1. AMAÇ

Bu prosedürün amacı; Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı bilgi varlıklarını tespit etmek ve uygun koruma sorumluluklarını tanımlamak.

2. KAPSAM

Bu prosedürde belirtilen ve uyulması gereken hususlar tüm bilgi varlıkları için geçerlidir.

3. TANIMLAR

Bilgi Varlığı Yaşam Döngüsü: Bilgi yaşam döngüsü oluşturma, işleme, depolama, iletme, silme ve imhayı içerir.

4. REFERANSLAR

TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi
TS ISO / IEC 27002 Bilgi Teknolojisi-Güvenlik Teknikleri Bilgi Güvenliği Yönetimi için Uygulama Kuralları

5. UYGULAMA

5.1. Varlıkların Sorumluluğu

5.2.Varlık Envanteri ve Varlıkların Sahipliği

Bilgi ve bilgi işleme tesisleri ile ilgili varlıklar belirlenerek ilgili varlıkların envanteri çıkartılır. Envanter, güncel, tutarlı, doğru ve diğer envanterler (demirbaş kaydı vb.) ile uyumlu olacak şekilde muhafaza edilir. Varlıklar oluşturulduğunda veya envantere dahil edildiğinde sahiplikleri belirlenir. Varlık sahibi varlık yaşam döngüsü boyunca varlığın uygun yönetiminden sorumludur.

Varlık sahibi;

a) Varlığın envantere kayıtlı olduğundan emin olmalı,
b) Varlıkların uygun şekilde sınıflandırıldığından ve korunduğundan emin olmalı,
c) Uygulanabilir erişim kontrol politikasını dikkate alarak önemli varlıklara erişim kısıtlamalarını ve sınıflandırmasını tanımlar ve periyodik olarak gözden geçirir,
d) Varlıkların Silinmesi ya da imha edilmesinde uygun işlemin uygulandığından emin olur,

5.3.Varlıkların Kabul Edilebilir Kullanımı ve İadesi

Bilgi ve bilgi işleme tesisleri ile ilgili bilgi ve varlıkların kabul edilebilir kullanımına dair kurallar belirlenerek, yazılı hale getirilir. Uygulanmak üzere tüm çalışanlarla paylaşılır. Çalışanların ve alt yüklenici çalışanlarının istihdamlarının veya sözleşmelerinin sonlandırılması durumunda zimmetlerindeki bilgi varlıkları yazılı bir belge ile iade alınır.

Ref: TA BGYS 006 Varlıkların Kabul Edilebilir Kullanımı Talimatı

5.4. Bilgi Sınıflandırma

5.4.1. Bilgilerin Sınıflandırılması ve Etiketleme

Bilgi için sınıflandırma ve ilgili koruma kontrollerinin de bilgi paylaşımı ya da kısıtlaması için yasal gereklerin yanı sıra iş ihtiyaçları dikkate alınır. Bilginin saklandığı, işlendiği ya da başka türlü ele alındığı ya da korunduğu bilgi dışındaki varlıklar da bilgi sınıflandırması ile uyumlu olarak sınıflandırılır. Bilgi varlıklarının sahipleri, yaptıkları sınıflandırmadan sorumludur.

Sınıflandırma, sınıflandırma ve sınıflandırmanın zaman içerisinde gözden geçirilmesi kriterleri için teamülleri içerir. Sınıflandırmadaki koruma düzeyi gizlilik, bütünlük ve erişebilirlik ve ele alınan tüm gereksinimler analiz edilerek değerlendirilir.

Sınıflandırma düzenine göre, bilginin etiketlenmesi sağlanır.

5.5.Varlıkların Kullanımı

Bilgi varlıkları kullanımında "Varlıkların Kabul Edilebilir Kullanım Kuralları" 'na uygun kullanıma dikkat edilir. Bunun yanı sıra, bilgi sınıflandırma düzenine uygun olarak;

- Bilgi sınıfına uygun erişim yetkilendirmesi sağlanır.
- Depolama alanı bulunduran bilgi varlıklarında, bilgi depolamada güvenlik kriterlerine uygun hareket edilir.
- Gizlilik seviyesi yüksek olarak belirlenmiş bilgi varlıklarının kurum dışına çıkarılması gerektiğinde birim yöneticisi izni aranır.

5.6. Ortam İşleme

5.6.1. Taşınabilir Ortam Yönetimi

Taşınabilir ortam için aşağıdaki hususlar dikkate alınır;

a) Artık gerekmiyorsa, kuruluştan kaldırılacak herhangi bir tekrar kullanılabilir ortamın içeriği geri kazanılamaz hale getirilir,
b) Mümkün olduğunda taşınabilir ortam kullanımı loglanır,
c) Tüm taşınabilir ortamlar, güvenli ortamda saklanır,
d) Taşınabilir ortam içerisinde gizlilik seviyesi yüksek bilgi bulunması durumunda kriptografik kontrollere ilişkin kurallar gereğince şifreleme uygulanır,
e) Depolanan veriye hala ihtiyaç duyuluyorsa medya riskini azaltmak için veri erişilemez olmadan önce yeni ortama transfer edilir,
f) Değerli verilerin birden fazla kopyası, veri hasarı ya da veri kaybı riskini azaltmak için ayrı bir ortamda saklanmalıdır,

g) Taşınabilir ortamın kaydedilmesi veri kaybı olasılığını sınırlandırmak amacıyla dikkate alınır,
h) Taşınabilir ortam sürücüleri sadece kullanmak için bir iş nedeni olduğunda etkinleştirilir,

5.6.2. Ortamın Yok Edilmesi

Gizli bilgileri içerin ortamın güvenli yok edilmesi için prosedürler, bilgilerin hassasiyeti ile orantılı olarak uygulanır. Ortamın yok edilmesinde aşağıdaki hususlar dikkate alınır:

a) Hassas bilgileri içeren ortam güvenli bir şekilde saklanır ve yok edilir; örneğin, yakma veya parçalama ya da kuruluşun başka bir uygulamasında kullanmak için verilerin silinmesi,
b) Hassas öğelerin yok edilmesi tutanaklar kayıt altına alınır.

5.7.Fiziksel Ortam Aktarımı

Taşınan bilgileri içeren ortamları korumak için aşağıdaki hususlara dikkat edilmelidir:

a) Güvenilir taşımacılık firmaları ya da kuryeler kullanılır,
b) Paketleme, taşıma sırasında ortaya çıkabilecek herhangi bir fiziksel hasardan korumak için yeterli ve üreticinin belirlediği teknik özelliklere uygun olmalıdır. Örneğin; ısı, nem ya da elektromanyetik alanlara maruz kalma gibi ortamın yenileme etkisini azaltacak herhangi bir çevresel faktörlere karşı koruma.
c) Taşınan bilgi dijital ortamda ise gerekli olması halinde kriptografi uygulanır, basılı evraklar kapalı zarflarda aktarılır.

5.8.Kuruluş dışındaki varlıkların güvenliği

Kurum dışında bulunan varlıklar da, kurum içinde bulunan varlıklarda aynı şekilde korunmaktadır. Kurum dışındaki varlıkları korumak için;

a) Zimmet formları eksiksiz takip edilir.
b) Gerektiğinde elektronik eşya sigortası yapılır.
c) Bilgisayarlarda disk şifrelemesi yapılır.

6. SORUMLULUK

Tüm çalışanlar prosedürün uygulanmasından sorumludur.

7. KONTROL

Dokümanlar ihtiyaç halinde revize edildiği gibi, yılda bir kez periyodik olarak kontrol edilir.

8. EKLER

-