1. AMAÇ

Bu talimat Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı kapsamındaki hayata geçirilen tüm projelerde Bilgi Güvenliğinin ele alınmasıdır.

2. KAPSAM

Bu talimat Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığındaki hayata geçirilen tüm projelerde Bilgi Güvenliğini kapsar**.**

3. YASAL DAYANAK: -

4. SORUMLULAR:

3.1 Proje Yöneticisi

- Projede bilgi güvenliği gerekliliklerinin uygulanmasını sağlar.
- Risk değerlendirmesinin yapılmasını ve güncellenmesini koordine eder.
- Ekiplerin bilgi güvenliği farkındalığını takip eder.

3.2 Proje Ekibi

- Talimatta belirtilen güvenlik gerekliliklerine uyar.
- Proje dokümanlarını güvenli şekilde saklar ve paylaşır.

3.3 BGYS Ekibi

- Gerekliliklerin standarda uygunluğunu kontrol eder.
- Proje başlangıç ve kapanışlarında bilgi güvenliği kontrollerine katılır.

3.4 Tedarikçi / Üçüncü Taraf Çalışanları

- Kurum güvenlik politikalarına ve gizlilik yükümlülüklerine uyar.

5. UYGULAMA

Proje Tanımı ve Kapsamı

Proje, önceden belirlenmiş bir süre içerisinde değişim yaratmayı hedefleyen, birbiriyle ilişkili amaç ve hedefleri olan, uygulanması sonucunda çeşitli ürünlerin elde edildiği bir çalışmadır. Projelerin türünden bağımsız olarak (Örneğin; ARGE Projeleri, IT Projeleri, İş Geliştirme Projeleri, Fiziksel ve Çevresel Projeler v.b.) tüm proje süreçlerinde bilgi güvenliği hedefleri ele alınmalıdır.

Projelerde Bilgi Güvenliği

Proje yönetiminde aşağıda belirtilen kriterlere dikkat edilmelidir. Yukarıda belirtilen kapsam dâhilindeki projeler için, proje yöneticileri tarafından "BİDB Devam Eden Yazılım Projeleri Listesi " ele alınmalıdır.

- Proje yönetim sürecinde yazışmalar Varlıkların Kabul Edilebilir Kullanımı Talimatında geçen e-posta kurallarına uygun olarak yapılmalıdır.
- Doküman paylaşımı güvenli kanallardan gerçekleştirilmelidir.

- Üçüncü taraflarla yapılacak çalışmalar öncesi gizlilik sözleşmesi yapılmalıdır.
- Proje dosyalarına erişimin erişim yetki matrislerine uygun olarak yapılması ve kontrolünün sağlanması gerekmektedir.
- Proje geliştirme sürecindeki ekiplerin sosyal mühendislik riskine karşı dikkatli davranması için farkındalık eğitimlerinin sürekli tekrarlanması sağlanmalıdır.
- Kullanılan bilgi varlıkları üzerinde Bilgi sınıflandırma sistemine uygun olarak hareket edilmesi sağlanmalıdır.
- Proje planlama aşamasında Proje süreçlerindeki Bilgi Güvenliği Riskleri "BİDB Devam Eden Yazılım Projeleri Listesi" çerçevesinde değerlendirilmeli, gerekli kontroller sağlanmalıdır.

BİDB Devam Eden Yazılım Projeleri Listesinde belirtilen kriterlere göre tavsiye edilen kontroller uygulanmalıdır. Uygulama aşamasında Bilgi Güvenliği temsilcileri ile iletişime geçilebilir.

Referanslar

- TA BGYS 006 Varlıkların Kabul Edilebilir Kullanımı Talimatı
- FR 3.03.1_01 Yeni Yazılım Ve Mevcut Yazılımda Değişiklik Talep Formu
- FR 3.03.2_16 Sistem_Yazılım Değişiklik Kayıt Formu