# 1. AMAÇ

Bu prosedürün amacı, Yıldız Teknik Üniversitesi Bilgi Teknolojileri hizmetlerinde kesinti sürelerini ve veri kayıplarını önlemek için sistem ve kurumsal verilerin düzenli olarak yedeklenmesi ve ihtiyaç halinde yedekten dönme kurallarını tanımlamaktır.

# 2. KAPSAM

Bu prosedür, Yıldız Teknik Üniversitesi’nde Bilgi Güvenliği Yönetim Sistemi içinde yer alan tüm dokümanları ve çalışmaları kapsar.

# 3. TANIMLAR

**Bilgi güvenliği:** Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

**Bilgi güvenliği yönetim sistemi:** Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.

# 4. SORUMLULUKLAR

Bu prosedürün hazırlanması ve yönetiminden Bilgi Güvenliği Ekibi sorumludur. Tüm doküman taleplerinde Bilgi Güvenliği Sorumlusu yetkilidir. Prosedürün uygulanmasına yönelik sorumluluklar prosedürde belirtilmiştir. Yedekleme süreçleri “LS-061-Bilgi İşlem Daire Başkanlığı Yedekleme Planı Listesi” üzerinden takip edilmektedir. Liste ihtiyaç duyuldukça gözden geçirilmektedir.

# 5. UYGULAMA

**5.1.YEDEKLEME**

Bilgi Güvenliği Yönetim Sistemi kapsamında, Üniversitemiz bünyesinde iş sürekliliğinin sağlanması ve veri kayıplarının önlenmesi amacıyla yedekleme ve yedekten dönme işlemleri yapılmaktadır.

**5.2.VERİ YEDEKLEME**

**5.2.1. Yedekleme Sistemi İşletim Planlaması**

* Yedekleme sistemi işletimi; sistem yöneticisi tarafından hazırlanır ve Birim Amiri onayı alındıktan sonra uygulanır. Verilerin güvenilir bir şekilde yedeklenmesi sağlanır. Bilgi varlıklarının yedeklenmesi sistem yöneticisi sorumluluğunda olup harici yedekleme ünitesine yedeklenir.

Yedekleme işletim planında;

* Yedeklenecek sistemler, veri alanları, iş uygulama yazılımları ve/veya veri tabanları belirlenir.
* Yedeği alınması gereken sistem ve veri tabanlarının hangi uygulamalar kullanılarak yedekleneceği belirlenir.
* Planlanan yedeklemelerin planda adı geçen her bir sistem / uygulama / veri tabanı için yedek zamanı, periyodu ve yedek sayısı belirlenir.
* Yıl içinde, herhangi bir nedenle yedekleme işletim planında bir değişiklik yapılması gerektiğinde plan kontrollü olarak değiştirilir.

**5.2.2. Yedekleme Periyodu**

Yedekleme periyodu 1 (bir) aydan daha uzun bir zaman dilimini içeremez. Sürenin belirlenmesinde , veri ,sistem veya cihazın kritiklik durumu göz önünde bulundurulur.

Uzun süreli kesinti ya da bakım işlemleri öncesi plan dışı olarak yedekleme işlemi yapılır.

**5.2.2.1. Otomatik Ödeme**

Veri ve sunucu, cihaz kritiklik seviyeleri aşağıdaki tabloda belirtilmiştir.

|  |  |  |
| --- | --- | --- |
| **Veri Tipi** | **Kritiklik Seviyesi** | **Açıklama** |
| Sunucu | Yüksek | Sunucu diskleri |
| Veritabanı | Çok Yüksek | Uygulama veritabanları |
| Veri Alanları | Yüksek | Sunucu Diskleri |
| Veri Saklama Alanları | Yüksek | Veri Paylaşım Alanındaki veriler |
| Cihaz Yapılandırma Dosyaları | Çok Yüksek  | Cihaz yapılandırma ayarları |
| Sistem Erişim Logları | Yüksek | Sunucu ve Sistemlere Erişim Kayıtları |

**5.2.2.1.1. Çok Yüksek Kritik Verilerin Yedekleme Yöntemi**

Kritiklik seviyesi “Çok Yüksek” olan verilerin yedeklenmesi 4 saatlik periyotlar ile yapılmaktadır.

**5.2.2.1.2. Yüksek Kritik Verilerin Yedekleme Yöntemi**

Kritiklik seviyesi “Yüksek” olan verilerin yedeklenmesi günlük yapılmaktadır.

**5.2.2.2. Manuel Yedekleme**

|  |  |  |  |
| --- | --- | --- | --- |
| **Veri Tipi** | **Sıklık** | **Yedekleme Yeri** | **Yedek Sayısı** |
| Veri, Sistem, Cihaz | Tek Seferlik | Yedekleme Ünitesi | Sınırsız |

**5.2.3. Yedekleme, Saklama Ortamları ve Saklama Şekli**

Alınan yedekler; Yedekleme Ünitesi (Backup Storage Unit) üzerinde saklanır.

Kullanılacak yedekleme ortamları ve yazılımları, yedekleme sistemi ekipleri tarafından belirlenir.

Yedeklenecek verinin veya bileşenin kritiklik derecesine göre birden fazla yedekleme ortamı da kullanılabilir.

Yedeklerin; gizlilik dereceleri birim sorumlusu tarafından belirlenir ve yedekleme dönemlerine göre sınıflandırılarak saklanır.

Yedeklerin saklama ortamları; kullanılan yedekleme ortamlarında bozulmaya neden olmayacak şekilde saklanır. Birden fazla saklama ortamı (Backup Storage Unit, External Disk, Cloud Backup) kullanmak, proje yöneticisi veya bölüm sorumlusunun yetkisindedir.

**5.3. YEDEKLEME ŞEKİLLERİ**

**5.3.1.Veri Yedekleme Yöntemi**

Üniversitemizde operasyonel veri kurtarma, veri eşleme ve uzun vadeli veri saklama dahil olmak üzere yedekleme süreçlerini otomatikleştiren IBM Spectrum Protect Plus yazılımının 10.1.6 Build: 1975 Jun 12 sürümü kullanmaktadır.

Yedeği alınacak verilerin Yedekleme periyodu ve saklama süreleri proje yöneticisi veya bölüm sorumlusunun da onayı alınarak yedekleme sisteme ekibi tarafından uygulanır.

Her bir proje veya uygulama özelinde yedeklemenin başlama zamanı, yedekleme periyodu sıklığı, verinin saklama süresi gibi paramaetreler özelleştirilebilmektedir.



**5.3.2.Veri Geri Yükleme Yöntemi**

Veri kaybı durumunda birimimize yapılan talep gereği başarılı alınmış yedeklerden ilgili tarihli setden yedekten dönme işlemi yapılır.

* Veri kaybının olduğu uygulamanın sorumlusu olan birimden e-posta veya resmi yazı ile talep gelir. Uygulamanın olduğu sistem için yedekten dönme işlemi yapılır.
* Son kullanıcı e-posta hesaplarında e-posta kaybı olduğunda yedekten dönme işlemi yapılır.

Yedeği alınan verilerin kontrolü amacıyla “geri yükleme testleri” kritiklik seviyesine göre belli periyotlarda yapılır.

# 6. 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.