1. Amaç

Bu prosedürün amacı, üniversite bünyesinde veya dışındaki teknoloji sistemleri aracılığıyla **depolanan, işlenen veya iletilen kritik verilerin envanterinin oluşturulması, yönetilmesi ve güvenliğinin sağlanmasına** ilişkin usul ve esasları belirlemektir.

2. Kapsam

Bu prosedür; kurumun teknoloji sistemleri tarafından yönetilen tüm fiziksel ve sanal sunucuları, bulut bilişim hizmetlerini, veri tabanlarını ve uygulama sistemlerini kapsar. Kurum bünyesinde veya dışındaki tüm **kritik veri hareketleri** bu kapsam dâhilindedir.

3. Dayanak

Bu prosedür aşağıdaki düzenleme ve standartlara dayanılarak hazırlanmıştır:

- TS ISO/IEC ISO 27001 Bilgi Güvenliği Yönetim Sistemi Yönergesi
- Bilgi Güvenliği Politikası
- Varlık Yönetim Politikası
- Görevler Ayrılığı ve Erişim Yönetimi Politikası.
- Bilgi ve İletişim Güvenliği Rehberi (BİGR).
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)
- İlgili mevzuat ve kurum içi düzenlemeler

4. Tanımlar

Bilgi Varlığı: Kurum faaliyetleri açısından değeri bulunan her türlü veri, sistem, uygulama ve dokümanı ifade eder.

Kritik Veri: Yetkisiz erişim, kayıp, değişiklik, silinme veya kesintiye uğraması halinde kurumun faaliyetlerini, hizmet sürekliliğini, mali yapısını, yasal yükümlülüklerini, itibarını veya bilgi güvenliğini olumsuz etkileyebilecek veridir.

Veri Sahibi/Birim Sorumlusu: Verinin doğruluğundan, güncelliğinden ve yönetiminden sorumlu kişi veya birimdir.

Veri Envanteri: Kurum bünyesinde bulunan veri varlıklarına ilişkin kayıtların tutulduğu yapılandırılmış listedir.

Teknoloji Sistemleri: Ağ altyapısı, sunucular (fiziksel/sanal), veri tabanları, uygulamalar ve bulut sistemleri.

5. Kritik Verilerin Belirlenmesi ve Sınıflandırılması

Kritik veriler, **Bilgi ve İletişim Güvenliği Rehberi**, bilgi güvenliği prensipleri ve kurumsal risk değerlendirme sonuçları dikkate alınarak belirlenir.

Bir verinin kritik olarak değerlendirilmesinde aşağıdaki kriterler esas alınır:

- **Gizlilik Etkisi:** Verinin yetkisiz kişiler tarafından erişilmesi durumunda oluşabilecek zarar düzeyi
- **Bütünlük Etkisi:** Verinin değiştirilmesi, bozulması veya doğruluğunu kaybetmesi durumunda oluşabilecek etkiler
- **Erişilebilirlik Etkisi:** Veriye erişilememesi veya hizmet kesintisi yaşanması durumunda operasyonel etkiler
- **Yasal ve Mevzuatsal Gereklilikler:** KVKK, Bilgi ve İletişim Güvenliği Rehberi, sözleşmeler ve ilgili mevzuattan doğan yükümlülükler
- **Operasyonel Kritik Seviye:** Kurumun temel hizmetlerini, akademik/idari süreçlerini veya iş sürekliliğini etkileme durumu
- **Mali Etki:** Maddi kayıp, yaptırım veya ek maliyet oluşturma potansiyeli
- **İtibar Etkisi:** Kurumsal güven, kamuoyu algısı ve paydaş ilişkileri üzerindeki etkiler
- **Ulusal/Kurumsal Kritiklik:** Kritik altyapılar, kamu hizmetleri veya stratejik süreçlerle ilişkili olma durumu

Yapılan değerlendirme sonucunda, gizlilik, bütünlük veya erişilebilirlik boyutlarından en az birinde yüksek etki oluşturan veriler **kritik veri** olarak sınıflandırılır.

6. Veri Envanteri Kapsamı

Kritik Veri Envanteri; **Bilgi ve İletişim Güvenliği Rehberi** kapsamında, kurumun hizmet sürekliliği, bilgi güvenliği ve yasal yükümlülükleri açısından kritik öneme sahip tüm veri varlıklarını kapsar.

- Ağ ve Sistemler
- Uygulamalar
- Taşınabilir Cihaz ve Ortamlar
- Nesnelerin İnterneti (IoT) Cihazları
- Fiziksel Mekânlar
- Personel

7. Kritik Veri Envanterinin Oluşturulması

Kritik Veri Envanteri, kurum bünyesindeki veri varlıklarının belirlenmesi, sınıflandırılması ve kayıt altına alınması amacıyla sistematik bir yaklaşımla oluşturulur.

Envanter oluşturma sürecinde; veri sahibi birimler tarafından veriler tanımlanır, Bilgi ve İletişim Güvenliği Rehberi doğrultusunda kritiklik ve sınıflandırma değerlendirmesi yapılır ve uygun formatta envantere kaydedilir. Envanter, veri yaşam döngüsü boyunca güncel tutulur ve değişiklikler düzenli olarak yansıtılır.

- Varlık Grubu Ana Başlığı
- Varlık Grubu Adı
- Varlık Sınıfı
- Kritiklik Derecesi
- Kritik Veri Bilişim Altyapı Sorumlusu
- Kritik Veri Saklama Ortamı

8. Roller ve Sorumluluklar

Kritik veri yönetimi sürecinin etkin, güvenli ve sürdürülebilir şekilde yürütülmesi amacıyla roller ve sorumluluklar aşağıda tanımlanmıştır.

- **Üst Yönetim:** Kritik veri yönetimi süreçlerinin uygulanması için gerekli politika, kaynak ve yönlendirmeleri sağlar; sürecin etkinliğini gözetir.
- **Bilgi İşlem Birimi:** Kritik veri envanterinin teknik olarak yönetilmesinden, sistemlerin güvenliğinden, erişim kontrollerinin uygulanmasından ve loglama süreçlerinden sorumludur.
- **Veri Sahipleri / Birim Sorumluları:** Sorumlu oldukları verilerin tanımlanması, sınıflandırılması, güncel tutulması ve erişim ihtiyaçlarının belirlenmesinden sorumludur.
- **Sistem Yöneticileri:** Teknik altyapı üzerinde erişim yetkilerinin uygulanması, güvenlik kontrollerinin işletilmesi ve kayıt mekanizmalarının çalıştırılmasından sorumludur.
- **Tüm Kullanıcılar:** Kurumsal bilgi güvenliği politikalarına uymak, kritik verileri yetkisiz şekilde işlememek ve olası güvenlik ihlallerini bildirmekle yükümlüdür.

9. Erişim ve Güvenlik

Kritik verilere erişim, **Bilgi ve İletişim Güvenliği Rehberi** kapsamında tanımlanan yetkilendirme ve erişim kontrol prensipleri doğrultusunda, görev ve sorumluluk esasına göre sağlanır.

- Kritik veri envanterine erişim yalnızca **yetkilendirilmiş personel** ile sınırlıdır.
- Erişim yetkileri, **rol bazlı erişim kontrolü** esasına göre tanımlanır ve yönetilir.
- Kritik verilerin korunması amacıyla **Bilgi ve İletişim Güvenliği Rehberi** doğrultusunda gerekli

idari ve teknik güvenlik tedbirleri uygulanır.

- Ağ ve sistem seviyesinde **loglama ve izleme faaliyetleri** yürütülür.
- Erişim kayıtları ve yetkiler düzenli olarak gözden geçirilir ve gerekli durumlarda güncellenir.

10. Güncelleme ve Denetim

Kritik Veri Envanteri, **Bilgi ve İletişim Güvenliği Rehberi** esas alınarak düzenli olarak gözden geçirilir ve güncellenir. Yapılan değişiklikler sisteme yansıtılır; risk ve eksikliklere ilişkin düzeltici ve iyileştirici faaliyetler yürütülür.

- Kritik Veri Envanteri düzenli aralıklarla ve ihtiyaç duyulan durumlarda güncellenir.
- Yeni sistem, süreç, veri veya altyapı değişiklikleri envantere yansıtılır.
- Kritik Veri Envanteri, **Bilgi ve İletişim Güvenliği Rehberi** doğrultusunda periyodik olarak gözden geçirilir ve denetlenir.
- Tespit edilen eksiklik, uygunsuzluk ve risklere yönelik gerekli düzeltici faaliyetler yürütülür.
- Güncelleme ve denetim kayıtları dokümante edilerek saklanır.

11. Saklama ve İmha

Kritik verilerin saklanması ve imhası, **Bilgi ve İletişim Güvenliği Rehberi** doğrultusunda yasal ve kurumsal saklama sürelerine uygun olarak gerçekleştirilir. Süresi dolan veya kullanım ihtiyacı ortadan kalkan veriler, güvenli yöntemlerle imha edilir ve imha işlemleri kayıt altına alınır.

- Kritik veriler, ilgili mevzuat ve kurumsal politika kapsamında belirlenen saklama süreleri boyunca güvenli şekilde muhafaza edilir.
- Saklama süresi dolan, kullanım ihtiyacı ortadan kalkan veya yasal zorunluluk gereği imha edilmesi gereken veriler güvenli yöntemlerle silinir, anonimleştirilir veya fiziksel olarak imha edilir.
- İmha işlemleri, izlenebilirliği sağlamak amacıyla kayıt altına alınır ve gerektiğinde denetlenebilir şekilde saklanır.
- Saklama ve imha süreçleri, Bilgi ve İletişim Güvenliği Rehberi ve ilgili kurumsal prosedürler doğrultusunda yürütülür.

12. Yürürlük

Bu prosedür, BGYS komisyonu tarafından onaylandıktan sonra Konya Teknik Üniversitesi Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

13. Yürütme

Bu prosedür, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.