1. AMAÇ

Bu prosedürün amacı, kullanımdan kalkan bilgi işlem cihazları ve veri depolama ortamları üzerindeki bilgilerin güvenli şekilde silinmesini ve imha edilmesini sağlamak; söz konusu süreçlerin Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) kapsamında iç kontrol, yönetişim ve denetim ilkelerine uygun olarak yürütülmesini temin etmektir.

2. KAPSAM

Bu prosedür, Kurum bünyesinde kullanılan ve kullanım dışı bırakılan tüm bilgi işlem cihazları ile veri depolama ortamlarını kapsar;

- Masaüstü bilgisayarlar ve dizüstü bilgisayarlar,
- Sunucular, depolama üniteleri (NAS, SAN vb.),
- Sabit diskler (HDD), SSD'ler, NVMe diskler,
- Taşınabilir bellekler (USB bellek, harici diskler),
- Mobil cihazlar (akıllı telefon, tablet),
- Yazıcı, fotokopi ve çok fonksiyonlu cihazların depolama birimleri,
- Ağ cihazları (modem, router, firewall vb.) üzerinde depolanan yapılandırma ve log verileri.

Prosedür, söz konusu varlıkların bilgi güvenliği, finansal raporlama, yatırımcı hakları ve piyasa güveni üzerindeki etkileri dikkate alınarak uygulanır.

3. DAYANAK VE REFERANSLAR

Bu prosedür hazırlanırken aşağıdaki mevzuat ve iyi uygulama rehberleri dikkate alınmıştır;

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve ikincil mevzuat,
Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10),
Kurumun Bilgi Güvenliği Politikası ve Varlık Yönetimi Politikası,
NIST Special Publication 800-88 Rev.1 – Guidelines for Media Sanitization.

4. TANIMLAR

Güvenli Silme: Cihaz üzerindeki verilerin, yazılım veya donanım tabanlı yöntemlerle geri getirilemeyecek şekilde silinmesi.

Fiziksel İmha: Cihazın veya depolama ortamının kırma, delme, eritme vb. yöntemlerle fiziksel olarak kullanılamaz hale getirilmesi.

Kullanımdan Kalkan Cihaz: Envanterden çıkarılan, arızalandığı için yenisi ile değiştirilen, kiralama süresi biten, hurdaya ayrılan veya bağışlanacak cihazlar.

İmha Tutanağı: Güvenli silme ve/veya fiziksel imha işlemlerinin yapıldığını gösteren, ilgili taraflarca imzalanan resmi kayıt.

5. SORUMLULUKLAR

5.1. Bilgi İşlem / BT Birimi

Cihazın envanterden düşülmesi, güvenli silme ve imha işlemlerinin teknik olarak gerçekleştirilmesinden sorumludur. Silme/imha işlemi sonrası tutanakları hazırlar, ilgili kayıtları arşivler.

5.2. Birim Yöneticileri

Birimlerinde kullanımdan kalkan cihazları BT birimine zamanında bildirir. Cihaz üzerinde iş birimine ait özel yazılımlar veya veriler varsa BT ile koordineli şekilde aktarımını sağlar.

5.3. Bilgi Güvenliği Sorumlusu / KVKK Temsilcisi

Bu prosedürün Sermaye Piyasası Kurulu Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) ile uyumunu gözetir, uygulamanın etkinliğini izler ve tespit edilen önemli uygunsuzlukları üst yönetime raporlar.

5.4. Satın alma / Lojistik / Demirbaş Birimi

6. PROSEDÜRÜN GENEL İLKELERİ

Kullanımdan kaldırılan hiçbir cihaz, üzerindeki veriler silinmeden üçüncü kişilere teslim edilmez, bağışlanmaz veya satılmaz.

Cihaz üzerinde kişisel veri veya kurumsal gizli bilgi bulunma ihtimali varsa, güvenli silme veya fiziksel imha zorunludur.

Silme ve imha süreçleri mutlaka kayıt altına alınır ve ilgili İmha Tutanağı kurum politika ve mevzuatına uygun süre boyunca saklanır.

Güvenli silme veya fiziksel imha yönteminin belirlenmesinde, cihazın barındırdığı bilgi varlığının güvenlik sınıfı, kritikliği ve risk seviyesi dikkate alınır; yüksek ve kritik risk seviyesine sahip bilgi varlıklarını içeren cihazlarda daha güçlü silme veya fiziksel imha yöntemleri tercih edilir.

7. SÜREÇ ADIMLARI

7.1. Cihazın Kullanımdan Kalkmasının Tespiti

Kullanıcı veya ilgili birim, cihazın arızalandığını, güncelliğini yitirdiğini, sözleşme/kiralama süresinin bittiğini veya yeni cihaz ile değiştirildiğini tespit ettiğinde BT birimine yazılı veya elektronik bildirimde bulunur. BT birimi, cihazı envanter kayıtlarından ve ilgili kullanıcı hesabı/zimmet bilgilerinden kontrol eder. Cihaza ait envanter numarası, kullanıcı bilgisi, cihaz türü ve durumu kayıt altına alınır.

7.2. Veri Yedekleme ve Aktarım

Cihaz üzerinde iş sürekliliği açısından gerekli olabilecek veriler varsa, ilgili birim yöneticisi onayıyla kurumsal dosya sunucusu, yedekleme sistemi veya yeni cihaz üzerine güvenli bir şekilde aktarılır.

Yedekleme/aktarım tamamlandıktan sonra, eski cihaz üzerinde veri kalmaması için sonraki adımlara geçilir.

7.3. Güvenli Silme Yöntemleri

7.3.1. Manyetik Diskler (HDD)

Mümkünse disk öncelikle tam disk şifreleme kullanılarak şifrelenmişse, şifreleme anahtarlarının güvenli biçimde yok edilmesi gerçekleştirilir. Ardından, yazılımsal güvenli silme aracı ile disk üzerine en az bir kez rastgele veri yazımı (overwrite) yapılır. Kullanılacak yazılımlar lisanslı ve kurumsal olarak onaylanmış olmalıdır. Silme işlemine ait log/rapor dosyası alınarak imha dosyasına eklenir.

7.3.2. SSD, NVMe, Flash Bellekler

SSD ve flash belleklerde klasik overwrite yöntemleri her zaman güvenilir sonuç vermeyebileceğinden, öncelikle üretici tarafından sağlanan "Secure Erase/Sanitize" komutları veya disk self-encrypting drive (SED) ise kriptografik erase (şifreleme anahtarının yok edilmesi) yöntemleri tercih edilir.

Bu yöntemlerin uygulanamadığı veya başarısız olduğu durumlarda, cihaz fiziksel imhaya yönlendirilir (bkz. 7.4).

7.3.3. Mobil Cihazlar (Telefon, Tablet)

Cihaz üzerindeki kurumsal e-posta hesapları, MDM (Mobil Cihaz Yönetimi) profilleri, uygulama ve belgeler MDM sistemi üzerinden veya cihazın ayarları aracılığıyla uzaktan ya da yerinden silinir. Cihaz fabrika ayarlarına döndürülür (factory reset). Mümkünse, cihaz depolaması şifrelenmiş olarak kullanılıyorsa, şifreleme anahtarlarının yok edildiği teyit edilir. İşlem sonrası MDM/kurumsal platform üzerinde cihazın kaydı kaldırılır.

7.3.4. Yazıcı, MFP, Fotokopi, Ağ Cihazları

Cihazın yönetim arayüzü (web arayüzü, konsol vb.) üzerinden disk/hafıza temizleme, log temizleme ve konfigürasyon sıfırlama (factory reset) işlemleri yapılır. Varsa takılı sabit disk/SSD çıkarılır ve 7.3.1, 7.3.2 veya 7.4'e göre işlem görür.

7.4. Fiziksel İmha Yöntemleri

Aşağıdaki durumlarda fiziksel imha zorunludur:

Cihaz üzerinde çok yüksek hassasiyetli veri bulunduğu biliniyor ve geri döndürülemez silmeden emin olunamıyorsa,

Cihaz arızalı olduğundan yazılımsal silme mümkün değilse,

Üretici secure erase desteklemiyorsa,

Kurumun bilgi güvenliği politikası özel olarak fiziksel imha öngörüyorsa.

Fiziksel imha yöntemleri:

Disk/Depolama Üzerinde Delme ve Parçalama: Disk plakalarının veya SSD yongalarının fiziksel olarak kırılması, delinmesi suretiyle okunamaz hale getirilmesi.

Sanayi Tipi Parçalayıcı (Shredder) Kullanımı: Kurumsal imkan varsa, diskler ve depolama ortamları metal/plastik parçalama makinelerinde küçük parçalara ayrılır.

Lisanslı İmha Firmasına Teslim: Kurumda imha imkanı yoksa, çevre mevzuatına uygun, yetkili ve lisanslı firmalar aracılığıyla gerçekleştirilir. İmha hizmeti alınan üçüncü taraf firmaların, Sermaye Piyasası Kurulu düzenlemelerine, bilgi gizliliği yükümlülüklerine ve denetim gerekliliklerine uygun faaliyet göstereceğine ilişkin yazılı taahhüt alınır. Üçüncü taraf imha süreçleri Kurum tarafından izlenir ve kayıt altına alınır. Firmadan imha sertifikası/raporu alınır ve ilgili tutanağa eklenir.

7.5. İmha Tutanağı ve Kayıt

Her güvenli silme veya fiziki imha işlemi için aşağıdaki bilgileri içeren bir "Güvenli Silme ve İmha Tutanağı" düzenlenir:

Cihaz türü (PC, sunucu, disk, telefon vb.),

Marka, model, seri numarası, envanter numarası,

Eski kullanıcı/zimmet bilgisi,

Uygulanan işlem türü (güvenli silme, secure erase/kriptografik erase, fiziksel imha),

İşlem tarihi ve yeri,

İşlemi yapan BT personeli adı-soyadı, imzası,

Gözlemci/ikinci kontrol (varsa Bilgi Güvenliği veya birim yetkilisi) imzası,

İmha firması kullanıldıysa, firmanın adı, yetkili imzası, imha sertifikası numarası.

Bu tutanak ve ilgili log, rapor ve sertifikalar, elektronik belge yönetim sistemi veya ilgili birim dosyalarında asgari 5 yıl süreyle saklanır ve yetkisiz erişime karşı korunur.

8. GÜVENLİK VE DENETİM

Silme ve imha işlemleri, görevler ayrılığı ilkesine uygun olarak en az iki kişi gözetiminde gerçekleştirilir (işlemi yapan BT personeli ve gözlemci).
Belirli periyotlarla (örneğin yılda bir) Bilgi Güvenliği veya İç Denetim birimi tarafından rastgele seçilen imha kayıtları kontrol edilir ve prosedüre uygunluk denetlenir.

Uygunsuzluk tespit edilirse, düzeltici/önleyici faaliyetler başlatılır ve gerekirse ilgili personele tekrar eğitim verilir.

9. ÇEVRE VE ATIK YÖNETİMİ

Fiziksel imha sırasında ortaya çıkan elektronik atıklar, çevre mevzuatına uygun şekilde bertaraf edilir.
Mümkün olan cihazlar, veri silme sonrası (yasal ve güvenlik şartları karşılanıyorsa) bağış, geri dönüşüm veya tekrar kullanım amacıyla değerlendirilebilir. Elektronik atıkların lisanslı geri dönüşüm/bertaraf firmalarına teslim edildiğine dair evraklar saklanır.

10. YÜRÜRLÜLÜK VE GÖZDEN GEÇİRME

Bu prosedür, üst yönetim onayı ile yürürlüğe girer. Prosedürün uygulanması ve etkinliğinin gözetimi üst yönetimin sorumluluğundadır. Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) ve ilgili mevzuatta meydana gelebilecek değişiklikler dikkate alınarak en az yılda bir kez gözden geçirilir ve gerekli güncellemeler yapılır.