SEFİNE BİLGİ SİLME POLİTİKASI

Bu politikanın amacı, kuruluş bünyesinde bulunan bilgi varlıklarının kullanım ömrü sonunda, güvenli ve geri getirilemeyecek şekilde silinmesini sağlamak; yetkisiz erişim ve veri sızıntısı risklerini önlemektir. TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve Siber Hijyen farkındalığına rehberlik etmektir.

Bu politika; tüm çalışanları, danışmanları ve üçüncü tarafları, elektronik ve fiziksel tüm bilgi varlıklarını, sunucular, kullanıcı cihazları, taşınabilir medya ve bulut ortamlarını kapsar.

Silme Prensipleri

-Veriler yalnızca ihtiyaç duyulduğu süre boyunca saklanır.

-Saklama süresi dolan veriler silinmelidir.

-Silme işlemleri doğrulanabilir ve kayıt altına alınabilir olmalıdır.

- “BGYS Varlık Yönetimi Prosedürü- SFN-BGP-06” uyarınca veri sınıflandırmasına uygun yöntemler kullanılmalıdır.

Silme Yöntemleri

Elektronik Veriler

-Güvenli silme (secure erase)

-Üzerine yazma (overwrite)

-Kriptografik silme (encryption key destruction) yöntemlerinden uygun olanları kullanılır.

Fiziksel Medya

-Parçalama (shredding)

-Manyetik yok etme (degaussing)

-Fiziksel imha (kırma vb.) yöntemlerinden uygun olanları kullanılır.

Veri Sınıfına Göre Silme

-“BGYS Varlık Yönetimi Prosedürü - SFN-BGP-06” uyarınca veri sınıfına uygun silme yöntemi tercih edilmelidir.

Genel Müdür

SEFİNE

SEFİNE BİLGİ SİLME POLİTİKASI

Saklama Süreleri

-Veri saklama süreleri yasal ve iş gereksinimlerine göre belirlenir.

-Süresi dolan veriler otomatik veya manuel olarak silinmelidir.

Yedeklerden Silme

-Silinen veriler yedeklerden de uygun sürede kaldırılmalıdır.
-Yedeklerdeki veriler saklama süresi dolana kadar korunur.
-Geri yükleme süreçlerinde silinmiş verilerin tekrar aktif ortama alınmaması sağlanır.

Bulut Ortamlarından Silme

-Silme işlemlerinin bulut tedarikçisi tarafından sözleşmeye uygun olarak gerçekleştiği teyit edilmelidir.

Loglama ve Kayıt

-Silme işlemleri kayıt altına alınmalıdır.

Doğrulama ve Test

-Silme işlemleri gerekli hallerde doğrulanmalıdır.

Üçüncü Taraflar

-Üçüncü tarafların veri silme yükümlülükleri sözleşmelerde tanımlanmalıdır.
-Hizmet sonlandırıldığında verilerin silindiği teyit edilmelidir.

Olay Yönetimi

-Yanlışlıkla veri silinmesi durumunda olay yönetim süreci başlatılır.

-Veri kurtarma (varsa) kontrollü şekilde yapılır.

Genel Müdür

SEFİNE BİLGİ SİLME POLİTİKASI

Denetim ve Uyum

-Silme süreçleri düzenli olarak denetlenir.

-Uygunsuzluklar için düzeltici faaliyetler uygulanır.

İhlal Bildirimi

-Bilgi güvenliği ihlali ya da şüphesi durumunda kullanıcılar derhal “Bilgi Güvenliği İhlal Olaylarını Kayıt Altına Alma Talimatı-SFN-DB-BT-T-017” uyarınca hareket etmelidir.

-Geç bildirimde bulunmak veya gizlemek disiplin süreci başlatabilir.

Yaptırımlar

-Bu politikanın ihlali durumunda; Disiplin işlemleri, Erişim kısıtlamaları, Sözleşme feshi,

-Gerekli durumlarda hukuki işlem uygulama hakkını Sefine kendinde saklı tutmaktadır.

6698 Sayılı Kişisel Verilerin Korunması Kanunu

- Veri toplama, veri sınıflandırma, veri etiketleme, veri işleme, veri transferi, saklama süreleri, sefine silme prensipleri, silme yöntemleri, yedekden silme, bulut ortamından silme, log ve kayıt işlemleri esnasında 16.a Kişisel Verileri Saklama ve İmha Prosedürü-SFN-KVKK-03 uyarınca hareket edilir.

İklim Değişikliği

TS EN ISO/IEC -A1 İklim Değişikliği uyarınca iklim değişikliğinin bilgilerin ve diğer ilişkili varlıklarına etkisi proaktif yaklaşılarak göz önüne alınmaktadır.

Genel Müdür