REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH

1. Amaç

Bu prosedürün amacı, bilgi güvenliği tehditlerini etkili bir şekilde izlemek, değerlendirmek ve yönetmek için gereken adımları belirlemektir. Tehdit istihbaratı, bilgi güvenliği risklerini azaltmak amacıyla güncel ve doğru tehdit bilgilerini toplama ve analiz etme sürecini içerir.

2. Kapsam

Bu prosedür, organizasyonun tüm bilgi güvenliği tehditlerini izleme, analiz etme ve raporlama faaliyetlerini kapsar. Prosedür, Bilgi Güvenliği Yöneticisi ve Bilgi Güvenliği Ekibi tarafından yürütülecektir.

3. Tanımlar

- **Tehdit İstihbaratı:** Bilgi güvenliği tehditleri hakkında bilgi toplama, analiz etme ve değerlendirme süreci.
- **Tehdit:** Bilgi güvenliği üzerinde olumsuz etkileri olabilecek herhangi bir durum veya olay.

4. Sorumluluklar

- **Bilgi Güvenliği Yöneticisi:** Tehdit istihbaratını yönetir, ilgili kaynakları belirler ve gerekli raporlamaları yapar.
- **Bilgi Güvenliği Ekibi:** Tehdit bilgilerini toplar, analiz eder ve uygulama önerileri sunar.

5. Tehdit İstihbaratı Süreci

5.1 Tehdit Bilgilerinin Toplanması

- Tehdit bilgileri, güvenilir iç ve dış kaynaklardan toplanmalıdır. Bunlar şunları içerebilir:
    - Güvenlik raporları ve analizler
    - Endüstri standartları ve uyarılar
    - Güvenlik açıkları ve siber saldırı haberleri
    - Güvenlik forumları ve ağları
- Bilgi toplama süreçleri düzenli olarak gözden geçirilmeli ve güncellenmelidir.

5.2 Tehdit Bilgilerinin Analiz Edilmesi

- Toplanan tehdit bilgileri, organizasyonun bilgi güvenliği riskleri ile ilişkilendirilmeli ve değerlendirilmelidir.
- Analiz, aşağıdaki faktörleri içermelidir:
  - Tehdidin olasılığı
  - Tehdidin potansiyel etkisi
  - Tehdidin mevcut güvenlik kontrolleri ile ilişkisi

5.3 Tehdit Bilgilerinin Değerlendirilmesi

- Analiz sonuçları, bilgi güvenliği risk değerlendirme sürecine entegre edilmelidir.
- Öncelikli tehditler belirlenmeli ve bu tehditlerle başa çıkmak için gerekli önlemler önerilmelidir.

5.4 Tehdit Bilgilerinin Raporlanması

- Elde edilen sonuçlar düzenli olarak raporlanmalı ve ilgili taraflarla paylaşılmalıdır. Raporlar, şunları içermelidir:
  - Tehditlerin tanımlanması
  - Analiz bulguları
  - Önerilen eylemler ve önlemler
  - İlgili risk düzeyleri

5.5 Eylem Planlarının Oluşturulması

- Belirlenen tehditlere karşı uygun eylem planları oluşturulmalıdır.
- Eylem planları, risk azaltma stratejilerini içermeli ve uygulanabilir olmalıdır.

5.6 İzleme ve Gözden Geçirme

- Tehdit istihbaratı süreci düzenli olarak izlenmeli ve gözden geçirilmelidir.
- Süreçteki iyileştirme fırsatları belirlenmeli ve uygulanmalıdır.