	TNKÜ **KABLOSUZ ERİŞİM POLİTİKASI**	Doküman No:	EYS-PO-011
		Hazırlama Tarihi:	07.09.2018
		Revizyon Tarihi:	14.08.2025
		Revizyon No:	2
		Toplam Sayfa Sayısı:	3

1 AMAÇ

Bu politikanın amacı kablosuz cihazların firmanın bilişim güvenliğini riske etmeden bilgisayar ağımıza entegre edilmesi için söz konusu cihazların sahip olması gereken minimum standartları tanımlamaktır.

Kablosuz iletişim ağı Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı genel ağ altyapısının bir parçası olduğundan, kablosuz iletişim ağlarının tasarımı, kurulumu ve yönetimi ağın güvenliği açısından önem arz etmektedir

2 KAPSAM

Bu politika, Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı ağına bağlanan tüm kablosuz bağlantılar için geçerlidir.

Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde kullanılabilecek kablosuz veri transferi sağlayabilen herhangi bir cihaz bu politikanın kapsamındadır.

3 SORUMLULAR

Bu prosedürün oluşturulmasından BGYS Yönetim Temsilcisi sorumludur. Bu süreçte BGYS Yöneticisi tarafından destek sağlanır.
Politikanın uygulanmasından Sistem ve Ağ Sorumlusu sorumludur.

4 KURALLAR

Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı sorumluluğundaki tüm Kablosuz iletişim ağları IT Yöneticisi ve ekibi tarafından izlenir ve muhafaza edilir. Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı ağ altyapısına bağlanan herhangi bir Erişim Noktası (Access Point) veya kablosuz cihaz, Sitem ve Ağ Sorumlusu sorumluluğu altında kabul edilir.
Aşağıdaki kurallar bu politikanın uygulama esasları olarak tanımlanmıştır.

- Personelin Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı ağında kullandığı tüm Erişim Noktalarının ve kablosuz cihazlarının, kablosuz ağın ilgili tüm yasal düzenlemelerine, standartlarına ve Sistem ve Ağ Sorumlusu tarafından tanımlanmış kurallara uygun olması gerekir.
- Standart olmayan Erişim Noktalarının veya kablosuz cihazların kurulumu yasaktır.

- Kablosuz erişim cihazlarında, Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı'nin belirlemiş olduğu güvenlik ayarları kullanılmalıdır.
- Erişim cihazlarının tamamı Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı'nın fiziksel olarak korunmuş alanı içinde konumlandırılmalıdır.
- Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı, mevcut onaylanmış Erişim Noktalarını veya cihazlarını parazite neden olabilecek standart dışı, yetkisiz cihazları devre dışı bırakma hakkına sahiptir. Bu tür cihazlar önceden haber verilmeden çıkartılabilir. Kablosuz ağların izlenmesi, Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından düzenli olarak yapılmaktadır.
- Kimlik doğrulaması olmayan açık erişim, Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı çevresinde kablosuz noktalar yoluyla veya güvenli kablosuz ağdan ayrı olarak sağlanmalıdır.
- Tekirdağ Namık Kemal Üniversitesi Bilgi İşlem Daire Başkanlığı güvenli kablosuz ağında, yalnızca lisanslı veya açık kaynak kod lisanslı yazılımların kullanılmasına izin verilir.
- Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.
- Kullanıcılar tarafından kurumun tüm internet bant genişliğinin tüketilmesi engellenmelidir.
- Kablosuz ağa dahil olan kurum çalışanları için bile erişimler sınırlandırılmalıdır. Sadece internete çıkacak olan kullanıcıların kablosuz ağ üzerinden diğer uygulamaların (ses, güvenlik, mobilite vb) çalıştığı networklere erişimi engellenmeli gerekirse networkler farklı IP aralıkları üzerinde ayarlanmalı, cihaz üzerinde Access Control Listler (Yetki kuralları) oluşturulmalıdır.
- Kablosuz ağ cihazlarına erişim sadece yetkili kişiler tarafından Access Controller, SSH ya da cihaz başında console (konsol) ile yapılmalı, http ve telnet protokolleriyle erişim kapatılmalıdır.
- Yetkili Kullanıcılar, aile üyelerinden bile olsa, giriş bilgilerini ve şifrelerini korumalıdır.
- Kuruluşlar ve kullanıcılar, kablosuz iletişim ağlarını uygulamadan ve kullanmadan önce güvenlik tehditlerini anlamaları gerekir. Aşağıda açıklanan tehditler, genel olarak kablosuz ağ cihazları ile ilgili olabilecek tehditlerdir.
    - Denial of Service - Saldırgan, kablosuz ağların veya ağ aygıtlarının normal kullanımını veya yönetimini engeller veya sınırlar.
    - Dinleme - Saldırgan, kimlik doğrulama kimlik bilgileri de dahil olmak üzere kablosuz ağları veri için pasif olarak izler.
    - Man-in-the-Middle - Saldırgan, kablosuz istemciler ve AP'ler arasındaki iletişimleri aktif olarak engeller, böylece kimlik doğrulama kimlik bilgileri ve veriler elde edilir.
    - Masquerading - Saldırgan, yetkili bir kullanıcıyı taklit eder ve kablosuz ağlara belirli yetkisiz ayrıcalıklar kazandırır.

- İleti Değişikliği - Saldırgan, kablosuz ağlar yoluyla gönderilen meşru bir iletiyi silerek, ekleyerek, değiştirerek veya yeniden sıralamayla değiştirir
- Mesaj Yeniden Oynatma - Saldırgan, kablosuz ağlar vasıtasıyla iletimleri pasif olarak izler ve mesajı tekrar gönderir; saldırgan meşru bir kullanıcıymış gibi davranıyor.
- Trafik Analizi - Saldırgan, iletişim modellerini ve katılımcılarını belirlemek için kablosuz ağlar vasıtasıyla iletimleri pasif olarak izler.
- Fiziksel olarak Tampered – AP'nin (Access Point – Erişim Noktası) antenindeki değişikliklerden veya AP başka bir yere taşınırsa, şifreler donanımdan alınabilir. Bu, saldırganın lehine olan sinyal gücünü artırır.

5 YAPTIRIM

Bu politikanın ihlal edilmesi durumunda Disiplin Prosedürü uygulanacaktır.

6 İLGİLİ DOKÜMANLAR

EYS-PO.021 - DİSİPLİN PROSEDÜRÜ