1. AMAÇ

Bu doküman, OSTİM Teknik Üniversitesi tarafından yönetilen projelerin Bilgi Güvenliği Yönetim Sistemine ilişkin çıkabilecek riskleri önceden değerlendirip, proje başlamadan önce gerekli aksiyonların ortaya konması ve gerçekleştirilmesi için izlenecek süreci belirtmek amacıyla hazırlanmıştır.

2. KAPSAM

Bu doküman OSTİM Teknik Üniversitesi'nde yürütülen ve proje olarak nitelendirilen işlerde uygulanır.

3. UYGULAMA

OSTİM Teknik Üniversitesi bünyesinde tanımlanmış tüm projelerde projenin karakteristiğinden bağımsız olmak üzere aşağıdaki hususlar değerlendirilir.

- Proje ile ilgili risk değerlendirmesi yapılarak bilgi güvenliği riskleri tanımlanır ve proje içinde uygun kontroller adreslenir.
- Proje ile ilgili olarak bilgi güvenliği ihtiyaçları değerlendirilir ve bilgi güvenliği ihtiyaçlarının uygun yerlerde proje içinde gerekli kaynak olarak atanması sağlanır.

a. Proje Yönetiminde Bilgi Güvenliği Değerlendirilmesi

OSTİM Teknik Üniversitesi bünyesinde başlayacak her türlü projenin (İnşaat, tesis, bilgi teknolojileri ve üretim alanında gibi) proje başlangıç adımında bilgi güvenliği gereksinimleri ve riskleri ortaya konulur. Projenin yürütüleceği birim amiri tarafından projenin başında Bilgi güvenliği gereksinimleri ve riskleri değerlendirilerek öngörülen bilgi güvenliği riskleri ilgili birimin amiri tarafından gerekli tedbirler alınır. Yapılan bu risk değerlendirmeler sonucu, gerekirse Bilgi güvenliği yönetim sistemi formal risk değerlendirme sürecinde kullanılan tablolar güncellenir.
OSTİM Teknik Üniversitesi yapılan değerlendirmeler, sorumlular ile paylaşılarak onaylanır. Proje ile ilgili aksiyonların takibi, proje yöneticisi tarafından gerçekleştirilir.

b. Değerlendirme Kriterleri ve Risk Noktaları

Proje kapsamına göre aşağıdaki konu başlıkları, projeye başlamadan önce değerlendirilir. Değerlendirme bu konu başlıkları ile sınırlı olmayıp bunlar dışında olan bir bilgi güvenliği riski varsa o riskler de değerlendirmeye alınır. Değerlendirme sonucu varsa riskler tanımlanır ve gerekli aksiyonlar uygulanır. Belirlenen riskler form üzerinde ayrıntılı olarak açıklanır.

Genel riskler:

- Kritik ve hassas bilgiler tanımlanmış mıdır? Bu bilgilere yönelik işlem yapılacak mıdır? (Örneğin finansal bilgiler, rekabet avantajı sağlayan gizli şirket bilgileri gibi) Bu bilgiler hakkında proje ekibinin bilgilendirilmemesi
- Projeden olumlu/olumsuz etkilenebilecek tüm taraflar proje hakkında bilgilendirilme yapılmaması kaynaklı iş sürekliliği riskleri meydana gelebilmesi
- Taşınabilir ortamlar (Laptop, Tablet, El terminali, USB, CD/DVD) kullanılacak ve kritik bilgiler taşınabilir ortamlar üzerinde tutulacak mıdır? Bu konuda gerekli güvenlik önlemlerinin alınmaması
- Proje kapsamında özel bir yasal gereksinim varsa buna uygun olarak projenin planlanmaması.

Tedarikçi kaynaklı olabilecek riskler:

- Proje kapsamında tedarikçi çalıştırılması ve sözleşmesinin yapılmaması
- Proje kapsamında çalışacak tedarikçinin kritik altyapı sistemlerine erişmesi veya İşletme çalışma ortamına erişmesi
- Tedarikçilere kritik tesis veya sistemlere erişim yetkisi verilmesi hususunda gerekli izinlerin alınmaması

Fiziksel ve altyapı güvenliğine ilişkin riskler:

- Bir inşaat projesi yapılacaksa, mevcut tesislere ve altyapı sistemlerine zarar verebilmesi
- Proje kapsamında yanıcı patlayıcı madde kullanılacaksa çevre tesislerine ve teçhizatlarına zarar verebilmesi

İnsan kaynaklı riskler:

- Çalışacak insan kaynağının o işi yapabilme kabiliyeti hakkında yeterliliği
- Proje kapsamında çalışacak personele gerekiyorsa verilecek ek erişim yetkileri için gerekli izinlerin alınmaması
- Proje kapsamında yer alacak kişiler arasında görevler ayrılı ilkesine uygun olarak görev ve sorumluluklar belirlenmemiş olması

Teknoloji kaynaklı riskler:

- Uygulama, sistem veya bileşenler halka açık ağlar, internet, kablosuz ağlar üzerinden erişilebilecek bir proje ise güvenli protokollerin tercih edilmemesi
- Yeni bir sistem veya mevcut sistemlerde büyük bir değişiklik söz konusu ise sistem kabul ve güvenlik testlerinin yapılmasının şartnameye konmaması veya planlanmaması
- Söz konusu projedeki uygulama ve bileşenler için yetkili kullanıcıların (adminler vs.) proje başında belirlenmemiş olması
- Proje kapsamında şifreleme (encryption) teknikleri, kriptografik altyapı kullanımına gereksinim varsa, uygun güvenlik anahtarlarının oluşturulmaması

Erişim kaynaklı riskler:

- Kritik sistemler olarak tanımlanabilecek tesisler ve yazılımlara iç personelin erişimi olabilir, dış kaynaklı personelin erişimi de sınırlı olabilir. Bunun içinde gerekli izinlerin yazılı olarak alınması gerekir.

4.REVİZYON GEÇMİŞİ

Revizyon No	Tarih	Açıklama
01	07.11.2024	Entegre Kalite Yönetim Sisteminde kalite yönetiminde zorluklar ile karşılaşılması sebebiyle ISO 9001 Kalite Yönetim Sistemi (KYS) ve ISO 27001 Bilgi Güvenliği Yönetim Sisteminin (BGYS) ve dokümanlarının ayrılması ve ayrı ayrı takip edilmeleri kabul edilmiştir. Bu sebeple doküman kodlamalarında revizyon yapılmıştır.

Hazırlayan	Kontrol Eden	Onaylayan
İlknur ALŞAHİN Kalite Birimi	Kenan IŞIK Kalite Koordinatörü	Prof.Dr. Murat Ali YÜLEK Rektör
E-imzalıdır/paraflıdır	E-imzalıdır	E-imzalıdır