	TNKÜ **SUNUCU GÜVENLİK POLİTİKASI**	Doküman No:	EYS-PO-003
		Hazırlama Tarihi:	07.09.2018
		Revizyon Tarihi:	14.08.2025
		Revizyon No:	2
		Toplam Sayfa Sayısı:	2

1 AMAÇ

Bu politikanın amacı, sunuculara direkt veya uzaktan yapılan (remote, ssh vb) erişimlerde yetkisiz kullanımdan kaynaklı kritik sistemlerde meydana gelebilecek zararları, hassas bilgilerin kaybını, iş sürekliliğini ve uygulamalardan kaynaklı sistem uygulama yazılımlarından doğabilecek riskleri önlemeye ve azaltmaya yönelik standartları tanımlamaktır.

Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı içerisinde bulunan sunucular varlık envanterinde tanımlanmış, ilgili her bir varlık gizlilik, bütünlük ve erişebilirlik olarak sınıflandırılmıştır.

2 KAPSAM

Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı sunucu sistemleri ve hizmet verdiği projelerin bulunduğu her türlü sistemler kapsam olarak tanımlanmıştır.

3 SORUMLULAR

Bu prosedürün oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Bu süreçte BGYS Yöneticisi ile beraber çalışmak IT Yöneticisi sorumluluğundadır.

Politikanın uygulanmasından IT Yöneticisi ve teknik ekibi sorumludur.

4 UYGULAMA

- Sunucu sistemlerine fiziksel erişim sadece yetkilendirilmiş kişilerce mümkün olmalıdır.
- Sistem odasında yapılacak her türlü bakım, iyileştirme çalışmaları veya kurulum vb. çalışmalar yetkili personel tarafından veya yetkili personel gözetiminde hizmet alınan kuruluş personelleri tarafından gerçekleştirilmelidir.
- Sunucu sistemleri ısı seviyesi, kapasite, loglama vb. olarak gözlemlenebilmelidir.
- İlgili sunucu sistemleri varlık değerine göre yönetilmelidir.
- Farklı hizmetleri ve farklı kullanıcı grupları olan sunucu rolleri fiziksel veya kavramsal olarak birbirinden ayrılmalı veya yalıtılmalıdır.
- Sunuculara uzaktan erişim yapılması durumda güçlü kimlik doğrulama yöntemlerine ek olarak ağ yalıtımı da sağlanmalıdır.
- Sistem odasında soğutma sistemi, UPS ve yangın dedektörü gibi iş sürekliliğini etkileyecek unsurlar bulunmalıdır.
- Sunucular üzerinde (windows) güncel anti-virüs programları çalışmalıdır.
- Sunucular için bir yedekleme politikası tanımlanmış ve minimum (tahammül edilebilir) bilgi kaybına sebep verecek şekilde bir rotasyonlu yedekleme politikası uygulanmalıdır.

- Bütün sunucu sistemleri ve verileri yedeklenerek saklanmalıdır.
- Sunucu yedekleri bulunmayan veya yedeklenmeyen sunucuların ise iş sürekliliğini etkilemeyecek, hızlı bir şekilde kurulabilmesi ve ayağa kaldırılması sağlanmalıdır.
- Sunucuların gereksiz portları sunucu üzerinde de kapalı olmalıdır ve gereksiz servisler pasif veya kurulmamış olmalıdır.
- Sunucular daima kritik güncellemeleri alıyor olması veya kuruluyor olması sağlanmalıdır.
- Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı sistemlerinde yılda en az 1 kez sızma testi ile sunucuların ve ağ sisteminin zafiyeti test edilmeli ve incelenmelidir.
- Sunuculara ait IP bilgileri ve diğer önemli bilgiler sadece bilmesi gerekenler çerçevesinde bilinmesi sağlanmalıdır.
- Sunucular üzerinde bulunan ve çalışan uygulamaların/servislerin logları tutulmalı ve yaşanabilecek zafiyetlere yönelik belli aralıklarla kontrol edilmelidir.

5 YAPTIRIM

Bu politikanın ihlal edilmesi durumunda Disiplin Prosedürü uygulanacaktır.

6 İLGİLİ DOKÜMANLAR

EYS-PO.021 - DİSİPLİN PROSEDÜRÜ