1. **AMAÇ:**

Bu talimatın amacı Üniversitemizin bilgi güvenliği yönetim sistemi kapsamında yürütülen faaliyetlerde görev alan üçüncü tarafların çalışmaları ile ilgili güvenlik kurallarını tanımlamaktır.

1. **KAPSAM:**

Bilgi Güvenliği kapsamında yürütülen tüm birimleri kapsamaktadır.

1. **UYGULAMA**

**3.1 Üçüncü Taraf Bilgi Güvenliği**

Kurumda üçüncü taraflar, çoğunlukla ya kurumun iş süreçlerinden bazılarını tamamıyla yürütmekte ya da bazı iş süreçlerine dahil olarak çalışmaktadır. Bu nedenle üçüncü taraflar, kurum tarafından uygulanmakta olan BGYS’nin gereklerini yerine getirir, BGYS politika ve prosedürlerine uygun olarak çalışırlar.

Kurum, verilecek hizmetlerin daha etkin şekilde gerçekleştirilebilmesi için, gerekli görülen fiziksel veya elektronik erişim yetkilerini geçici olarak üçüncü taraflara verebilir. Bu yetkilerin verilebilmesi için, üçüncü taraf ile kurum arasında yapılan ana sözleşmeye ek olarak, kurum ile firma arasında Tedarikçi Gizlilik Taahhütnamesi, üçüncü taraf personeli ile de Personel Gizlilik Taahhütnamesi düzenlenir ve imza altına alınır. Sözleşmeler taraflarca imzalanmadan erişim yetkileri verilmez.

Üçüncü taraf personeli veya firma temsilcisi, ihtiyaç duydukları erişim yetkisi taleplerini üçüncü taraf hizmetinden faydalanan birime bildirir. Üçüncü taraf hizmetinden faydalanan birim, erişim isteklerini değerlendirir. Bu değerlendirmede erişim yetkisine olan ihtiyaç (tek sefer, dönemsel, sürekli vb.), hizmet süresi, erişilecek varlığın kritikliği vb. unsurlar dikkate alınır.

Üçüncü taraf personelinin hizmeti gereği kurum kritik varlıklarının bulunduğu alanlara veya yalıtılmış hassas bölgelere (sistem odası, UPS odası vb.) erişmesi gerekiyor ise, bu alanlara erişim kurum personelinin nezaretinde gerçekleştirilmesi sağlanır ve ilgili lokasyonlara erişimler (giriş yapan kişiler, giriş saatleri çıkış saatleri, giriş amacı vb.) kaydedilir.

Üçüncü taraf personelinin elektronik erişim yetkileri Erişim Yönetimi Prosedürü’ne uygun olarak yönetilir. Bu erişim yetkileri verilirken özellikle “Bilmesi Gereken Prensibi” dikkate alınır. Bu yetkilerin verilmesi ve geri alınması Bilgi Güvenliği Ekibi tarafından gerçekleştirilir.

Üçüncü taraf personeline verilen yetkilerin kötüye kullanılıp kullanılmadığını takip etmek amacıyla izleme faaliyetleri gerçekleştirilir. Bu amaçla, üçüncü taraf personeline verilen kullanıcılar izlenebilirlik açısından tekil ve kişiye özeldir. Bu kullanıcıların aktiviteleri, gerçekleştirdikleri değişiklikler sistem logları üzerinde kaydedilmektedir.

**3.2 Dışarıdan Alınan Hizmetlerin Kontrolü**

Kurum, mevcut iş süreçlerini yerine getirmek, Bilgi teknolojileri altyapısının sürekliliğini sağlamak ve/veya bu kapsamdaki istekler neticesinde ortaya çıkan talepleri karşılamak üzere, ihtiyaç durumunda, Bilgi Teknolojileri sistemleri ile ilgili bakım, teknik destek, sunucu yönetimi, eğitim, yazılım geliştirme gibi süreçleri dış kaynaklı olarak gerçekleştirmek amacıyla üçüncü taraf firmalardan hizmet alabilmektedir.

Dış kaynaklı olarak gerçekleştirilen hizmetlerde, hizmeti veren firmanın sözleşme şartlarına bağlılığının takibi, hizmetin beklenen hedeflere ulaşıp ulaşmadığının izlenmesi, Bilgi Güvenliği Ekibi tarafından gerçekleştirilir.

**3.3 Tedarik Zinciri Güvenliği**

Doğrudan temin ve ihale usullerine göre alınan mal ve hizmetlere yönelik tedarikçi/tedarikçilerin belirlenmesi Bilgi Güvenliği Ekibi sorumluluğundadır. Esas olarak bilgi teknolojileri ile ilgili ürün/hizmet alımlarında altyüklenici kabul edilmemekte, tüm sorumluluk ana tedarikçiye verilmektedir. Bazı durumlarda, üçüncü tarafların sözleşmelerinin gerektirdiği ürün ve/veya hizmetleri yerine getirirken başka tedarikçiler, üreticiler veya altyükleniciler ile çalışması gerekebilir. Bu gibi durumlarda, bu politikada ilgili ürün veya hizmetle ilgili olarak belirtilen güvenlik gereksinimleri bu altyüklenici ve/veya üreticiler için de geçerli olması sağlanır. Bunun için şartname ve sözleşmelere konuyla ilgili maddeler eklenir. Tedarikçilerle yapılan sözleşmelerde bazı işler altyüklenici tarafından yapılacaksa tedarikçi bu durumu sözleşme öncesinde bildirir. Kurumun bu durumu kabul veya ret etme hakkı vardır. Ayrıca ilerleyen dönemde alt yüklenicinin değiştirilmesi tedarikçiden istenebilir.

Tedarikçi firmalar belediyemize hizmet veren üçüncü taraf personellerin işten ayrılması durumunda bilgi vermek ile yükümlüdür.

Tedarikçiler ve tedarik zinciri ile ilgili riskler Risk Değerlendirme Prosedürü’ne uygun olarak belirlenir, değerlendirilir ve işlenir.

**3.4 Projelerde Bilgi Güvenliği**

Üniversitemizde Bilgi Güvenliği Yönetim Sistemi Kapsamı dahilinde yürütülen, bilgi/bilgi varlıklarının kullanıldığı, işlendiği, saklandığı ve taşındığı projelerde aşağıdaki güvenlik kontrolleri uygulanır.

* Proje kapsamında bilgi güvenliği ile ilgili riskler Risk Değerlendirme Prosedürü’ne uygun olarak değerlendirilir.
* Proje kapsamında ele alınan bilgi/bilgi varlıklarına yönelik olarak BGYS politikaları uygulanır.
* Proje kapsamında bilgi/bilgi varlıklarına erişen üçüncü taraf personeli Personel Gizlilik Taahhütnamesi imzalar.
* Proje kapsamında çalışılan Tedarikçi firmalar ile Tedarikçi Gizlilik Taahhütnamesi imzalanır.
* Özellikle Bilgi güvenliği yönetim sistemini ve belediyemizin altyapısını etkileyecek olan sistem ve yazılım değişikliklerinde Proje Yönetiminde Bilgi Güvenliği Formu doldurulur.

Bu kontrollerin uygulanması, projenin yönetiminden sorumlu birim/personel ve/veya Bilgi Güvenliği Ekibi sorumluluğundadır. Projelerde uygulanan bilgi güvenliği kontrolleri Bilgi Güvenliği Ekibi tarafından periyodik olarak gözden geçirilir.

1. **DAĞITIM**

4.1 Tüm Birimler