SEFİNE BULUT HİZMETLERİ POLİTİKASI

Bu politikanın amacı, kuruluş tarafından kullanılan bulut hizmetlerinin güvenli, kontrollü ve mevzuata uygun şekilde kullanılmasını sağlamak; bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumaktır. TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve Siber Hijyen farkındalığına rehberlik etmektir.

Bu politika; tüm çalışanları, danışmanları ve üçüncü tarafları, tüm bulut hizmet modellerini, kurum tarafından kullanılan veya kullanılması planlanan tüm bulut platformlarını kapsar.

Bulut Hizmeti Seçim Kriterleri

-Güvenlik sertifikaları (ISO 27001 vb.).

-Veri merkezi konumu ve veri yerleşimi (data residency).

-Yasal ve düzenleyici uyumluluk.

-Hizmet sürekliliği (SLA).

-Yedekleme ve felaket kurtarma yetenekleri göz önüne alınmalıdır.

Veri Sınıflandırma ve Kullanımı

-Buluta taşınacak veriler “Sefine Veri Sınıflandırma Etiketleme Politikası-SFN-PT-24” sınıflandırılmalıdır.

-Kişisel verilerin işlenmesi mevzuata uygun olmalıdır.

Erişim Kontrolü

-“Sefine Erişim Kontrolü Politikası-SFN-PT-27” uyarınca hareket edilmelidir.

-Kullanıcı erişimleri rol bazlı (RBAC) olmalıdır.

-En az yetki prensibi (Principle of Least Privilege (PoLP)) uygulanmalıdır.

-Çok faktörlü kimlik doğrulama (MFA) zorunlu olmalıdır.

-Ayrıcalıklı hesaplar kontrol altında tutulmalıdır

Genel Müdür

SEFİNE

SEFİNE BULUT HİZMETLERİ POLİTİKASI

Kimlik ve Erişim Yönetimi

-“Erişim Kontrolü Politikası” uyarınca hareket edilmelidir.

-Merkezi kimlik yönetimi (IAM) kullanılmalıdır.

-Hesap açma, değiştirme ve kapatma süreçleri tanımlı olmalıdır.

-Yetkisiz erişim girişimleri izlenmelidir.

Kriptografik Kontroller

-“Kriptografik Kontroller Talimatı-SFN-DB-BT-T-008” uyarınca kriptografi kullanımında veri şifreleme gereksinimleri, sertifika kullanımı ve anahtar yönetimi prensiplerine dikkat edilmelidir.

İzleme ve Loglama

-İşlemler loglanır.

-Başarısız yedekleme işlemleri raporlanır.

-Loglar düzenli olarak gözden geçirilir.

Kullancı Sorumluluğu

-Kullanıcılar, veri yedeklemelerini yalnızca Sefine tarafından yetkilendirilmiş bulut servisleri üzerinden gerçekleştirmelidirler.

-Dış paylaşımlar sadece iş gerekçesiyle ve süre sınırı belirlenerek yapılmalıdır.

-Tüm paylaşımlar “Sefine Bilgi Transferi Politikasına- SFN-PT-21” uygun olmalıdır.

Tedarikçi ve Sözleşme Yönetimi

-Bulut sağlayıcı ile sözleşme yapılmalıdır.

Genel Müdür

SEFİNE BULUT HİZMETLERİ POLİTİKASI

Uyum ve Yasal Gereklilikler

-KVKK ve ilgili veri koruma mevzuatına uyum sağlanmalıdır.

-Veri transferleri yasal gerekliliklere uygun olmalıdır.

Olay Yönetimi

-Yetkisiz ve uygun olmayan bulut faaliyet girişimleri 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

İş Sürekliliği

-Bulut hizmet kesintilerine karşı proaktif önlemler alınmalıdır.

Yasaklı Kullanımlar

-Hassas verilerin kontrolsüz ortamlara yüklenmesi yasaktır.

-Kurum politikalarına aykırı veri paylaşımı yasaktır.

6698 Sayılı Kişisel Verilerin Korunması Kanunu

- Bulut hizmeti seçim kriterleri, veri toplama, veri sınıflandırma, veri etiketleme, erişim kontrolü, kimlik ve erişim yönetimi, veri işleme, kriptografik kontroller, 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