# AMAÇ:

Bu politikanın amacı üniversitenin tüm iletişim türlerinde bilgi transferinin güvenli yöntemlerle yapılmasını sağlamak için kuralların tanımlanmasıdır.

# KAPSAM:

Bilgi Güvenliği kapsamında yürütülen tüm birimleri kapsamaktadır.

# GENEL BİLGİ İŞLEME KURALLARI

Yapılan toplantılarda üniversiteye ait bilgiler hakkında konuşulması, kurum içinde evraklar ile yapılan işlemler, bilgi sistemleri üzerinde yapılan sorgulama, hesaplama, raporlama, vb. işlemler “bilgi varlıklarının işlenmesi” kapsamında değerlendirilen örnek durumlardır.

* 1. Bilginin, yazılı, sözlü, görsel ortamlarda işlenmesi söz konusu olduğunda, bilginin kullanıldığı ortamın ve altyapının, Bilgi İşlem bilgi güvenliği politika ve prosedürlerine uygunluğu sağlanmalı; bilgiyi kullanan tüm tarafların da bu politika ve prosedürlerin gereklerinden haberdar olduğundan ve bunlara uyduğundan emin olunmalıdır.
  2. Gizlilik dereceli bilgiler kamuya açık alanlarda kullanılmaz (okunmaz, tartışılmaz, vb.).
  3. Gizlilik dereceli bilgiler üzerinde çalışma yapılırken, bu bilgilere erişim yetkisi olduğundan emin olunmayan bir başka kişinin çalışma ortamına gelmesi durumunda, fiziksel veya elektronik ortamdaki bu bilgiler, gelen kişinin erişimini veya görüşünü engelleyecek şekilde korunur.
  4. Gizlilik dereceli bilgiler ile ilgili çalışmalar ortak alanlarda yapıldığında (örn. toplantı salonları) bu ortam terk edilirken, geride hiçbir bilgi ve belge kalmayacak şekilde kontrol ve temizlik yapılır.
  5. Çalışmanın yürütülmesinden sorumlu birim yöneticisinin izni olmadıkça, gizlilik dereceli belge ve bilgilerin kullanıldığı çalışmaların yürütüldüğü ortamda herhangi bir kayıt işlemi (ses kaydı, görüntü kaydı, vb.) yapılamaz.

# GÜVENLİ BİLGİ AKTARIMI

* 1. Gizlilik dereceli bilgilerin aktarımından önce, bilgiyi talep edenin bu bilgiye erişim yetkisi bulunduğundan emin olunur. Erişim yetkisinin bulunduğunu belgelendirme sorumluluğu bilgiyi talep eden tarafındır. Şifahi olarak gizlilik dereceli bilgilerin Bilgi İşlem Daire içinde ve dışında aktarımı söz konusu olamaz.
  2. Gizlilik dereceli bilgilerin kurum içinde veya kurum dışına elektronik posta olarak aktarılması söz konusu olduğunda, bilgiler sıkıştırılıp şifrelenmiş olarak e-postanın ekindeki bir dosyada yer alır. Şifre sms ile iletilir.
  3. Gizlilik dereceli elektronik bilgilerin taşınabilir depolama ortamları ile (usb bellek vb.) aktarımı söz konusu ise, işlem tamamlanıp gizli bilgiler uygun şekilde bu taşınabilir ortamdan silinmedikçe, bu taşınabilir depolama cihazları başka bir amaç için kullanılamaz ve başka bilgisayarlara bağlanamaz.
  4. Sistemlere yönetim amaçlı yapılan uzaktan erişimler vpn gibi güvenli metodlar ile yapılır.

# FİZİKSEL ORTAMDA BİLGİ AKTARIMI

* 1. Bilgi varlığı, zarf içine sığabilecek boyutlarda ise (CD, Kağıt gibi), zarfa konularak yapıştırılmak suretiyle kapatılır. Gönderen kişi, zarf kapağını imzalayarak kuryeye teslim eder.
  2. Gönderen taraf, aktarılan varlığın alıcının eline geçip geçmediğini kontrol eder (örneğin telefon ile teyit alınır).
  3. Gizlilik dereceli bilgilerin fiziksel gönderimi sırasında iki ayrı ambalaj kullanılacak, dış ambalajda özel bir işaretleme yapılmayacak, iç ambalaj ise ambalaj içeriğini belli etmeyecek şekilde koruyucu olacak, gönderinin alıcısı dışında kişilerce açılmasını engelleyecek şekilde işaretlenecektir (örn. gizlilik derecesini belirtir kaşe basılması).
  4. Bilgi varlığı, disk, bilgisayar gibi, zarf içine sığmayacak boyutlarda ise, uygun şekilde paketlenir. Paketler, gönderilen varlığa zarar gelmesini önleyecek nitelikte ve sağlamlıkta olmalıdır. Paketlerin yolda açılmadığından emin olmak için kapak bölümü imzalanır.
  5. Alıcı taraf, aktarım esnasında gönderilen paketin açılmadığından emin olmalıdır.
  6. Aktarımların dolaylı yollarla, elden ele teslimat şeklinde değil, bir seferde gönderenden alıcıya ulaşacak şekilde gerçekleşmesi esastır.

# SÖZLÜ VE GÖRSEL OLARAK BİLGİ GÜVENLİĞİ AKTARIMI

* 1. Elektronik ve fiziksel ortamlarda bilginin aktarımı konusunda olduğu gibi, sözlü iletişimde de bilgi güvenliğinin korunması sağlanır.
  2. Üniversiteye özel konular hakkında, kamuya açık alanlarda yüksek sesle konuşulmaz.
  3. Telefon görüşmelerinde, toplantılarda, vb. sözlü iletişimin sağlandığı ortamlarda karşı tarafın (telefonla görüşülen kişi, toplantı katılımcıları gibi) gizlilik dereceli bilgiye erişim yetkisi yoksa veya erişim yetkisinden emin olunamıyorsa, gizlilik dereceli bilgiler paylaşılmaz.
  4. Çalışanlar “sosyal mühendislik” yöntemi konusunda bilgilendirilir ve yetkisiz kişilere bilgi vermez.
  5. Kurumun kamu oyundaki imajını oluşturan, reklam, web sitesi, afiş, tanıtım videosu gibi tanıtım materyalleri bir bilgi güvenliği ihlali olup olmadığı (gizlilik dereceli bilgilerin dahil edilmiş olması, teknik altyapıya ilişkin detaylı bilgilerin bulunması vb.) kontrol edilerek kamuoyuna sunulur.

1. **YAPTIRIM**

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Temsilcisi tarafından e-posta üzerinden yazılı olarak uyarılır. Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3’ten fazla tekrar ederse “PR-033-Bilgi Güvenliği İhlal Olayları ve Disiplin Soruşturması Prosedürü” gereğince kişiler hakkında işlem yapılır. Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, birim amirinin bilgisi dahilinde BGYS Ekibi’ne en kısa sürede bildirme sorumluluğundadır.