1. Amaç

Bu politikanın amacı; kurum bünyesinde kullanılan tüm bilgi sistemlerinden üretilen log verilerinin doğru, bütünlüklü, güvenli ve kesintisiz bir şekilde oluşturulması, toplanması, saklanması, işlenmesi, izlenmesi ve gerektiğinde analiz edilmesine ilişkin esasları belirlemektir.

Log yönetimi;

- Siber güvenlik tehditlerinin tespiti,
- Olay müdahale süreçlerinin yürütülmesi,
- Adli bilişim ihtiyaçlarının karşılanması,
- Mevzuat gerekliliklerinin yerine getirilmesi,
- Denetim süreçlerine destek sağlanması

açısından kritik öneme sahiptir.

2. Kapsam

Bu politika; Konya Teknik Üniversitesi'ne ait veya üniversitenin hizmet aldığı tüm bilgi sistemleri ile bu sistemleri yöneten birimleri kapsar.

Politika kapsamına giren varlıklar:

- Sunucular (fiziksel ve sanal)
- Ağ cihazları (router, switch, firewall, access point vb.)
- Uygulama yazılımları ve veri tabanları
- İşletim sistemleri
- Güvenlik bileşenleri (IDS/IPS, WAF, antivirüs, DLP, SIEM vb.)
- Bulut tabanlı hizmetler
- Kullanıcı cihazları (masaüstü, dizüstü, mobil cihazlar)
- Log üreten tüm diğer bilgi teknolojileri bileşenleri

3. Dayanak

Bu politikanın temel dayanağı TS ISO/IEC ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNERGESİ ve ilgili diğer mevzuatlardır.

4. Tanımlar

- **Log (İz Kaydı):** Bilişim sistemlerinde gerçekleştirilen işlemlerin, işlem zamanı (zaman damgası) ile birlikte kaydedildiği veri kayıtlarıdır.
- **Log Yönetimi:** Log verilerinin toplanması, zaman damgası ile ilişkilendirilmesi, güvenli bir şekilde saklanması, işlenmesi ve gerektiğinde raporlanmasını kapsayan süreçler bütünüdür.
- **Log Toplama:** Sunucu, uygulama, ağ cihazı ve diğer kaynak sistemlerden üretilen log verilerinin, gerçek zamanlı veya belirli periyotlarla merkezi bir sistemde toplanması işlemidir.

- **Log Saklama:** Toplanan log verilerinin, bütünlük, gizlilik ve erişilebilirlik ilkelerine uygun olarak, belirlenen süreler boyunca güvenli bir şekilde muhafaza edilmesidir.
- **Zaman Damgası:** Elektronik bir verinin üretildiği tarihi ve değişmezliğini ispatlamak amacıyla, yetkili elektronik sertifika hizmet sağlayıcıları tarafından sağlanan dijital mühürdür.
- **SIEM (Security Information and Event Management):** Log verilerinin analiz edilmesi, güvenlik olaylarının tespit edilmesi ve ilişkilendirilmesi amacıyla kullanılan Güvenlik Bilgileri ve Olay Yönetimi sistemidir.
- **Kullanıcılar:** Konya Teknik Üniversitesi bünyesinde görev yapan tüm personel ve öğrenciler ile kurumsal bilişim sistemlerine erişim yetkisi bulunan geçici kullanıcılar, yükleniciler ve üçüncü taraf hizmet sağlayıcıları ifade eder.

5. Sorumluluklar

5.1 Bilgi İşlem Daire Başkanlığı

- Politikanın uygulanmasını sağlamak.
- Log yönetim altyapısını kurmak, işletmek ve güncel tutmak.
- Logların bütünlüğünü, gizliliğini ve erişilebilirliğini sağlamak.
- Logların saklama sürelerine uyumunu takip etmek.
- Kritik sistem loglarını düzenli olarak incelemek.
- Olay müdahale süreçlerinde log analiz desteği sağlamak.

5.2 Birimler

- Kendi yönetimindeki sistemlerde log tutulmasını sağlamak.
- Gerekli durumlarda log inceleme taleplerini BİDB ile koordine etmek.
- Log oluşturmayı engelleyecek yapılandırmalardan kaçınmak.

6. Log Yönetim İlkeleri

Tüm kurumsal sistemlerde (örneğin sunucular, uygulamalar, ağ cihazları, güvenlik sistemleri ve diğer bilgi teknolojileri bileşenleri) log kaydı tutulması zorunludur. Log kayıtları, bilgi güvenliğinin sağlanması, sistem bütünlüğünün korunması, olay müdahale süreçlerinin yürütülmesi ve mevzuat yükümlülüklerinin yerine getirilmesi açısından kritik öneme sahiptir.
Logların toplanması, güvenli biçimde korunması, izlenmesi, saklanması ve gerektiğinde analiz edilmesi süreçleri, Bilgi İşlem Daire Başkanlığı'nın sorumluluğundadır. Bu kapsamda aşağıdaki esaslar uygulanır:

6.1 Logların Toplanması ve Saklanması

- Tüm log verileri düzenli olarak toplanmalı, merkezi log yönetim sistemine güvenli protokoller aracılığıyla iletilmelidir.

- Logların bütünlüğünün sağlanması için zaman damgası uygulanmalı ve kayıtlar değiştirilmez biçimde saklanmalıdır.
- 5651 sayılı Kanun kapsamında tutulması zorunlu loglar, zaman damgası ile birlikte **en az 2 yıl** süreyle saklanmalıdır.
- Tüm sistemlerde zaman senkronizasyonu (NTP) aktif olmalı ve kurumsal olarak belirlenmiş tek bir zaman kaynağı kullanılmalıdır.
- Logların mümkün olduğunca merkezi bir SIEM veya Log Yönetim Sistemi üzerinde toplanması esastır.
- Konsolide logların düzenli aralıklarla izlenmesi, analizi ve raporlanması yapılmalıdır.

6.2 Logların Korunması ve Güvenliği

- Log kayıtları hiçbir kullanıcı tarafından silinemez, değiştirilemez veya devre dışı bırakılamaz. Bu kural, ayrıcalıklı erişim haklarına sahip kullanıcılar için de geçerlidir.
- Log dosyalarına erişim yalnızca yetkilendirilmiş Bilgi İşlem Daire Başkanlığı personeli tarafından gerçekleştirilebilir.
- Zaman damgası uygulanmış log dosyalarının bütünlüğünü bozacak herhangi bir işlem yapılması kesinlikle yasaktır.
- Log kayıtlarının saklandığı sistemler, fiziksel ve dijital güvenlik kontrolleri ile korunmalıdır (erişim kontrolü, şifreleme, dosya bütünlük kontrolü vb.).
- Loglar şifreli iletişim protokolleri ile iletilmelidir (TLS, SSH vb.).

6.3 Logların Paylaşılması ve Yasal Süreçler

- Bir olay durumunda veya yasal mercilerden gelen talep üzerine, log dosyaları kurum içinde açılmadan, zaman damgalı ve bütünlüğü korunmuş sıkıştırılmış formatta ilgili makamlara iletilmelidir.
- Logların açılması, incelenmesi veya analiz edilmesi sadece olay müdahale ekipleri ve yetkilendirilmiş teknik personel tarafından gerçekleştirilebilir.

6.4 KVKK Kapsamındaki Loglar

- Kişisel veri niteliği taşıyan loglar yalnızca işlendikleri amaçla sınırlı olarak saklanır.
- Mümkün olan durumlarda IP, kullanıcı adı vb. bilgiler maskeleme ile minimize edilir.
- Bu loglara erişim KVKK rol ve yetki prensiplerine göre sınırlandırılır.
- Logların aktarımı ve işlenmesi sırasında kişisel veri güvenliği sağlanır.

6.5 Logların Erişim Yetkisi

- Logları görüntüleme ve inceleme yetkileri görev tanımları ile sınırlıdır.
- Tüm erişimler ayrıca loglanır.

- Yetkisiz erişim şüphelerinde olay yönetimi süreci başlatılır.

6.6 Yedekleme ve Felaket Kurtarma

- Log verileri düzenli olarak yedeklenmeli, güvenli ortamlarda saklanmalı ve yetkisiz erişime karşı korunmalıdır.
- Felaket kurtarma ve iş sürekliliği planları kapsamında log kayıtlarının sürekliliği garanti altına alınmalı, yedekleme ve geri yükleme süreçleri belirli periyotlarda test edilmelidir.

7. Log Kaydı İlkeleri

7.1 Tutulacak Log Türleri

Aşağıdaki olaylara ilişkin logların tutulması zorunludur:

- Sistem erişim kayıtları (login, logout, başarısız giriş denemeleri)
- Yetki değişiklikleri
- Dosya, veri ve sistem değişiklikleri
- Uygulama erişim ve işlem kayıtları
- Ağ trafiği ve güvenlik cihazı logları
- Sistem ve hizmet kesintileri
- Yedekleme, kurtarma ve bakım işlemleri

7.2 Log Formatı

- Loglarda kullanıcı adı, IP adresi, tarih-saat bilgisi (UTC+3), işlem türü, olay açıklaması gibi bilgiler yer almalıdır.
- Logların tutarlılığı için NTP üzerinden merkezi zaman senkronizasyonu yapılmalıdır.

8. Yaptırım

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

9. Yürürlülük

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

10. Yürütme

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.