SEFİNE DEPOLAMA ORTAMI POLİTİKASI

Bu politikanın amacı, Sefine'nin bilgi varlıklarının fiziksel ve dijital ortamlarda güvenli şekilde depolanmasını sağlamak, yetkisiz erişim, değişiklik, kayıp ve sızıntı risklerini azaltmaktır. TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve Siber Hijyen farkındalığına rehberlik etmektir.

Depolama Ortamlarının Sınıflandırılması

-Tüm bilgi varlıkları gizlilik seviyelerine göre sınıflandırılmalı ve buna uygun depolama ortamlarında saklanmalıdır.

-Hassas Veriler "C2" (Hassas Sınırlı) ve "C3" (Ticari Gizli) bilgiler sadece güvenli depolama alanlarında ve yetkilendirilmiş kullanıcılar tarafından erişilebilir şekilde saklanmalıdır.

Erişim Kontrolleri

-Depolama ortamlarına erişim, "Yetki Matris"i çerçevesinde sınırlandırılmalıdır.

-Yetkisiz erişimler önlenmeli, erişim log'ları izlenmeli ve düzenli olarak denetlenmelidir.

Şifreleme ve Koruma

-Harici ortamlarda (örn: USB bellek, harici disk) saklanan hassas bilgiler uygun şifreleme algoritmalarıyla korunmalıdır.

-Bulut hizmetleri kullanılıyorsa, veri hem aktarım sırasında hem de depolama sırasında şifrelenmelidir.

Fiziksel Güvenlik

-Fiziksel sunucular ve diğer depolama cihazları, yetkisiz girişe kapalı, güvenlik kameraları ve giriş kontrol sistemleri ile korunan alanlarda saklanmalıdır.

Taşınabilir Ortamların Kullanımı

-Taşınabilir ortamlarda hassas bilgi saklanması zorunlu ise cihaz şifreleme ve parola koruması uygulanmalıdır.

-Kullanımı izne tabi olmalı, kim tarafından ne amaçla kullanıldığı kayıt altına alınmalıdır.

Genel Müdür

Sefine Depolama Ortamı Politikası

Yedekleme ve Kurtarma

-Bilgiler, belirlenmiş yedekleme planına göre düzenli olarak yedeklenmelidir.

-Yedekler şifreli olarak tutulmalı, farklı fiziksel konumlarda saklanmalı ve kurtarma planları dahilinde kurtarma testleri yapılmalıdır.

Depolama Ortamlarının İmhası

-Kullanım dışı kalan veya ömrünü tamamlayan depolama cihazları, ilgili bilgi silme politikasına göre geri döndürülemez şekilde yok edilmelidir.

-İmha işlemi kayıt altına alınmalı ve sorumlu kişi tarafından onaylanmalıdır.

Uygunsuz Davranışlar ve Yaptırımlar

Bu politikaya aykırı davranışlar, bilgi güvenliği ihlali sayılacak olup Sefine disiplin yönetmeliği ve ilgili yasal düzenlemelere göre işlem yapılmasına neden olabilir.

İzleme Faaliyetleri

Şüpheli trafik ve erişim denemeleri izlenmektedir.

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