1. AMAÇ

Bu prosedürün amacı, Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamında bilgi güvenliğine yönelik mevcut ve ortaya çıkabilecek tehditlere ilişkin bilgilerin toplanması, analiz edilmesi, değerlendirilmesi, ilgili taraflara aktarılması ve gerekli bilgi güvenliği önlemlerinin alınmasını sağlamaktır.

2. KAPSAM

Bu prosedür; Süleyman Demirel Üniversitesi Daire Başkanlıkları, Genel Sekreterlik ve Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi dahilinde kullanılan bilgi sistemleri, ağlar, sunucular, uç cihazlar, uygulamalar ve Üniversite adına hizmet alınan üçüncü taraf bilgi teknolojileri hizmetlerini kapsar.
Tehdit istihbaratı kapsamında elde edilen bilgiler, yalnızca bilgi güvenliği risklerinin değerlendirilmesi ve gerekli güvenlik önlemlerinin alınması amacıyla kullanılır.

3. SORUMLULAR

- **Bilgi İşlem Daire Başkanlığı:** Tehdit istihbaratı kaynaklarını takip etmek, tehdit bilgilerini değerlendirmek ve gerekli teknik önlemlerin alınmasını sağlamak.
- **İlgili Birimler:** Kendilerini ilgilendiren tehdit bilgilerini değerlendirmek ve gerekli faaliyetleri yürütmek.
- **Kullanıcılar:** Kendilerine bildirilen bilgi güvenliği tehditleri ve alınması gereken önlemlere uygun hareket etmek.

4. UYGULAMA

4.1. Tehdit Bilgilerinin Toplanması

- Bilgi güvenliğine yönelik tehdit bilgileri, güvenilir ve güncel kaynaklardan düzenli olarak takip edilir.
- Tehdit istihbaratı kapsamında aşağıdaki kaynaklardan yararlanılabilir:
  - USOM ve diğer ulusal siber güvenlik kaynakları,
  - Uluslararası CERT/CSIRT kuruluşları,
  - Siber güvenlik kuruluşlarının yayımladığı güvenlik bültenleri ve raporlar,
  - İşletim sistemi, yazılım ve donanım üreticilerinin güvenlik duyuruları,
  - Üniversitenin kullandığı güvenlik ürünlerinden elde edilen bilgiler,
  - Güvenilir sektör ve bilgi güvenliği paylaşım platformları.
- Üniversite bünyesinde kullanılan güvenlik sistemlerinden elde edilen tehdit göstergeleri ve güvenlik olayları da tehdit istihbaratı kapsamında değerlendirilir.

4.2. Analiz ve Değerlendirme

- Toplanan tehdit bilgileri; Üniversitenin bilgi varlıkları, kullanılan teknolojiler, mevcut zafiyetler ve olası etkiler dikkate alınarak değerlendirilir.

- Tehditlerin önem düzeyi, oluşturduğu risk ve Üniversite bilgi varlıkları üzerindeki olası etkileri dikkate alınarak önceliklendirme yapılır.
- Değerlendirme sonucunda gerekli görülen tehdit bilgileri ilgili risk kayıtlarına, zafiyet yönetimi süreçlerine veya diğer ilgili süreçlere aktarılır.
- Kritik veya acil müdahale gerektiren tehditler için periyodik raporlama beklenmeden gerekli önlemler alınır.

4.3. Önlemlerin Alınması

- Değerlendirilen tehditlere karşı gerekli teknik ve idari kontroller belirlenir.
- Gerekli görülmesi halinde;
  - Güvenlik yapılandırmaları güncellenir,
  - Güvenlik yamaları uygulanır,
  - Erişim yetkileri gözden geçirilir,
  - Güvenlik kuralları güncellenir,
  - Kullanıcılara yönelik bilgilendirme yapılır,
  - İlgili güvenlik olayları ve zafiyetler ilgili süreçler kapsamında yönetilir.
- Alınan önlemlerin etkinliği, gerekli görülen durumlarda kontrol edilir.

4.4. Raporlama ve Paylaşım

- Tehdit istihbaratı faaliyetlerinin sonuçları, ihtiyaç ve risk durumuna göre raporlanır.
- Önemli veya kritik tehditlere ilişkin bilgiler, ilgili birimlere zamanında iletilir.
- Tehdit istihbaratı raporları ve kayıtları yetkisiz erişime karşı korunur.

4.5. Periyodik Gözden Geçirme

- Tehdit istihbaratı kaynakları ve takip yöntemleri **en az yılda bir kez** gözden geçirilir.
- Yeni tehditler, teknolojik gelişmeler, güvenlik olayları ve risk değerlendirmeleri doğrultusunda tehdit istihbaratı kaynakları ve uygulamaları güncellenir.

4.6. Gizlilik

- Tehdit istihbaratı kapsamında elde edilen bilgiler, bilgi sınıflandırma kuralları ve ilgili bilgi güvenliği düzenlemelerine uygun şekilde korunur.
- Tehdit istihbaratı bilgilerinin Üniversite dışındaki taraflarla paylaşılması gerektiğinde, ilgili mevzuat, sözleşmeler ve gizlilik yükümlülükleri dikkate alınır.

5. İLGİLİ DOKÜMANLAR

- Güvenlik Açıkları Tespit Etme Politikası

- Risk Yönetimi Prosedürü
- Tehdit İstihbaratı Raporu

6. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	29.09.2025	İlk yayın.
001	16.09.2026	SDÜ EYS yapısına uyum sağlanması, kapsam ve sorumlulukların güncellenmesi, tehdit istihbaratı toplama, değerlendirme, önlem alma, raporlama ve gözden geçirme süreçlerinin yeniden düzenlenmesi.