

SEFINE VERİ SINIFLANDIRMA ETİKETLEME POLİTİKASI

Bu politikanın amacı, kuruluşun sahip olduğu bilgi varlıklarının önem derecesine göre sınıflandırılması ve uygun şekilde etiketlenerek korunmasını sağlamak; bilgi güvenliği risklerini azaltmaktır. TS EN ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi ve Siber Hijyen farkındalığına rehberlik etmektedir.

Bu politika; tüm çalışanları, üçüncü tarafları ve danışmanları, tüm bilgi varlıklarını (elektronik veri, fiziksel dokümanlar, sözlü bilgi vb.) ve tüm bilgi işleme ortamlarını kapsar.

Sınıflandırma Prensipleri

- Sınıflandırma; gizlilik, bütünlük ve erişilebilirlik kriterlerine göre yapılır.
- En az yetki prensibi (Principle of Least Privilege (PoLP)) uygulanır.
- Veriler için gereksiz yere yüksek sınıflandırma yapılmamalıdır.
- Veri sınıflandırması düzenli olarak gözden geçirilmelidir.

Veri Sınıfları

Veri Sınıfı	Etiketlenecek mi ?	Etiket İsmi
Tasnif Dışı	Etiketsiz	X
C1 (Dahili Kullanım)	Etiketsiz	X
C2	Etiketli	Hassas Sınırlı
C3	Etiketli	Ticari Gizli

Tasnif Dışı

Kurum dışında serbestçe dağıtılabilen ve bu nedenle özel koruma gerektirmeyen bilgiler. Veri gizli değildir ve genele (Sefine dışına) açılmasında sakınca yoktur. Veri bütünlüğü hayati değildir.

C1 Dahili Kullanım

Sadece Sefine çalışanlarının erişimine açık olan ve Sefine dışına çıkarılması uygun olmayan bilgilerin tamamını içerir.

SEFINE VERİ SINIFLANDIRMA ETİKETLEME POLİTİKASI

C2 Hassas Sınırlı

Bilgi varlığının yalnızca iş sahibi birimler tarafından erişilebilecek olması esastır. Sadece Sefine içi, grup şirketleri, tedarikçiler ve yan sanayi gibi iş ilişkileri çerçevesinde paylaşılan ve bunun haricinde Sefine dışına çıkması onaylanmayan, izinsiz paylaşımı ya da kaybı Sefine organizasyonu için imaj kaybı gibi sonuçlar doğurabilecek uygunsuzluk yaratabilecek bilgilerdir.

C3 Ticari Gizli

Bu gruptaki veriler Sefine içinde gizli bilgilerdir ve dış erişimden korunurlar. Yetkisiz personelce erişilmesi durumu, Sefine' nin operasyonel verimliliğini etkileyebilir. Önemli mali kayıplara neden olabilir. Rakiplere önemli kazançlar sağlayabilir ya da müşteri güveninde ciddi düşüşlere yol açabilir.

Etiketleme Kuralları

-Tüm bilgi varlıkları uygun sınıf etiketi ile işaretlenmelidir.

Elektronik belgelerde;

-Alt bilgi etiketi,

Fiziksel Belgelerde;

-Görünür etiket

Veri Saklama ve Depolama

- Veriler sınıfına uygun ortamlarda saklanmalıdır.
- Hassas veriler şifreli ortamlarda tutulmalıdır.
- Fiziksel dokümanlar kilitli alanlarda saklanmalıdır.

Veri Transferi

- “Sefine Bilgi Transferi Politikası-SFN-PT-21” uyarınca gerçekleştirilmektedir.
- Veri sınıflandırmasına göre transfer yöntemi belirlenir.
- Yetkisiz paylaşım yasaktır.

SEFINE VERİ SINIFLANDIRMA ETİKETLEME POLİTİKASI

Veri İmhası

- Veriler sınıfına uygun şekilde "Sefine Bilgi Silme Politikası-SFN-PT-29" uyarınca imha edilmelidir.
- Fiziksel belgeler parçalanarak (kağıt kıyıcı) yok edilmelidir.
- Elektronik veriler güvenli silme yöntemleri ile silinmelidir.

İzleme ve Denetim

- Veri erişimleri izlenir.
- Etiketleme uyumu denetlenir.
- Uygunsuzluklar raporlanır.

Tedarikçi ve Üçüncü Taraflar

- Paylaşılan verilerde veri sınıfları uyarınca hareket edilmelidir.
- Sözleşmelerde veri koruma hükümleri yer almalıdır.

Tedarikçi ve Üçüncü Taraflar

- Yanlış; veri sınıflandırma, etiketleme ve bunlar uyarınca yanlış olarak gerçekleştirilen depolama ve transfer 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

SEFINE VERİ SINIFLANDIRMA ETİKETLEME 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 prensipleri, veri etiketleme, veri işleme, veri transferi, saklama süreleri, sefine silme prensipleri, silme yöntemleri, yedekten silme, bulut ortamından silme, log ve kayıt işlemleri esnasında 16.a Kişisel Verileri Saklama ve İmha Prosedürü-SFN-KVKK-03 uyarınca hareket edilir.