları genişletilmiştir.