1. **İçindekiler**

[1 AMAÇ 2](#_Toc7535432)

[2 KAPSAM 2](#_Toc7535433)

[3 SORUMLULAR 2](#_Toc7535434)

[4 UYGULAMA 2](#_Toc7535435)

[5 İLGİLİ DOKÜMANLAR 3](#_Toc7535436)

# AMAÇ

Bu prosedürü amacı, Tekirdağ Namık Kemal Üniversitesi bünyesinde uygulanan BGYS sistemi için Bilgi Sistemlerinin edinim, geliştirme ve uyum süreci adımlarının tanımlanmasıdır.

# KAPSAM

Tekirdağ Namık Kemal Üniversitesi içerisinde yer alan tüm bilgi sistemleri bu prosedür kapsamındadır.

# TANIMLAR VE KISALTMALAR

# SORUMLULAR

Bu prosedürün hazırlanmasından BGYS Yönetim Temsilcisi sorumludur. Prosedürün uygulanmasından genel sorumlu BGYS Yönetim Temsilcisidir. Bunun dışında özel olarak sorumluluğu bulunan roller prosedürün uygulama adımlarında verilmiştir.

# UYGULAMA

* Bilgi sistemlerinin yönetimi kontrollü bir şekilde yapılmakta olup bu kapsamda politikalar ortaya konmuş, prosedürler ve talimatlar oluşturulmuş ve bunlar dokümante edilmiştir. Bilgi sistemlerinin yönetimi genel olarak buralarda tanımlanan esaslara göre yapılmaktadır.
* Bilgi Sistemlerinde yapılacak değişiklik kontrollü bir şekilde *Değişiklik Yönetim Prosedürü* esas alınarak yapılmaktadır.
* Geliştirme faaliyetleri *Güvenli Yazılım Geliştirme ve Destek Prosedürü* esas alınarak kontrollü bir şekilde yapılmaktadır.
* Yapılan geliştirmeler kontrollü olarak devreye alınmaktadır. Bu kapsamda geliştirmeler için testler uygulanmaktadır.
* Geliştirme, test ve işletim (prod) ortamları yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmıştır.
* Geliştirme süreçlerinde, kontrolsüz müdahale durumlarının önüne geçmek için ortamlara erişimlerde kimlik doğrulama ve yetkilendirme uygulanmaktadır. Bu kapsamda; *Erişim Kontrol Politikası, Sunucu Güvenlik Politikası, Uzaktan Bağlantı Politikası ve Kimlik Doğrulama ve Yetkilendirme Prosedürü* oluşturulmuştur.
* Geliştirme Süreçlerinde veri kaybını engellemek için *Yedekleme Prosedürü* oluşturulmuştur.
* Bilgi güvenliği anlamında zafiyetlerin tespiti sistematik bir şekilde *Güvenlik Açıklarını Tespit Etme Prosedürü* esas alınarak yapılmaktadır.
* Gizlilik, bütünlük veya erişebilirlik seviyesi “yüksek” ve üzeri olan ortamlara yazılım kurulumu ancak doğrudan grup başkanı veya onun görevlendirdiği kişi tarafından yapılabilir. Bu süreçte bir problem çıkması durumunda sistem önceki çalışan konfigürasyona geri döndürülür.
* Yapılan kurulumlar doğruluğu test edilmedikçe devreye alınmaz. Bu süreçte *Değişiklik Yönetim Prosedürü* esas alınır.
* Üst Yönetim, BGYS yönetiminin tanımlanan esaslara göre işletildiğine dair geri dönüşleri almakta, toplantılarda gözden geçirmekte ve sisteme uyumunu takip etmektedirler.

# İLGİLİ DOKÜMANLAR

* EYS-PO.004 Erişim Kontrol Politikası
* EYS-PO.003 Sunucu Güvenlik Politikası
* EYS-P0.005 Uzaktan Bağlantı Politikası
* EYS-PR.019 Değişiklik Yönetim Prosedürü
* EYS-PR.018 Güvenli Yazılım Geliştirme ve Destek Prosedürü
* EYS-PR.010 Bilgi Sistemleri Yedekleme Prosedürü
* EYS-PR.011 Güvenlik Açıklarını Tespit Etme Prosedürü