1. **AMAÇ:** Bu politikanın amacı, bilgi güvenliği ihlal olaylarının sistematik ve hızlı bir şekilde, güvenlik olayları ve açıklıklarının da dahil edilerek, raporlanması ve iyileştirmelerin yönetilmesidir.

2. **KAPSAM:** Tüm KÖKSAN çalışanları, daimi servis sağlayıcıları ve sözleşmeli personel ihlal bildirimi ve iyileştirilmesi kapsamındadır.

3. **TANIMLAR:**

   BGYK: Bilgi Güvenliği Yönetim Kurulu.

4. **SORUMLULAR:**

   - 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 etmekle yükümlüdür.

   - Tüm olay yönetimi ve bilgi güvenliği olayları KÖKSAN BGYK üzerinde yönetilir ve kayıt altına alınır.

   - BGYK ihlal olaylarını izler ve ilgili birim tarafından başarılı bir şekilde sonuçlandırılmasını takip eder.

5. **UYGULAMA:**

   5.1. Bilgi güvenliği olaylarının rapor edilmesi:

   Bilgi güvenliği olayları ve zayıflıkları, zamanında düzeltici önlemlerin alınabilmesi için rapor edilmelidir.

- Güvenlik risklerini azaltmak için tüm şirket çalışanlarının Bilgi Varlıklarında gözlemlenen veya şüphelenilen güvenlik açıklarını veya bu sistemlere yönelik tehditleri BGYK' ye rapor etmeleri gerekir.

- Raporlama belli kurallarda ve bu konuda yayınlanmış politika dikkate alınarak yapılmalıdır.

- Raporlanan Bilgi güvenliği ihlal olaylarına tutarlı ve etkili bir yaklaşım sağlamak için güvenlik olayları ve iyileştirmelerinin sistematik bir yöntemle ele alınması gereklidir.

- 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 durumları mutlaka kayıt altına alınmalıdır.

- Güvenlik olayının oluşması durumunda ertelenmeden 5N1K prensibine uygun olarak en kısa sürede aşağıdaki bilgiler bulunacak şekilde raporlanmalıdır;

    - ❖ Neden – İhlal olayının Sebebi
    - ❖ Ne – İhlal olayının kısa tanımı
    - ❖ Nasıl – İhlal olayının nasıl olduğu
    - ❖ Nerede – İhlal olayının gerçekleştiği birim yada kurum
    - ❖ Ne Zaman- İhlal olayının ne zaman gerçekleştiği
    - ❖ Kim – İhlal olayını kimin gerçekleştirdiği

- Bilgi güvenlik olayı raporlarının bildirilmesi aşağıda belirtilen aşamalarda gerçekleştirilir:

a. Bilgi varlığının kaybolması,

b. Bilgisayar, telefon, tablet vb. bilgi işleme araçlarının anormal çalışması (yavaş, farklı uyarılar, ısınma, açılmaması ve her zamankinden farklı çalışması vb.),

c. İhlalin gerçekleştiğine dair objektif delillere rastlanılması (açık bırakılan kapılar, dolaplar ve çekmeceler vb.),

d. Beklenmeyen bir kaza sonucunda varlığın zarar görmesi,

e. Bilgi Güvenliğini etkileyeceğini düşündüğünüz her türlü anormal durumda aşağıdaki raporlama kanallarından biri kullanılabilir:

- BGYK (Bilgi Güvenliği Yönetim Kurulu)'na;
    - e-posta: bgyk@koksan.com
    - Telefon no : **1909** ,**1912** (Şirket dahili)

- Raporlama kayıt işlemi File Server üzerinde bulunan Fr-Bt-45 Siber Olay Bildirim ve Değerlendirme Formu üzerine yapılır. Herhangi bir şekilde sistemi etkileyecek bir olay durumunda Raporlama KÖKSAN BGYK olarak QDMS sistemi üzerinden DÖF (Düzeltici ve Önleyici Faaliyet) açılarak BGYK Temsilcisine ulaşır. BGYK Temsilcisi sorunu analiz ederek, güvenlik uyarılarının ve uyarı mesajlarının sorumlu birimlerce ele alınıp bertaraf edilmesi için, sorumlu birimlere aktarır.

5.2. İhlal Bildirim Yönetimi

- Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci bgyk@koksan.com mail adresine gönderilmelidir.

- Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, DOS atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler acilen 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 firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.

- Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi konuları dikkate alınır.

- Bilgi güvenliği olaylarının değerlendirilmesi sonucunda aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecek kayıt yapısı oluşturulmalıdır.

5.3. Kanıt Toplama ve Disiplin

- Güvenlik ihlaline neden olanlar hakkında ihlalin kuruma etkisi ve büyüklüğüne göre çalışanlar için disiplin, üçüncü taraflar içinse hukuki süreç başlatılır.

- İhlali yapan kullanıcı yada üçüncü taraf tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

- Güvenlik ihlaline neden olan Kurum içerisinde disiplin faaliyeti için delil toplanırken uygulanacak genel kurallar şunlardır;

  - ❖ Kanıtın disiplin cezası için yada mahkemede kullanılıp kullanılamayacağı ile ilgili kabul edilebilirlik derecesi,
  - ❖ Kanıtın niteliği ve kesinliğini gösteren bilgiler,
  - ❖ Bilgi güvenliği ihlallerine karışılması, politika, prosedür ve talimatlarına uyulmaması halinde, İnsan Kaynakları Disiplin Yönetmeliğinin ilgili maddesi gereği işlem yapılır.

6. KURALLAR:

6.1. -

7. KAYITLARIN SAKLANMASI:

7.1. Tüm kayıtlar, **'Dökümante edilmiş bilgi Prosedürü'** ne göre saklanır.

8. İLGİLİ DOKÜMANLAR:

'Dökümante edilmiş bilgi Prosedürü'
'Siber Olay Bildirim ve Değerlendirme Formu'