

	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği Politikası		Doküman Kodu	BG. PLTK-16
			İlk Yayın Tarihi	29.05.2025
			Revizyon Tarihi	-
			Revizyon No	00
			Sayfa No	1 / 4
Hazırlayan		Kontrol Eden	Onaylayan	
Bilgi İşlem Personeli		Bilgi İşlem Daire Başkanı	BGYS Komisyonu	

1. Amaç

Bu politika, kurum bünyesinde kullanılan **Nesnelerin İnterneti (IoT)** cihazlarının güvenliğini sağlamak, bilgi güvenliği ihlallerini önlemek, yetkisiz erişimleri sınırlamak ve ilgili tehditlere karşı kurumu korumak amacıyla hazırlanmıştır.

2. Kapsam

Bu politika, kurum ağına bağlı veya dolaylı olarak erişimi olan veya kurum ağına bağlı olmasa da kurumun fiziksel sınırları içinde olan tüm IoT cihazlarını, bu cihazlardan sorumlu kişileri ve bu cihazların bağlı olduğu altyapıları kapsar.

3. Sorumlular

Bu politikanın oluşturulmasında Bilgi İşlem Daire Başkanlığı, Politikanın onaylanmasından BGYS Komisyonu, Politikanın uygulanmasından ise IoT cihazından sorumlu kişiler ve tüm kullanıcılar sorumludur.

4. Tanımlar

Cihaz Kimlik Bilgisi:

Cihazların kimlik bilgileri, genellikle kullanıcı adı, şifre, API anahtarları veya tokenler gibi erişim kontrol mekanizmalarıdır. Bu bilgilerin açık bir şekilde saklanması veya iletilmesi, saldırganların cihazlara yetkisiz erişim sağlamasını kolaylaştırır. Bu nedenle, şifreleme kullanılarak cihaz kimlik bilgilerinin gizliliği korunmalıdır.

Bilgiler, hem dinlenme halinde (cihaz üzerinde depolanırken) hem de iletişim sırasında (cihaz ile sunucu arasındaki veri aktarımı) şifrelenmelidir. Bu sayede cihaz kimlik bilgilerini ele geçirmek isteyen kötü niyetli kişilerin bu verilere ulaşması engellenmiş veya ele geçirilse bile kullanılamaz hale getirilmesi sağlanmış olur.

	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği Politikası		Doküman Kodu	BG. PLTK-16
			İlk Yayın Tarihi	29.05.2025
			Revizyon Tarihi	-
			Revizyon No	00
			Sayfa No	2 / 4
Hazırlayan	Kontrol Eden		Onaylayan	
Bilgi İşlem Personeli	Bilgi İşlem Daire Başkanı		BGYS Komisyonu	

IoT Cihazı:

IoT (Internet of Things) cihazları, otonom bir şekilde çalışabilen, internet üzerinden veri iletimi yapabilen ve genellikle sensörler kullanarak çevrelerinden bilgi toplayıp bu verileri analiz etmek ya da başka cihazlarla paylaşmak amacıyla tasarlanmış cihazlardır. Bazı cihazlar(Örneğin akıllı telefonlar) IoT cihazı olarak tasarlanmamış olsa da üzerine yüklenen yazılımlarla IoT cihazı haline gelebilmektedir.

5. IoT Cihazları:

- Akıllı Sınıf Teknolojileri: Öğrencilerin ve öğretim görevlilerinin etkinliklerini izleyen sensörler ve akıllı tahta teknolojileri. Örneğin, öğrenci katılımını izleyen, ders ortamını daha interaktif hale getiren IoT tabanlı cihazlar.
- Akıllı Bina Sistemleri: Enerji tüketimini izlemek, iklim kontrolü sağlamak ve güvenlik için kullanılan IoT cihazları. Örnek olarak, sıcaklık ve nem sensörleri, ışıklar, güvenlik kameraları, akıllı kapılar.
- Akıllı Kampüs Güvenliği: IoT tabanlı güvenlik kameraları, hareket sensörleri, yüz tanıma sistemleri ve acil durum uyarı sistemleri.
- Akıllı Kütüphane Sistemleri: Kitap takibi, ödünç verme, otomatik raf düzenleme ve içeriği izleme gibi işlemleri gerçekleştiren IoT tabanlı sistemler.
- Laboratuvar ve Araştırma Ekipmanları: Veri toplamak, analiz yapmak ve ekipman durumunu izlemek için IoT cihazları. Örneğin, laboratuvar ortamlarında ölçüm yapan sensörler.
- vb.

6. Kurallar

- Tüm IoT cihazları, güvenli kimlik doğrulama yöntemleri ile korunmalıdır.
- Cihazların kimlik bilgileri, şifreleme ile korunmalı ve varsayılan şifreler değiştirilmelidir.
- IoT cihazları, iletilen ve saklanan verilerin şifrelenmesi için uygun güvenlik protokollerini kullanmalıdır. (Örneğin cihazlar arasındaki veri iletimi HTTPS, SSL/TLS, FTPS gibi

	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği Politikası		Doküman Kodu	BG. PLTK-16
			İlk Yayın Tarihi	29.05.2025
			Revizyon Tarihi	-
			Revizyon No	00
			Sayfa No	3 / 4
Hazırlayan	Kontrol Eden		Onaylayan	
Bilgi İşlem Personeli	Bilgi İşlem Daire Başkanı		BGYS Komisyonu	

protokollerle, kritik verilerin saklandığı hafıza birimleri ise bitlocker veya veracrypt gibi kriptolama yazılımları ile şifrelenmelidir.)

- Hassas veriler, minimum düzeyde toplanmalı ve saklanmalıdır.
- Cihaz yazılımlarının düzenli olarak güncellenmesi ve güvenlik yamalarının zamanında uygulanması zorunludur.
- Cihaz üreticileri, güncellemelerin otomatik olarak veya kullanıcı onayı ile yapılmasını sağlamalıdır.
- IoT cihazları, güvenli ağ protokolleri (ör. WPA3) kullanarak bağlanmalıdır.
- Ağa bağlı cihazlar, güvenlik duvarları ve saldırı tespit sistemleri ile korunmalıdır.
- Kullanıcılar, IoT cihazlarının güvenliği hakkında bilgilendirilmeli ve güvenli kullanım konusunda eğitilmelidir.
- Kullanıcılar, güçlü şifreler oluşturma ve cihaz ayarlarını güvenli hale getirme konularında bilgilendirilmelidir.
- IoT cihazları, güvenlik ihlallerini tespit etmek için sürekli izlenmelidir.
- Güvenlik olayları ve ihlalleri, derhal rapor edilmeli ve gerekli önlemler alınmalıdır.
- IoT cihazlarını ele geçiren saldırganlar cihazın bağlı olduğu ağdan diğer cihazlara da zarar verebileceği için IoT cihazlarına özel ayrı izole ağlar oluşturulmalıdır.
- IoT cihazları, kullanıcıların aktiviteleri, sağlık verileri, konum bilgileri, ses verileri ve daha fazlasını kaydedip internet üzerinden iletme potansiyeline sahip olduğundan kişisel veri ihlaline yol açmamak için bu tür bir işlem yapılmadan önce:
 - İlgili makamlardan mevzuatın gerektirdiği izinler alınmalıdır.
 - Verinin anonimleştirilmesi veya minimal veri toplama ilkesine sadık kalınmalıdır.
 - Kullanıcılara, hangi verilerin toplandığı ve nasıl kullanılacağı hakkında net bilgi verilmelidir.
 - İlgili mevzuat (KVKK, GDPR vb.) doğrultusunda kullanıcı onayı alınmalıdır.

	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği Politikası		Doküman Kodu	BG. PLTK-16
			İlk Yayın Tarihi	29.05.2025
			Revizyon Tarihi	-
			Revizyon No	00
			Sayfa No	4 / 4
Hazırlayan		Kontrol Eden	Onaylayan	
Bilgi İşlem Personeli		Bilgi İşlem Daire Başkanı	BGYS Komisyonu	

7. Yaptırım

Bu politikanın ihlal edilmesi durumunda KTÜN BİLGİ GÜVENLİĞİ POLİTİKASI'nda belirtilen “POLİTİKANIN İHLALİ VE YAPTIRIMLAR” başlığı altındaki maddeler geçerlidir.

8. Yürürlük

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

9. Yürütme

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.