1. **AMAÇ:**

Bu talimatın amacı; Yıldız Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı, fiziksel ve çevresel güvenlik uygulaması kurallarını belirlemektir.

1. **KAPSAM:**

Bilgi Güvenliği kapsamında yürütülen tüm birimleri kapsamaktadır.

1. **UYGULAMA** 
   1. **FİZİKSEL VE ÇEVRESEL GÜVENLİK**

* Hizmet binaları ve çalışanlarımızın güvenliği için tüm güvenlik (güvenlik kamera, kartlı giriş, yangın algılama ve alarm vb.) sistemleri kurulmuştur. BİDB hizmet binasına kartlı girişler sadece erişim izni olan personel tarafından gerçekleştirilmektedir. Ziyaretçiler için kampüs girişi ve BİDB hizmet binası girişlerinde ziyaret kaydı tutulmakta ve girişler güvenlik personeli gözetiminde gerçekleştirilmektedir. Kamera kayıtları ve kartlı geçişler Güvenlik Amirliği tarafından kayıt altına alınmaktadır. Bu kayıtlara istenildiği zaman Güvenlik Amirliği üzerinde ulaşılabilmektedir.
* BİDB hizmet binası İSG kuralları gereğince periyodik olarak ziyaret edilerek risk analizleri gerçekleştirilmektedir. Risk analizinde belirtilen risk faktörlerinin giderilme dereceleri bir sonraki periyodik ziyarette veya ISO 45001 İSG denetimlerinde incelenmektedir.
* Ana sunucu binası girişleri bu alanda görevli personelin bilgisi dahilinde BİDB çalışanları ve/veya üniversitenin sahip olduğu ISO belgeleri gereği (24001, 14001 vs.) yapılacak iç denetimlerde görevlendirilmiş kurum personeli tarafından gerçekleştirilmektedir. Bahsi geçen kişiler dışında sunucu binasına giriş mümkün olmamaktadır. Ana kapı görevli personelin anahtarı ile açılmaktadır. Sunucu binasındaki diğer kapılar ise dışarıdan açılması mümkün olmayacak şekilde tasarlanmıştır. Sunucu binası görevlisinin bulunamaması ihtimali karşı yedek anahtar başka bir personelin erişemeyeceği şekilde saklanmaktadır ve kullanım yetkisi Daire Başkanı bilgisi dahilinde bina sorumlusuna aittir.
* BİDB hizmet ve sunucu binalarında yer alan yangın algılama ve alarm sistemine ait ihbar butonları gereksiz yere kullanılmamalı, duman detektörleri sökülmemeli ve üzerleri duman girişini engelleyecek şekilde kapatılmamalıdır.
  1. Hizmet binalarımızda yer alan kameraların yönleri ve görüş açıları yetkisiz kişilerce değiştirilmemeli, kameraların görüş açıları hiçbir nedenle kapatılmamalıdır. Söz konusu faaliyetlerin gerçekleşmesi durumunda “PR-033-Bilgi Güvenliği İhlal Olayları ve Disiplin Soruşturması Prosedürü” kapsamında işlem yapılacaktır.
  2. **TEÇHİZAT GÜVENLİĞİ**
* BİDB hizmet binası ve sunucu binası altyapı hizmetlerinde kullanılan telekomünikasyon ve enerji sistemleri başta olmak üzere tüm teçhizatın kurulumu için 4/11/1984 tarihli ve 18565 sayılı Resmî Gazete’de yayımlanan Elektrik İç Tesisleri Yönetmeliği hususları dikkate alınır. Söz konusu teçhizatların korunması için pano içi konumlandırılmış koruma röleleri ve sigortaları, topraklama tertibatı ve paratoner tesisatı ile herhangi bir kaçak akım ve olası diğer elektriksel olumsuzluklara karşı korunmaktadır.
* Kurum teçhizatı bakım ve benzeri gerekçeler ile kurum dışına taşınması halinde bakım sözleşmesi imzalanan taraflar sürecin takibi ve sorumluluğunu üstlenmektedir.
* Teçhizat bakımı ihtiyaç halinde Destek Hizmetleri Müdürlüğü Bakım Onarım Birimi tarafından veya teçhizatın bakım sözleşmesine dahil olan ilgili taraflarca gerçekleştirilmektedir. Bakım formlarının bir nüshası Daire Başkanlığı tarafından saklanmaktadır.
* Üniversite dışında teçhizat ve varlık bulunmamaktadır.
* Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımdan önce tüm hassas verilerinin ve lisanslı yazılımlarının kaldırılması veya güvenli bir şekilde üzerine yazılmasından BİDB sorumludur. Hurda malzemeler Destek Hizmetleri tarafından teslim alınmakta ve zimmetten düşülmektedir. Bilgi içeren (hard disk vb.) teçhizatlar imha politikasına göre değerlendirilmektedir.

1. **YAPTIRIM**

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Temsilcisi tarafından e-posta üzerinden yazılı olarak uyarılır. Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3’ten fazla tekrar ederse “PR-033-Bilgi Güvenliği İhlal Olayları ve Disiplin Soruşturması Prosedürü” gereğince kişiler hakkında işlem yapılır. Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, birim amirinin bilgisi dahilinde BGYS Ekibi’ne en kısa sürede bildirme sorumluluğundadır.