Varlık Sınıflandırması

Bilgi varlığı; korunma gereksiniminin, önceliklerinin ve derecesinin belirlenmesi için sınıflandırılmaktadır. Bu talimat, Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) ile Kurumun Bilgi Güvenliği Yönetim Sistemi kapsamında uygulanır. Varlık sınıflandırması için kullanılacak standartlar ve prosedürler belgelenmeli ve uygulanmalıdır. Varlık sınıflandırmasında aşağıdaki konular göz önünde bulundurulmaktadır;

- Varlık sınıflandırması ihtiyaç, önem ve koruma için ayrılacak kaynak gereksinimini yansıtmalıdır;
- Bilgi varlıkları değişik önem ve hassasiyet derecesine sahip olabilirler;
- Bazı bilgi varlıkları, ilave korunma seviyesine veya özel olarak ele alınmaya gerek duyabilir;
- Bilgi varlıkları sınıflandırma sistemi, uygun koruma seviyesi tanımlanması için kullanılmalıdır;
- Bilgi varlıklarının zaman içerisinde sınıflandırma derecesi değişebilir;
- Bilgiye ait bir öğenin; örneğin bir belgenin, veri kaydının, veri dosyasının veya taşınabilir ortamın; sınıflandırılmasının, ilgili bilgi varlığı envanteri ile ilişkilendirilmesinin ve bu sınıflandırmanın belirli zamanlarda gözden geçirilmesinin sorumluluğu yaratıcıda veya bilgiye atanmış sahibindedir. Sınıflandırma gözden geçirmeleri, Tebliğ (VII-128.10) kapsamında en az yılda bir yapılır ve sonuçlar kayıt altına alınır.
- Bilgi varlığı aşağıdaki kategorilerde sınıflandırılmıştır. Aşağıdaki sınıflar; bilginin gizlilik, bütünlük ve erişilebilirlik etkileri ile Kurumun finansal raporlama süreçleri, yatırımcıların korunması ve piyasa güveni üzerindeki olası etkileri dikkate alınarak uygulanır:

(a). **Çok Gizli**

İzinsiz olarak açıklanması; Kurumun kritik bilgi sistemlerinin güvenliğini, finansal raporlama süreçlerinin bütünlüğünü, yatırımcı haklarını ve piyasa güvenini ciddi şekilde etkileyebilecek; yüksek düzeyde gizlilik gerektiren bilgi varlıkları "Çok Gizli" olarak nitelendirilir. Bu sınıfa; kritik bilgi sistemlerine ait yapılandırma/erişim bilgileri, ayrıcalıklı hesap bilgileri, zafiyet/penetrasyon test raporları, kritik sistem logları, şifreleme anahtarları, finansal raporlama sistemlerine ilişkin kritik veriler, KVKK kapsamında hassas kişisel veriler ve Kurum açısından ticari sır niteliğindeki en kritik bilgiler dâhildir.

Çok gizli bilgi varlıkları, erişim yetkileri sınırlandırılmış ortamlarda saklanmalı; kopyalama, iletme, paylaşım ve imha işlemleri yazılı/onaylı iş akışı ile yetkilendirilmelidir. Elektronik ortamdaki çok gizli bilgiler için asgari olarak güçlü kimlik doğrulama, erişim kontrolü, şifreleme ve kayıt (log) tutulması sağlanır. Fiziksel ortamda bulunan çok gizli varlıklar kilitli ortamda saklanır ve imha işlemleri kontrollü şekilde gerçekleştirilir. İmha işlemleri kayıt altına alınır ve Tebliğ (VII-128.10) kapsamında en az 5 yıl muhafaza edilir.

(b). **Gizli**

İzinsiz olarak açıklanması veya yetkisiz erişim; Kurumun iş sürekliliğini, operasyonlarını, finansal raporlamasını, yatırımcı iletişimini veya itibarını olumsuz etkileyebilecek bilgi varlıkları "Gizli" olarak nitelendirilir. Bu sınıfa; finansal veriler (raporlama taslakları, mutabakat dosyaları), sözleşmeler, müşteri/tedarikçi bilgileri, iç denetim bulguları, güvenlik olay kayıtları, sistem mimarisi ve teknik belgelendirme gibi bilgiler dâhildir.

Gizli bilgi varlıklarına erişim "bilmesi gereken" prensibi ile sınırlandırılır. Kopyalama, paylaşım, iletme ve imha işlemleri yetki/onay mekanizmasına tabi tutulur. Elektronik ortamda gizli veriler için erişim kontrolü, şifreleme (uygunsa), yedekleme ve loglama uygulanır. Fiziksel ortamda gizli varlıklar güvenli alanlarda saklanır ve imha kontrollü şekilde yapılır. İşlemler kayıt altına alınır ve Tebliğ (VII-128.10) kapsamında en az 5 yıl muhafaza edilir.

(c). **Kuruma Özel**

Kurum dahilinde üretilen; yönergeler, talimatlar, standartlar, prosedürler, politikalar ve Kurum içi işleyişe ilişkin dokümanlar ile bu bilgilerin bulunduğu ortamlar "Kuruma Özel" olarak sınıflandırılır. Bu bilgilerin Kurum dışına çıkarılması, paylaşılması veya üçüncü taraflarla paylaşım yapılması için yetkili yönetici onayı gerekir.

Kurum içinde kullanımında ve kopyalanmasında, ilgili erişim yetkileri ve bilgi güvenliği kurallarına uyulması şartıyla sakınca yoktur. Elektronik ortamdaki Kuruma Özel bilgilerin erişimi rol bazlı yetkilendirme ile kontrol edilir ve gerekli görülen durumlarda loglanır.

(d). **Hizmete Özel**

Sadece belli bir grup tarafından (örneğin proje ekipleri, belirli bir birim veya görevli personel) görülebilecek; diğer yüksek gizlilik sınıflarına girmemekle birlikte yetkisiz erişime karşı korunması gereken bilgi varlıkları "Hizmete Özel" olarak sınıflandırılır. Bu sınıfa; proje dokümanları, iş planları, operasyonel raporlar, çalışma dosyaları ve süreç dokümanları dâhildir.

Hizmete Özel bilgi varlıklarının kopyalanması, iletilmesi, paylaşımı ve imhası yetkilendirme kurallarına tabidir. Kurum dışına paylaşım yapılması veya üçüncü taraflarla aktarım yapılması halinde ilgili yönetici onayı alınır ve güvenli paylaşım yöntemleri kullanılır.

(e). **Kişiye özel**

Sahibine özel kullanılan, Kurum bilgi varlığı niteliği taşımayan veya Kurum süreçlerini etkilemeyen kişisel içerikler bu sınıfta değerlendirilir. Ancak Kurum sistemlerinde işlendiği/depolandığı ölçüde, kişisel veriler (KVKK kapsamındaki veriler dâhil) "Kişiye özel" sınıfı altında değil; ilgili sınıflandırma kuralları kapsamında (Gizli / Çok Gizli gibi) değerlendirilir.

Kurum sistemlerinde tutulan kişisel veriler için KVKK ve bilgi güvenliği kuralları uygulanır; erişim ve işleme faaliyetleri kayıt altına alınır.

(f). **Yayınlanabilir, Umumi**

Kullanılması veya paylaşılması bilgi güvenliği açısından risk doğurmayan, kamuya açık olarak yayınlanması uygun olan bilgilerdir. Bu sınıfa; kamuya açık duyurular, onaylanmış kurumsal yayınlar, kamuya açık web içerikleri ve yetkili makamlarca yayınlanmış bilgiler dâhildir.

Yayınlanabilir bilgilerin doğruluğu ve güncelliği, ilgili birim tarafından kontrol edilerek yayınlanır.

2. **Bilgi Etiketleme ve İşleme**

Gerekli olduğu durumda, fiziki ve elektronik ortamda olan bilgi varlıkları; sınıflandırma derecesini gösterecek şekilde etiketlenmelidir. Bilgi etiketleme ve işleme için kullanılacak standartlar ve prosedürler belgelenmeli ve uygulanmalıdır. Etiketleme ve işleme kuralları, Tebliğ (VII-128.10) kapsamında bilgi varlıklarının envanteri ile uyumlu olacak şekilde uygulanır ve kontroller (erişim, paylaşım, şifreleme, loglama, saklama ve imha) sınıflandırma seviyesine göre belirlenir. Bilgi etiketleme ve işlemede aşağıdaki kurallar uygulanmalıdır:

a) Fiziksel etiketler, mümkün olduğu durumlarda kullanılmalıdır. Bununla beraber, elektronik biçimdeki belgeler gibi bazı bilgi varlıkları fiziksel olarak etiketlenemezler. Bu nedenle, bu tür belgelerde elektronik anlamda etiketlemenin kullanılması gerekmektedir. Sınıflandırma etiketi, mümkün olduğu ölçüde ilgili varlık envanter kaydı ile ilişkilendirilir.

b) Dokümanlar, içerdiği bilginin en yüksek güvenlik seviyesi göz önüne alınarak sınıflandırılmalı ve bu sınıflandırma derecesi her sayfanın sol üst ve alt köşesinde büyük harflerle ve altı çizili olarak yer almalıdır. Çok Gizli ve Gizli sınıfındaki dokümanlar için paylaşım kısıtları, yetkilendirme ve kayıt (log) gereklilikleri ayrıca uygulanır.

c) Manyetik kayıt ortamındaki (kartuş, disk, disket, CD, kaset vb.) bilgi varlıkları sınıflandırılmalı ve sınıflandırma seviyesi büyük harflerle ve altı çizili olarak medya üzerine yazılmalıdır. Taşınabilir ortamların (USB, harici disk vb.) kullanımı sınıflandırma seviyesine göre sınırlandırılır; gerekli durumlarda şifreleme uygulanır ve hareket kayıtları tutulur.

d) Elektronik ortamdaki belgelerde de (Word, Excel, Powerpoint dosyaları vb.) sınıflandırma derecesi her sayfada sol üst ve alt köşede büyük harflerle ve altı çizili olarak bulunmalıdır. Elektronik belgelerin paylaşımı ve saklanması, sınıflandırma seviyesine göre tanımlanan erişim kontrolü ve güvenli paylaşım yöntemleri ile yapılır.

e) Çok gizli, gizli, hizmete özel bilgilerin gerekli güvenlik önlemi olmaksızın e-posta, faks, telefon, cep telefonu, sesli mesaj, telefon gibi ortamlarda aktarılmamalıdır. Bu tür bilgilerin elektronik ortamda paylaşımı zorunlu ise, Kurum tarafından onaylı güvenli kanallar, şifreleme ve yetkilendirme yöntemleri kullanılmalıdır.

f) Çok gizli, gizli, hizmete özel güvenlik seviyesine sahip bilgi varlıklarının "bilmesi gereken" prensibi kapsamında yetkisiz kişiler tarafından görülmemesi sağlanmalıdır. Bu kapsamda erişim yetkileri rol bazlı olarak tanımlanır; kritik erişimler gerektiğinde izlenir ve kayıt altına alınır. Sınıflandırma ve etiketleme uygulamaları Tebliğ (VII-128.10) kapsamında en az yılda bir gözden geçirilir ve gerekli iyileştirmeler yapılır.

EK-1: BİLGİ VARLIKLARI ENVANTERİ – ASGARİ ALANLAR

Bu talimat kapsamında sınıflandırılan tüm bilgi varlıkları, Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) uyarınca Kurumun bilgi varlıkları envanteri ile ilişkilendirilir.

Bilgi varlıkları envanterinde asgari olarak aşağıdaki alanlar yer alır:

- Bilgi varlığının adı ve tanımı
- Bilgi varlığının sahibi ve sorumlu birim
- Bilgi varlığının bulunduğu ortam (fiziksel / elektronik / sistem)
- Sınıflandırma seviyesi (Çok Gizli, Gizli, Kuruma Özel vb.)
- Veri türü (kişisel veri, hassas kişisel veri, finansal veri, ticari sır, kritik sistem verisi vb.)
- Kritik bilgi sistemi ile ilişkisi (var/yok)
- Gizlilik, bütünlük ve erişilebilirlik etkisi
- Uygulanması gereken temel güvenlik kontrolleri
- Saklama süresi ve imha yöntemi
- Üçüncü taraf erişimi olup olmadığı

Envanter kayıtları güncel tutulur ve en az yılda bir kez gözden geçirilir.

EK-2: SINIFLANDIRMAYA GÖRE ASGARİ GÜVENLİK KONTROLLERİ

Bilgi varlıklarına uygulanacak asgari güvenlik kontrolleri, sınıflandırma seviyesine göre aşağıdaki şekilde belirlenir. Bu kontroller, Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) kapsamında uygulanır.

Çok Gizli:
- Güçlü kimlik doğrulama ve rol bazlı erişim kontrolü
- Şifreleme (saklama ve iletim sırasında)
- Ayrıntılı loglama ve izleme
- Yetkili onay olmaksızın paylaşım yasağı
- Kontrollü ve kayıtlı imha

Gizli:
- Rol bazlı erişim kontrolü
- Gerektiğinde şifreleme
- Loglama ve izlenebilirlik
- Kurum dışı paylaşım için yönetici onayı

Kuruma Özel / Hizmete Özel:
- Yetkilendirilmiş erişim
- Kurum dışı paylaşımda onay ve güvenli aktarım
- Uygun saklama ve imha kuralları

Kişiye Özel:
- KVKK ve ilgili mevzuat hükümlerine uygun işleme
- Yetkisiz erişime karşı temel kontroller

Yayınlanabilir:
- Yetkili birim onayı sonrası kamuya açık kullanım
- Doğruluk ve güncellik kontrolü

Kontroller, risk değerlendirmesi sonuçlarına göre gerektiğinde güçlendirilebilir.