1. Amaç

Bu politikanın amacı, kurum sınırları içerisindeki kablosuz ağ kullanımına ilişkin standartları belirlemektir. Bu politika, kullanıcı ve cihazların kurumun kablosuz ağına güvenli bir şekilde erişimine yardımcı olmak için tasarlanmıştır.

2. Kapsam

Bu politika, kuruma ait tüm alanlar, kurumun tüm kablosuz yayınları , üniversite personeli, öğrencileri, ziyaretçileri ve diğer kullanıcıları kapsamaktadır..

3. Sorumlular

Bu politikanın oluşturulmasından BİDB ve onaylamasından BGYS komisyonu sorumludur. Uygulanmasından kurum sınırları içerisinde kablosuz ağ teknolojilerini kullanan herkes sorumludur.

4. Kurallar

Üniversite sorumluluğundaki tüm Kablosuz iletişim ağları BİDB tarafından izlenir ve muhafaza edilir. Kurum sınırları içerisinde kullanılan herhangi bir Erişim Noktası (Access Point) veya kablosuz cihaz, BİDB kontrolü altında olmalıdır. Aşağıdaki kurallar bu politikanın uygulama esasları olarak tanımlanmıştır.

- Tüm Erişim Noktalarının ve kablosuz cihazlarının, kablosuz ağın ilgili tüm yasal düzenlemelerine, standartlarına ve BİDB tarafından tanımlanmış kurallara uygun olması gerekir.
- BİDB tarafından onaylanan kablosuz ağ erişim cihazları kullanılmalıdır.
- Standart olmayan Erişim Noktalarının veya kablosuz cihazların kurulumu yasaktır.

- Kablosuz erişim cihazlarında, BİDB'nin belirlemiş olduğu güvenlik ayarları kullanılmalıdır.
- Erişim cihazlarının tamamı kurumun fiziksel olarak korunmuş alanı içinde konumlandırılmalıdır.
- BİDB, 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, BİDB tarafından düzenli olarak yapılır.
- Kullanıcılar tarafından kurumun tüm internet bant genişliğinin tüketilmesi BİDB tarafından engellenir.
- Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, BİDB tarafından sınırlandırılır.
- Kablosuz ağ cihazlarına erişim sadece yetkili kişiler tarafından Access Controller, SSH ya da cihaz başında console (konsol) ile yapılır.
- Yetkili Kullanıcılar, giriş bilgilerini ve parolalarını kimse ile paylaşmamalıdır.
- Kablosuz iletişim ağlarını kullananların gerekli güvenlik tedbirlerini almaları 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. Yaptırım

Bu politikanın ihlal edilmesi durumunda KTÜN BİLGİ GÜVENLİĞİ POLİTİKASI'nda belirtilen "POLİTİKANIN İHLALİ VE YAPTIRIMLAR" başlığı altındakiler geçerlidir.

6. Yürürlük

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

7. Yürütme

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.