1. AMAÇ

Bu politikanın amacı Bilgi Güvenliği olay ihlal süreçlerini belirlemektir.

2. KAPSAM

Bu politika tespit edilen ihlallerin nasıl yönetileceğini kapsamaktadır.

3. SORUMLULUK

Bu politikanın uygulanmasından tüm personeller sorumludur.

4. UYGULAMA

- Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.
- Yaşanan Bilgi Güvenliği olayları bilgi işlem daire başkanlığı siber olaylara müdahale ekibine bildirilmelidir.
- Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
- Bilgi Güvenliği ihlali oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.
- Güvenlik olayının oluşması durumunda ola anında raporlanmalıdır. İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
- Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurmalıdır.
- Tüm Çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor etmelidir.
- Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, DDOs atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlalleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınmalıdır.
- Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınır.
- İç problem analizi, adli incelemeler veya üretici kurumdan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.
- Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.

- Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.
- Kanıt toplama; kuruluş içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;
    - Kanıtın mahkemede kullanıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi, Kanıtın niteliği ve tamlığını gösteren ağırlığı.

5. YAPTIRIM

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ile ilgili maddeleri esas alınarak işlem yapılır.