1. **AMAÇ**

Bu politikanın amacı, Yıldız Teknik Üniversitesi Bilgi Teknolojileri sistemleri ve uygulamaları tarafından üretilen performans, durum, olay ya da problem bildirimlerinin kayıt altına alınması, sınıflandırılması, değerlendirmesi ve bunlardan yola çıkarak düzenlenecek hata önleme aktivitelerinin gerçekleştirilmesi ile ilgili kuralları tanımlamaktır.

1. **KAPSAM**

Bilgi Güvenliği Yönetim Sistemi faaliyetlerini yürüten tüm birimleri kapsamaktadır.

1. **SORUMLULUK**

Bu dokümandaki görevlerin yerine getirilmesinden tüm Yıldız Teknik Üniversitesi personeli sorumludur.

1. **KISALTMALAR / TANIMLAR**

**Kurum:** Yıldız Teknik Üniversitesi

**BGYS:** Bilgi Güvenliği Yönetim Sistemi

**Bilgi Varlığı:** Kurum için değerli olan ve bu yüzden korunması gereken veri, doküman, sistem vb. unsurları

**Bilgi Güvenliği:** Kurum bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik açılarından korunması

**Güvenlik Olayı:** BGYS’ ye ait tüm politika, prosedür, talimat ve anlaşmalara uyulmama, ters düşme veya bir Kurum varlığının güvenliğinin zarar görmesi durumu

**Varlık Sahibi:** Varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi veya kişilerdir.

1. **UYGULAMA**

**5.1 Bilgi Güvenliği İzleme**

Üniversitemiz bünyesinde bilişim teknolojileri altyapısını oluşturan sistem faaliyetlerine hizmet veren çeşitli marka ve modelde cihazlar kullanılmaktadır. Üniversitemiz faaliyetlerinin gerçekleştirilmesi amacı ile kullanılan cihazlarda oluşan sorunlar ve performans durumlarının izlenmesi ve takibinin merkezi bir noktadan yapılabilmesi amacı İle izleme ve yönetim sistemleri kurulmuş ve gerekli yapılandırma işlemleri gerçekleştirilmiştir. İzleme yönetimi kapsamındaki tüm cihazlar yetkisiz erişimleri engellemek amacıyla hassas yalıtılmış ortam olan sistem odasında tutulmaktadır. Ayrıca sunucular, aktif ağ cihazları, güvenlik cihazları, veri depolama üniteleri, iklimlendirme cihazları, gazlı söndürme, güç kaynağı ve ortam izleme cihazları sistem odasında bulunmaktadır.

**5.2 Bilgi Güvenliği Kayıtları**

Kurum BT sistemlerinde üretilen güvenlik ile ilgili kayıtlar en az aşağıdaki bilgileri içerir ve en az 1 yıl boyunca Bilgi Sistemleri Daire Başkanlığı tarafından saklanır:

* Kullanıcı/istemci kimliği/user ID
* Başarılı ve başarısız giriş - çıkışlar
* Başarılı/başarısız sistem erişimleri denemeleri
* Sistem konfigürasyonu değişikliği
* Ayrıcalıklı hesapların kullanımı (hesap yönetimi, politika değişiklikleri, aygıt konfigürasyonu)
* Sistem araç ve uygulamalarının kullanımı
* Dosya erişimleri ve erişim türü
* Ağ adresleri ve protokolleri
* Koruma sistemlerindeki (IPS, Firewall, Antivirus) değişiklikler (aktivasyon, deaktivasyon, konfigürasyon vb.)
* Dış dünyaya açık kurum web sunucularına gelen istekler için kaynak IP, tarih ve erişilmek istenen adresler

**5.3 Kayıtların Depolanması, İletimi ve Erişimi**

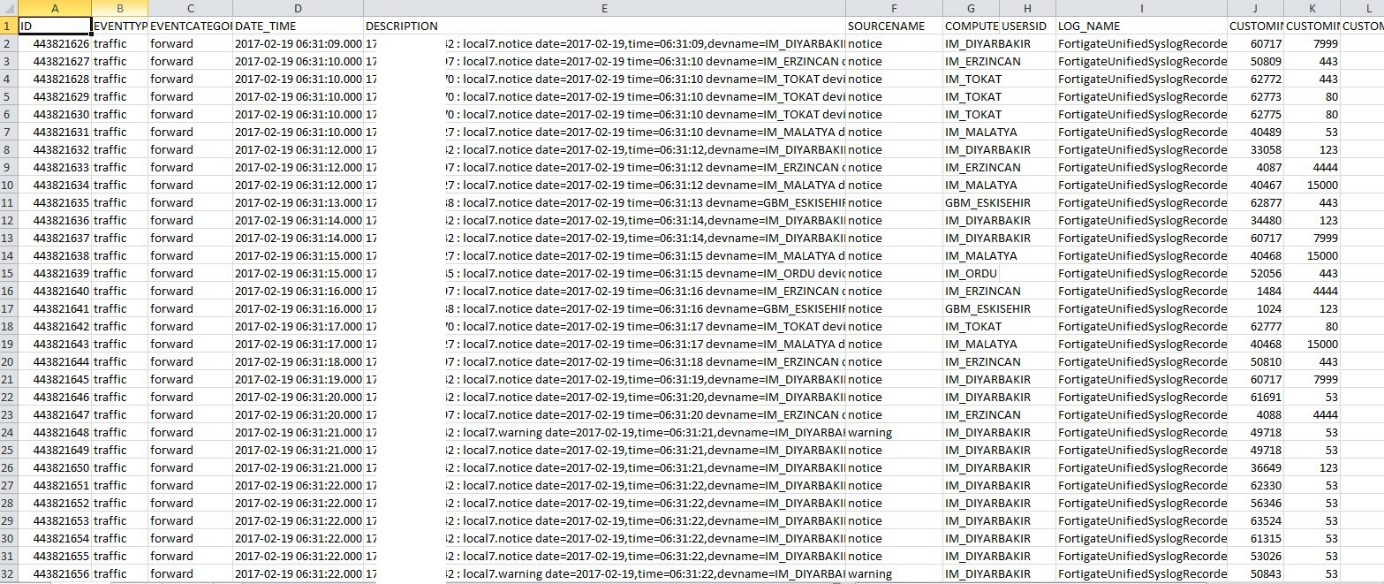
Kayıtlar yedekli yapıda çalışan güvenlik cihazlarının loglarında güvenli olarak saklanır.

* Kayıtlara sadece Bilgi İşlem yetkili personel tarafından erişilir.
* 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi kanununun gerektirdiği tüm kayıtlar saklanır.
* Kayıtların tutulmasını ve yapılandırmanın doğru olup olmadığını Bilgi İşlem kontrol eder.
* Kayıtlar periyodik olarak ve herhangi bir güvenlik olayından şüphelenildiğinde Bilgi İşlem Yöneticisi tarafından incelenir ve uygunsuzluklar üst yönetime rapor edilir.
* Kayıtların takibi aynı zamanda ilgili mevzuata göre yapılmalıdır. Mevzuattaki değişiklikler öncelikli olarak uygulanır.

**5.4 Kayıt Türleri**

**5.4.1** DHCP sunucusunun logları.

**5.4.2** Güvenlik duvarlı logları tutulmaktadır.

****

**5.4.3** Misafir kullanıcıların internet girişleri loglanmaktadır. Burada misafir olan kullanıcının giriş yapabilmesi için, karşısına gelen login ekranında telefon numarasına gelen bir şifreye ihtiyaç vardır.

**5.4.4** Sistem odası giriş çıkış işlemleri loglanmaktadır.

**5.5 Kayıtların İzlenmesi**

Yetkili erişim, ayrıcalıklı işlemler, yetkisiz erişim denemeleri, ağ trafiği, sistem uyarı ve hataları, sistem güvenlik ayarları ve kontrollerinde değişiklikler veya değişiklik teşebbüsleri ile ilgili kayıtlar Bilgi Sistemleri tarafından izlenir. Bu kayıtların saklanma şekli, kontrolü ve gözden geçirme sorumlulukları Bilgi Sistemleri tarafından yerine getirilir. Kayıtların gözden geçirilmesi sırasında tespit edilen olumsuzluklar İletişim ve Bilgi Sistemleri Daire tarafından belirlenir ve bunlarla ilgili alınacak faaliyetler Bilgi Sistemleri tarafından gerçekleştirilir.

**5.6 Saat Senkronizasyonu**

Tüm istemci ve sunucu saatleri, herhangi bir resmi soruşturma durumunda gerekliliği nedeniyle ve sistem denetim kayıtlarının doğruluğunu göstermek amacıyla Türkiye Saatine göre ayarlanır. Bu ayarlama için NTP vb. servisler kullanılır. Saatlerin ileri veya geri alınması uygulamalarına göre saat senkronizasyonu sağlanır.

**5.7 Kayıtların Korunması**

Kayıt sistemleri ve kayıtlar ile ilgili oluşabilecek yetkisiz değişim veya operasyonel problemler ile ilgili önlemler alınır. Tutulan kayıtların değiştirilmesinin önlenmesi Bilgi Sistemleri sorumluluğundadır. Kayıtların silinmemesi veya değiştirilmemesi, kayıtların saklandığı depolama medyalarının kapasitelerinin kontrol edilmesi ve eski kayıtların üstüne yazımın engellenmesi için Bilgi Sistemleri gerekli tedbirlerin alınmasını sağlar. Kayıt bilgilerinin korunmasının en önemli adımlarından biri de yedeklerinin düzenli ve sağlıklı bir şekilde alınmasıdır. Kayıtların yedeklerinin alınmasından Bilgi Sistemleri sorumludur. Kayıt sistemleri periyodik olarak kontrol edilir, herhangi bir uyarı veya sorun varsa rapor edilir ve düzeltici faaliyet başlatılır.

**5.8 Yönetici ve Operatör Kayıtları**

Bilgi Sistemleri ve diğer sistem yöneticilerinin aktiviteleri ile ilgili kayıtlar düzenli olarak tutulur.

Bu kayıtlar aşağıdaki bilgileri içerir:

* Yedekleme zamanları, geri kurtarma, test ve diğer operasyonel faaliyetlerin kayıtları
* Sistem olaylarının başlangıç ve bitiş zamanları ve olaylarda kimlerin yer aldığı
* Sistem hataları (hata bilgisi, tarih, saat) ve yapılan düzeltici faaliyetler
* Değişiklikler, değişikliklerin onay ve uygulama detayları
* Kayıtlar, doğru prosedürlerin takip edildiğinden emin olmak üzere düzenli olarak kontrol edilir ve gözden geçirilir.

**5.9 Hata Kaydı**

Bilgi sistemlerinde meydana gelen olay veya hatalar kayıt altına alınır, hataların giderilmesi için gerekli faaliyetler başlatılır ve hatanın tamamen ortadan kaldırıldığından emin olmak için tekrar kayıtlar incelenir. Sistemlerde hata kaydı (error logging) aktif tutulur. Bu süreç Bilgi Sistemleri tarafından takip edilir.

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.