SEFİNE KULLANICI UÇ NOKTA CİHAZLARI POLİTİKASI

Bu politikanın amacı, kuruluş bilgi varlıklarına erişim sağlayan uç nokta cihazlarının güvenliğinin sağlanması, yetkisiz erişimlerin önlenmesi ve bilgi güvenliği risklerinin azaltılmasıdır. TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve Siber Hijyen farkındalığına rehberlik etmektir.

Bu politika; çalışanlar, yükleniciler, tedarikçiler ve ilgili taraflar tarafından kullanılan tüm masaüstü bilgisayarlar, dizüstü bilgisayarlar, tablet, mobil cihazlar ve diğer uç nokta cihazlarını kapsar.

Genel Güvenlik

-Tüm uç nokta cihazları kurumsal güvenlik standartlarına uygun yapılandırılır.

-Cihazlarda yalnızca yetkilendirilmiş kullanıcılar işlem yapabilir.

-En az ayrıcalık (Least Privilege) prensibi uygulanır.

-Tüm uç nokta cihazlar yalnızca yetkili çalışana zimmetlenir, etiketlenir, sınıflandırılır ve kişisel amaçla kullanımı sınırlandırılır.

-Sefine bünyesinde kullanılan uç nokta cihazları güvenli, verimli ve Sefine standartlarına uygun şekilde kullanılmalıdır.

-“Sefine Yedekleme Politikası-SFN-PT-22” uyarınca dijital varlıkların gizlilik, bütünlük, erişilebilirliğinden emin olunması için dosya sunucusunda (ortak alanda) çalışılmalıdır.

- Uç nokta cihazlarında “BGYS Varlık Yönetimi Prosedürü-SFN-BGP-06” uyarınca veri sınıflandırma ve veri depolama kurallarına uygun hareket edilmelidir.

Kimlik Doğrulama ve Erişim

-“Sefine Erişim Kontrolü Poitikası-SFN-PT-27” uyarınca kimlik doğrulama, erişim işlemleri, kullanıcı hesapları yönetilmeli ve yetkilendirilmelidir.

-Güçlü parola politikaları uygulanır.

-Çok faktörlü kimlik doğrulama (MFA) mümkün olan sistemlerde zorunludur.

-Oturum kilitleme ve zaman aşımı ayarları uygulanır.

Genel Müdür

SEFİNE KULLANICI UÇ NOKTA CİHAZLARI POLİTİKASI

Yazılım ve Güncelleme Yönetimi

-Tüm cihazlarda lisanslı ve onaylı yazılımlar kullanılır.

-Güvenlik yamaları ve güncellemeler düzenli olarak uygulanır.

-Uç nokta cihazlarına yetkisiz yazılım kurulumu yasaktır, gerekli görülen yazılım kurulumları iş ihtiyaçları da belirtilerek Bilgi Teknolojilerine bildirilmelidir. “Fikri Mülkiyet Hakları Politikası-SFN-PT-28” uyarınca lisanslı yazılım kullanıldığından emin olunmalıdır.

Zararlı Yazımlara Karşı Koruma

-Antivirüs çözümleri kurulu ve güncel tutulur.

-Gerçek zamanlı koruma aktif olmalıdır.

Veri Koruma

-Taşınabilir medya kullanımı sınırlandırılır ve kontrol altına alınır.

-Veri kaybı önleme (DLP) kontrolleri uygulanır.

-USB ve harici bellek kullanımında dikkatli olunmalı, yalnızca taranmış ve güvenli medyalar kullanılmalıdır.

Fiziksel Güvenlik

-Cihazlar yetkisiz erişime karşı korunur.

- Uç nokta cihazları fiziksel olarak korunmalı, kilitli dolapta saklanmalı veya gözetimsiz bırakılmamalıdır. Bu konuda Sefine ilgili tarafları “Sefine Çevresel Fiziksel Güvenlik Politikası-SFN-PT-26”, “Sefine Bilgilerin ve Diğer İlişkili Varlıkların Kabul Edilebilir Kullanım Politikası-SFN-PT-19” ve “Sefine Temiz Masa Temiz Ekran politikasına-SFN-PT-25” uygun hareket etmelidir.

-Ofis dışı kullanımda cihazların güvenliği ayrıca sağlanır.

-Kayıp/çalıntı durumları derhal bildirilir.

Genel Müdür

SEFİNE KULLANICI UÇ NOKTA CİHAZLARI POLİTİKASI

Ağ Güvenliği

-Güvenli ağlar kullanılmalı, uzaktan erişimde VPN zorunlu olmalıdır.

-Uç noktalar ağa bağlanmadan önce güvenlik kontrollerinden geçmelidir.

-Uç nokta cihazları Antivirüs kullanımı, güvenlik yamalarının uygulanması, firewall aktif olması, disk şifreleme, USB ve harici medya kontrolü gerçekleştirilmektedir.

-Sefine ağına bağlanan cihazlar düzenli olarak güncellenmeli ve antivirüs yazılımı bulundurmalıdır. Bu yazılım kaldırılmaya çalışılmamalıdır.

Kriptografik Kontroller

-Kriptografi kullanımında veri şifreleme gereksinimleri, sertifika kullanımı ve anahtar yönetimi prensiplerine dikkat edilmelidir.

İzleme ve Denetim

-Kullanıcı aktiviteleri loglanır, uç nokta cihazları düzenli olarak izlenir ve denetlenir.

-Güvenlik olayları kayıt altına alınır ve analiz edilir.

Sınırlamalar

“Sefine Bilgilerin ve Diğer İlişkili Varlıkların Kabul Edilebilir Kullanım Politikası-SFN-PT-19” uyarınca belirlenen kişisel kullanım sınırları, yasaklı faaliyetler ve Internet / E-posta kullanımları sınırlandırılmıştır.

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 KULLANICI UÇ NOKTA CİHAZLARI POLİTİKASI

İhlal Yönetimi

-Cihaz kaybolduğunda, çalındığında veya şüpheli bir durum yaşandığında derhal Bilgi Teknolojileri / İdari İşler ekibine bildirilmelidir. Herhangi bir güvenlik ihlali durumunda "Bilgi Güvenliği İhlal Olaylarını Kayıt Altına Alma Talimatı-SFN-DB-BT-T-017" uyarınca hareket edilmektedir.

-Bu politikanın ihlali durumunda; disiplin işlemleri, erişim kısıtlamaları, sözleşme feshi,

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

Kullanıcı Sorumlulukları

Bilgi Güvenliği sadece sistemler tarafından oluşturulamaz, sadece Bilgi Teknolojileri ekibinin de görevi değildir. Kullanıcı davranışları da en az sistemler kadar etkilidir.

Genel Müdür