LEJANT

- Süreç Başlangıcı Faaliyeti — Başlangıç
- Bilgi Sistemlerine Dahil Olmayan Süreç Faaliyeti — Faaliyet
- Bilgi Sistemlerine Dahil Olan Süreç Faaliyetleri:
  - ERYS — Faaliyet
  - Faaliyet
  - Excel — Faaliyet
  - Faaliyet
  - Faaliyet
- Bilgi Sistemlerine Dahil Edilebilecek Süreç Faaliyeti — Faaliyet
- Karar Faaliyeti — Karar
- Yönlendirme — Evet / Hayır
- Kontrol
- Risk
- Performans
- Parametre İşaret Numarası — 1
- Faaliyet Çıktısı — Evrakın Yı...
- Prosedür Bağlantısı — ... Prosedürü
- Talimat Bağlantısı — ... Talimatı
- Süreç Bağlantısı — .... Süreci
- Süreç Sonu Faaliyeti — Son
- Süreç Parametresi Açıklaması — Açıklama Metni
- BT Sistem Veri Kaydı
- Mail Gönderimi
- Çıktı Alınması
- Dosyaların Kargolanması
- Sayfa İçi Referans İşlemleri — Ref.
- Hesap Makinesi İşlemleri
- Dosyayı Elle Taşıma
- Paralel Faaliyetler

SİBER OLAY YÖNETİMİ SÜRECİ

İlgili Birim	Sistem ve Ağ Şube Müdürlüğü	Bilgi Güvenliği Birimi	Dış Paydaş (Siber Tehdit İstihbarat Kaynakları)	Kontrol Noktası	Referans Doküman	Risk	Performans Kriteri	Pozisyon Kodlamaları	İyileştirme Önerileri	Açıklama

Aşama 1

İş Takip Sistemi Veya Eposta Üzerinden Saldırı Bildirilir.

IDS/Firewall Üzerinden Saldırı Tespit Edilir.

Kaynaklar Üzerinden (CULTA, USOM, YÖK Gibi) Olay Bildirimi Gelir.

Takip Sistem ve Ağ Şube Müdürlüğü'ne iletilir.

Tespit edilen veya ihbirlerinde yer alan zararlı bağlantılar, saldırıya konu IP adresleri vb bağlalar IPS sistemi üzerinde filtrelenir veya engellenir.

Log incelenir ve analiz edilir.

Talebe uygun çözüm geliştirilerek güvenlik prosedürleri uygulanır.

Çevrikli not eklenerek İş Takip Sisteminde talep çözümlenir ve kapatılır.

İş Kayıtlı kapatılarak paydaşlara bildirim gönderilir.

Son

K1: Tespit edilen veya bildirilen saldırı bulgularının kontrolü

Üniversite Bilişim Kaynakları Kullanım Politikası

R1: Saldırının engellenememesi sonucu veri ihlali ve kayıp riski

R2: Saldırının engellenememesi sonucu veri sızıntısı riski

R3: Saldırının engellenememesi sonucu kurum itibarının zarar görmesi riski

PR1: Siber olayın doğru bir şekilde yönetilmesi

PR2: Siber olaya zamanında müdahale edilmesi

PR3: Siber olayın engellendiğine dair ilgili paydaşlara zamanında bildirimde bulunulması

P1: Şube Müdürü
P2: Bilgi Güvenliği Yöneticisi
P3: Sistem Mühendisi Uzmanı
P4: Sistem Destek Uzmanı
P5: Network Mühendisi/Uzmanı
P6: Bilgi Güvenliği Sorumlusu/Yöneticisi

Süreç Tipi

Operasyonel / Yönetsel / Destek Süreç

Amaç ve Kapsam

.....