SEFİNE ERİŞİM KONTROLÜ POLİTİKASI

Bu politikanın amacı, kuruluşun bilgi varlıklarına erişimin yetkilendirilmiş kişilerle sınırlandırılması, yetkisiz erişimlerin engellenmesi ve bilgi güvenliğinin sağlanması için gerekli kuralları belirlemektir. TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve Siber Hijyen farkındalığına rehberlik etmektir.

Bu politika; tüm çalışanları, danışmanları ve tüm üçüncü tarafları, tüm bilgi sistemlerini,

uygulamaları ve ağları, fiziksel ve mantıksal erişim süreçlerini kapsar.

Erişim Kontrolü Prensibleri

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

-Görevler ayrılığı (Segregation of Duties) sağlanır.

-İhtiyaç kadar erişim (Need-to-Know) uygulanır.

-Varsayılan olarak erişim reddedilir (Default Deny).

Kullanıcı Kimlik Yönetimi

-Her kullanıcıya benzersiz kullanıcı hesabı atanır.

-Ortak hesap kullanımı sınırlandırılır ve kontrol altında tutulur.

-Kullanıcı hesapları yaşam döngüsüne göre yönetilir (oluşturma, değiştirme, kapatma).

-Yeni kullanıcı oluşturma, yetki verme, kaldırma ve değişiklik işlemleri sadece Bilgi Teknolojileri onayıyla yapılmalıdır.

-Kullanıcı hesapları belirli süre kullanılmazsa otomatik olarak askıya alınmalıdır.

Genel Müdür

SEFİNE

SEFİNE ERİŞİM KONTROLÜ POLİTİKASI

Kimlik Doğrulama Kuralları

-Güçlü parola politikası uygulanır.

-Çok faktörlü kimlik doğrulama gerekli hallerde (MFA) kullanılır.

-Parola paylaşımı yasaktır.

-Varsayılan şifreler değiştirilmelidir.

Yetkilendirme ve Erişim Hakları

-Rol tabanlı erişim kontrolü (RBAC) uygulanır.

-Erişim talepleri onay sürecine tabidir.

-Erişim hakları düzenli olarak gözden geçirilir.

Ayrıcalıklı Erişim Yönetimi

-Yönetici (admin) hesapları kontrol altında tutulur.

-Ayrıcalıklı erişimler kayıt altına alınır.

-Ayrıcalıklı işlemler izlenir ve loglanır.

Ağ ve Sistem Erişimi

-Sistemlere erişim güvenli protokoller üzerinden sağlanır.

-Uzaktan erişimlerde VPN kullanımı zorunludur.

-Yetkisiz erişim girişimleri izlenir.

Genel Müdür

SEFiNE

SEFİNE ERİŞİM KONTROLÜ POLİTİKASI

Uygulama ve Erişimi

-Uygulama erişimleri rol bazlı olmalıdır.

-Hassas verilere erişim sınırlandırılmalıdır.

-Veri erişimleri loglanmalıdır.

Fiziksel Erişim Kontrolü

-Kritik alanlara erişim sınırlandırılır.

Erişim Gözden Geçirme

-Kullanıcı erişimleri periyodik olarak gözden geçirilir.

-Gereksiz erişimler kaldırılır.

Oturum Yönetimi

-Oturum zaman aşımı uygulanır.

-Kullanılmayan oturumlar otomatik olarak sonlandırılır.

-Ekran kilidi zorunludur.

Loglama ve İzleme

-Erişim faaliyetleri loglanır.

-Loglar düzenli olarak analiz edilir.

Genel Müdür

SEFİNE ERİŞİM KONTROLÜ POLİTİKASI

Olay Yönetimi

-Yetkisiz erişim 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

Üçüncü Taraf Erişimleri

-Üçüncü taraf erişimleri sınırlandırılır.

-Sözleşmelerle güvence altına alınır.

-Erişimler süreli ve kontrollü verilir.

Denetim ve Uyum

-Erişim kontrolleri düzenli olarak denetlenir.

-Uygunsuzluklar için düzeltici faaliyetler başlatılır.

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

Erişim kontrolü prensibleri, kullanıcı kimlik yönetimi, kullanıcı kimlik doğrulama, yetkilendirme ve erişim hakları, ayrıcalıklı erişim yönetimi, ağ ve sistem erişimi, uygulama ve erişimi, fiziksel erişim kontrolü, erişim gözden geçirme, oturum yönetimi, loglama ve izleme işlemleri Kişisel Verilerin İşlenmesi ve Korunması Prosedürü -SFN-KVKK-02 uyarınca gerçekleştirilmektedir.

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