1. **AMAÇ**

Bu talimatın amacı **Süleyman Demirel Üniversitesi**Kişisel Veri Güvenliği Yönetim Sistemi kapsamında kişisel veri içeren **Süleyman Demirel Üniversitesi** bilgi sistemlerinin oluşturduğu işlem hareketlerinin (Log) sürekli ve düzenli olarak yedeklenmesini sağlayan kuralları belirlemektir.

1. **KAPSAM**

Bu talimat **Süleyman Demirel Üniversitesi** bünyesinde kullanılan tüm kişisel veri içeren bilgi sistemlerini kapsamaktadır.

1. **SORUMLULUKLAR**

Uygulanmasından bilgi işlem birimi sorumludur.

Alınan ve saklanan tüm log kayıtlarına sadece Bilgi İşlem Birimi yetkilisi tarafından erişilebilecektir.

1. **UYGULAMA**
	1. **FIREWALL LOG KONFIGURASYON VE YONETIMI**

Süleyman Demirel Üniversitesibünyesinde kullanılan Firewall içerisinde yapılması gereken işlem adımları aşağıda sıralanmıştır.

* Firewall Cihazı içerisinde log ayarları (Log Setting ) sekmesinden Local Traffic Log seçeneği **Enable All** işaretlenir.
* Firewall Cihazı içerisindeki Event Logging sekmesi içerisinden **Enable All** işaretlenir.
* Yukarıda yapılan işlemler ile tüm iç ve dış trafik aktiviteleri kaydedilmeye başlanmalıdır.
* Kayıt altına alınmaya başlanan trafik kullandığımız cihaz özelliğine bağlı olarak e-posta yolu ile dışarı alınmalıdır. frwl.log@DEMO FİRMA.com.tr üzerine alınan log kayıtları en az 5 yıl süre ile kayıtlı olarak kalmalıdır. (E-posta kota dolması gibi bir sorun ile karşılaşmamak için yedekler aralıklar ile dışarı alınmalıdır.)
* Bir diğer çözüm olarak FORTILOGER, SYSLOG veya 3. Parti bir yazılım ile kayıtların alınması ve yedeklenmesi sağlanmalıdır.
* Alınan tüm kayıtlar her 3 aylık zaman aralıkları içerisinde harici bir disk ve NAS üzerinde ay ve yıl ismi (01-2020frwmailyedek) belirtilerek arşivlenmelidir.
	1. **İNTERNET TRAFİĞİ LOG KONFİGÜRASYON VE YÖNETİMİ**
* 5651 sayılı kanun ve 6698 sayılı KVKK uyarınca tüm internet aktiviteleri kayıt altına alınmalıdır. Kullanılmakta olan **FORTILOGER** üzerinde misafir ve tüm kullanıcıların kayıtları düzenli olarak alınmalı ve bu kayıtlar 5 yıl süresince saklanacak şekilde harici disk ve NAS içine 3 aylık dönemler halinde yedeklenmelidir.
	1. **FILE SERVER LOG KONFİGÜRASYON VE YÖNETİMİ**
* File Server olarak kullanılan sunucu üzerindeki dizin ve dosyalar üzerinde yapılan tüm işlemler kayıt altına alınmalıdır. Windows Server üzerinde birçok kullanıcı işlemi (Audit Logon Events - Audit Account Logon Events vb. ) kayıt altına alınabilmektedir. Sunucu üzerinde gereksiz iş yükü ve büyük log dosyaları oluşturmamak için bizim ihtiyacımız olan hareketleri Audit Object Acces özelliğini yapılandırarak kullanıma almalıyız. (Klasör ve dosyaların, hangi kullanıcı tarafından, ne zaman değiştirildiğini – değiştirilmeye çalışıldığını, okunduğunu – okunmaya çalışıldığını, silindiğini – silinmeye çalışıldığını vb. uygulamış olduğumuz Policy’ ler sayesinde tespit edebiliriz.)
* Sunucu içerisine alınan bu kayıtlar 3 aylık zaman dilimleri halinde NAS ve harici disk üzerine 5 yıl silinmeyecek şekilde kaydedilmelidir.
	1. **DATABASE SERVER LOG KONFİGÜRASYON VE YÖNETİMİ**
* Kişisel ve özel nitelikte verileri kaydettiğimiz Program ara yüzlerinde gözüken kişisel ve özel nitelikteki kişisel veriler maskeleme metodu ile \*\*\*\*\*\* haline getirilmelidir.
	1. **NAS FILE SERVER LOG KONFİGÜRASYON VE YÖNETİMİ**
* Kişisel veri içeren dosyaların NAS üzerinde paylaştırılması durumunda her kullanıcı için ayrı bir kullanıcı adı ve şifre oluşturulmalıdır. Kullanıcıların yetkilendirildikleri dizinler içinde yapacakları tüm düzenleme / silme / ekleme / kayıt hareketleri NAS server üzerinden 3 aylık zaman dilimleri halinde harici disk üzerine 5 yıl silinmeyecek şekilde kaydedilmelidir.
	1. **LOG ANALİZ / RAPORLAMA KONFİGÜRASYON VE YÖNETİMİ**

Öneri : Aşağıdaki ücretsiz yazılımları başlangıç seviyesinde kullanıma başlanıp ilerleyen dönemlerde ücretli sürümlerine geçiş yapılabilir.

### Syslog Server - PRTG ( Free Version ) - [Event Log Consolidator](https://www.solarwinds.com/free-tools/event-log-consolidator?CMP=ORG-BLG-DNS) ( Free Version ) - [SolarWinds Security Event Manager](https://www.solarwinds.com/security-event-manager?CMP=ORG-BLG-DNS) ( Free Version )

### [Kiwi Syslog® Server](https://www.solarwinds.com/free-tools/kiwi-free-syslog-server?CMP=ORG-BLG-DNS) ( Free Version ) - [ManageEngine EventLog Analyzer](https://www.manageengine.com/products/eventlog/) ( Free Version )

### [Graylog](https://www.graylog.org/) ( Open Source)