

YÖNETİMİN GÖZDEN GEÇİRMESİ PROSEDÜRÜ

1. AMAÇ

Bu prosedürün amacı, Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Yönetim Sisteminin etkin ve sürekli olarak devam ettirilmesi ve bu sistemin Bilgi Güvenliği Yönetim Sistemini politikasına uygunluğunu, yeterliliğini, gelişimini ve sürekli iyileştirme fırsatlarını yakalayabilmesi için planlı periyotlarda veya ihtiyaç duyulan dönemlerde gözden geçirilerek incelenmesi ve değerlendirilmesidir.

- 1.1. Düzenli olarak yılda **en az bir** defa tarihi, saati, yeri ve gündemi 15 gün öncesinden belirlenmek şartı ile Yönetimin Gözden Geçirmesi toplantıları yapılır.
- 1.2. İç Tetkiklerin ve dönemsel ihtiyaçlar nedeni ile gerektiğinde en az 15 gün öncesinden ilan edilmek suretiyle ara dönem Yönetimin Gözden Geçirme Toplantıları yapılabilir.
- 1.3. Toplantıya, Bilgi İşlem Daire Başkanı, Bilgi İşlem Şube Müdürü, BGYS Temsilcisi, katılması talep edilen Bölüm çalışanları ve ilave davetliler katılır.

1.4. YGG Toplantıları gündem maddeleri aşağıdaki gibidir.

1.4.1. ISO 27001:2017 Standardının belirlediği ve görüşülmesini şart koştuğu gündem maddeleri

- BGYS denetimleri ve gözden geçirmelerinin sonuçları,
- İlgili taraflardan edinilen geri bildirimler,
- Kuruluşta BGYS 'nin performansını ve etkinliği artırmak için kullanılacak teknikler, ürünler ya da prosedürler,
- Önleyici ve düzeltici faaliyetlerin durumu,
- Önceki risk değerlendirmede uygun olarak ifade edilmeyen açıklıklar ya da tehditler,
- Etkinlik ölçümlerinin sonuçları,
- Önceki yönetim gözden geçirmelerinden izleme eylemleri,
- BGYS 'yi etkileyebilecek herhangi bir değişiklik ve iyileştirme için öneriler

1.4.2. Yönetimin gözden geçirilmesi toplantılarında aşağıda belirtilen hususlar da ele alınabilir.

- Risk değerlendirme ve risk işleme planını güncelleştirme.
- İş gereksinimleri
- Güvenlik gereksinimleri,
- Düzenleyici ya da yasal gereksinimler
- Anlaşma yükümlülükleri
- Risk seviyeleri ve/veya risk kabul kriterleri
- Artık Riskler
- Kaynak ihtiyaçları
- Kontrollerin etkinliğinin nasıl ölçüldüğünü iyileştirme.

1.5. Toplantıda alınan kararlar **Toplantı Tutanağı Formu** 'na BGYS Temsilcisi tarafından kaydedilir. Planlanan faaliyetlere ilişkin sorumluları belirtilir.

1.6. Yıllık olarak, ilgili raporlar toplantı gündeminde değerlendirilir.

1.7. Toplantı tutanağının katılımcılara ve uygun görülen ilgililere dağıtımı sağlanır. Orijinali BGYS Temsilcisi kontrolünde dosyalanır ve ilgili eklerin arşivde saklanması sağlanır.