SEFİNE YEDEKLEME POLİTİKASI

Bu politikanın amacı, kuruluşun sahip olduğu bilgi varlıklarının veri kaybına karşı korunması, iş sürekliliğinin sağlanması ve veri bütünlüğünün temin edilmesi için yedekleme süreçlerinin esaslarını belirlemektir. TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve Siber Hijyen farkındalığına rehberlik etmektir.

Bu politika; Tüm bilgi sistemlerini, sunucuları, veri tabanlarını ve uygulamaları, son kullanıcı cihazlarını (kritik veriler için), bulut ortamlarını, tüm çalışanları ve ilgili üçüncü tarafları kapsar.

Yedekleme Prensipleri

-Veriler düzenli olarak yedeklenmelidir.

-Yedekler “Sefine Veri Sınıflandırma Etiketleme Politikası-SFN-PT-24” uygun olarak belirlenen veri sınıfı uyarınca korunmalıdır.

-Yedekleme süreçleri otomatikleştirilmelidir.

-Yedekler yetkisiz erişime karşı korunmalıdır.

Yedekleme Sıklığı

-Tam Yedekleme (Full Backup),

-Artımlı Yedekleme (Incremental Backup),

-Fark Yedekleme (Differential Backup) olacak şekilde yedekleme türü, sistem kritikliğine göre belirlenir.

Yedekleme Türleri

-Tam Yedekleme (Full Backup),

-Artımlı Yedekleme (Incremental Backup),

-Fark Yedekleme (Differential Backup) olacak şekilde yedekleme türü, sistem kritikliğine göre belirlenir.

Genel Müdür

SEFİNE YEDEKLEME POLİTİKASI

Yedekleme Ortamları

-Yedeklenen veriler farklı lokasyonlarda tutulmalıdır.

Yedeklerin Saklanması

-“Sefine Çevresel Fiziksel Güvenlik Politikası-SFN-PT-26” uyarınca çevresel ve fiziksel güvenlik önlemleri uygulanır.

Şifreleme ve Güvenlik

-Yedekler şifrelenmelidir.

-“Sefine Bilgi Transferi Politikası-SFN-PT-21” uyarınca veri transferi sırasında güvenli protokoller kullanılmalıdır.

-Kriptografik anahtar yönetimi güvenli şekilde yapılmalıdır.

Erişim Kontrolü

-Yedeklere erişim yetkilendirilmiş kişilerle sınırlandırılır.

-“Sefine Erişim Kontrolü Politikası-SFN-PT-27” uyarınca erişimler kayıt altına alınır ve izlenir.

Geri Yükleme (Restore) Testleri

-Yedeklerin geri yüklene bilirliği düzenli olarak test edilir.

-Test sonuçları kayıt altına alınır.

Olay Yönetimi

-Veri kaybı durumunda geri yükleme süreci başlatılır.

-Olaylar kayıt altına alınır ve analiz edilir.

Genel Müdür

SEFİNE YEDEKLEME POLİTİKASI

İzleme ve Loglama

-Yedekleme işlemleri loglanır.

-Başarısız yedekleme işlemleri raporlanır.

-Loglar düzenli olarak gözden geçirilir.

Her Çalışanın Sorumluluğu

-Yedekleme sadece Bilgi Teknolojileri' nin işi değildir. Her çalışan kendi elektronik varlıklarının farkında olmalı, hassas bilgileri Sefine'nin ortak güvenlik havuzuna dahil etmelidir.

Uyum

-Uygunsuzluklar için düzeltici faaliyetler başlatılır.

İhlal Bildirimi

-Yedekleme hataları ve yanlış silme işlemleri raporlanır.

-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.

-Güvenlik ihlalleri için müdahale süreçleri uygulanır

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

SEFİNE YEDEKLEME POLİTİKASI

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, yedekleme prensipleri, yedekleme sıklığı, yedekleme türleri, yedekleme ortamları, yedeklerin saklanması, geri yükleme testleri, erişim ve kontrolü, şifreleme ve güvenlik, 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.

Genel Müdür