BİLGİ İŞLEM GENEL MÜDÜRLÜĞÜ
BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Bu politikanın amacı, Kurum içi bilgi güvenliğinin sağlanması amacıyla iş gereksinimlerinin ilgili yasalara ve düzenlemelere göre belirlenmesi, Kurum envanterinde bulunan sistem, bilgi ve insan kaynağı varlıklarının gizlilik, bütünlük ve erişilebilirliğinin sağlanması maksadıyla Güvenlik Kurulu'nun bilgilendirilmesi ve desteğinin sağlanmasıdır.

2. KAPSAM

Bu politikanın kapsamı aşağıdaki maddelerde belirtildiği gibidir:

- BGYS-P-04:Bilgi Güvenliği Yönetim Sistemi Kapsam Prosedüründe yer alan lokasyonlar.
- Bilgi İşlem Genel Müdürlüğü çalışanları.
- Destek hizmetleri kapsamında çalışan gerçek ve/veya tüzel üçüncü kişiler.
- Kurum dahilinde hizmet veren bilgi ve bilgi işleme varlıkları.

3. SORUMLULAR

Bu politikanın hazırlanmasından ve revize edilmesinden Bilgi Güvenliği Şubesi, uygulanmasından ise kapsam başlığı altında belirtilen tüm çalışanlar sorumludur.

4. TANIMLAR VE KISALTMALAR

BİGM/Kurum **:** Bilgi İşlem Genel Müdürlüğü
BGYS **:** Bilgi Güvenliği Yönetim Sistemi
Prosedür **:** Bir işte uyulması, tutulması gereken yol ve yöntemlerin tümü
Politika **:** Bilgi Güvenliğinin sağlanması adına oluşturulan ve minimum gereksinimlerin belirtildiği çerçevedir.

5. UYGULAMA

5.1 Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Yönetim Sistemi; bilgi güvenliğini inşa etme, işletme, izleme ve geliştirerek sürdürme yaklaşımını temel alan yönetim sistemi bölümüdür. Yönetim sistemi kurumun yapısını, politikalarını, faaliyetlerini, sorumluluklarını, uygulamalarını, prosedürlerini, süreçlerini ve kaynaklarını içerir. BGYS'nin kapsamını varlıklar, sistemler, uygulamalar, veri iletişim ağları ve araçları ile bilginin oluşturulması, işlenmesi, kullanımı, saklanması ve gerektiğinde bilgiye ulaşım şeklini belirler. Bilgi güvenliği yönetim sistemi; yasal düzenlemelere uyumu kolaylaştırır, kurumun verimliliğini artırır, iş sürekliliğini sağlar, kurumun yapısının daha iyi anlaşılmasına yardımcı olur ve sonuç olarak kurumsal itibarı artırır.

Adalet Bakanlığı BİGM Bilgi Güvenliği Yönetim Sistemi, Bilgi Güvenliği Politikası ve bağlı diğer prosedür ve talimatlarla tanımlanmış esaslar ve sorumluluklar doğrultusunda gerçekleştirilir ve sürekli olarak iyileştirilir.

Bilgi Güvenliği Yönetim Sisteminin oluşturulmasını, sürdürülmesini ve etkinliğini temin etmek üzere, doğrudan Genel Müdür'e bağlı olarak görev alan ve BGYS ile ilgili sorunların çözümü için Kurum içinde gerekli bağımsızlığa ve yetkiye sahip olan Yönetim Temsilcisi Genel Müdür tarafından belirlenir. Yönetim Temsilcisi en üst seviyede BGYS uygulamalarına liderlik eder ve bağlılık gösterir.

Bilgi Güvenliği Şubesi bilgi güvenliği konusunda bilgi seviyesini ve kurum içi farkındalığı geliştirmeli, güncel tutmalı, bilgi güvenliğine yönelik saldırı ve tehditlere karşı erkenden haberdar olup önlem almalıdır. Bilgi güvenliği teknolojileri ve ürünleri ile ilgili yeni gelişmeleri takip etmek ve bilgi güvenliği olaylarının üstesinden gelmek için uygun irtibat noktaları geliştirmek amacıyla üzerine düşen görev ve sorumlulukları yerine getirir.

5.2 Bilgi Güvenliği Politikası

Bu politika, BİGM kapsamındaki hizmetlerin ve varlıkların güvenilirliğini, sürekliliğini ve sürdürülebilirliğini sağlamayı amaçlar. Bu doğrultuda aşağıdaki temel ilkelerin yerine getirileceğini taahhüt ve beyan eder.

- Bilgi güvenliği ile ilgili yasalar ve düzenlemelere göre Genel Müdürlük Makamı bilgilendirilerek ve desteği alınarak tüm Bilgi Güvenliği süreçlerinin sürdürülebilir olması sağlanır.
- Bilgi Güvenliği organizasyonunun rolleri ve sorumlulukları tanımlanır, uygulanması sağlanır ve düzenli kontrolleri yapılır.
- İstihdam öncesinde, çalışma süresince, istihdamın sonlandırılması veya değiştirilmesinde, bilgi güvenliğine ilişkin çalışanları yasal yönden bağlayıcı önlemler alınır ve kişilerin iş tanımlarına göre bilgi güvenliği sorumlulukları kendilerine tebliğ edilir.
- Kurumun bilgi ve bilgi işleme olanakları ile ilgili varlık envanteri oluşturulur, sorumluları belirlenir ve kullanıma dair kurallar belirlenip istihdam sonunda iadesi sağlanır.
- Bilgi ve bilgi kaynağı önem derecesine göre sınıflandırılır, etiketlenir ve oluşturulan prosedürlere göre kullanımı sağlanır.
- Bilgi varlıklarında depolanan bilginin güvenli bir şekilde saklanması, taşınması, bozulmaya karşı yedeklenmesi ve ihtiyaç kalmadığı durumda güvenli bir şekilde imhası sağlanır.
- **BGYS-POL-09 Erişim Kontrol Politikasına** göre bilgi ve bilgi varlıklarına izinsiz erişimlere, bilginin yetkisiz kullanımına ve bilgiye zarar verilmesine karşı önleyici tedbirler alınır. Bilgi varlıklarına erişim "Bilmesi Gereken" ve "En Az Haklar" ilkelerine göre sağlanır.
- Personel, çalışma alanlarında **"Temiz ekran/Temiz masa"** prensibine uygun olarak davranır. Kişiye özel veya gizli bilgilerin başkaları tarafından görülmesine imkân verilmeyecek şekilde önlemler alır.
- Bilginin gizliliği, değişmezliği ve bütünlüğünü korumak amacıyla kriptografi yöntemleri uygulanır.
- Bilgi ve bilgi varlıklarına yetkisiz kişilerin fiziksel erişimlerini önleme amacıyla kontrol noktaları ve fiziksel güvenlik seviyesine uygun olarak yalıtılmış ortamlar oluşturulur.
- Bilgi varlıklarını çevresel tehditlerden korumak amacıyla destekleyici alt yapı hizmetleri, fiziksel güvenlik, periyodik bakım ve imha süreçleri uygulanır.
- Sistemde işleyişi etkileyecek değişiklikler **BGYS-P-08 Bilgi Güvenliği Sürekliliği Prosedürüne** göre izlenir. Geliştirme, test ve işletim ortamları birbirinden ayrılır. Kaynakların kullanımı sürekli izlenerek kapasite takibi yapılır.
- Bilgi varlıklarının zararlı yazılımlara karşı korunması sağlanır.
- Veri kaybını önlemeye yönelik yedekleme sistemleri, olay kaydetme ve izleme mekanizmaları oluşturulur ve güvenli bir şekilde saklanarak gereği halinde kanıtlar toplanır.
- İşletimsel sistemlerin bütünlüğünü sağlamak amacıyla yazılım kurulum kontrolleri yapılır. Tespit edilen açıklıklar için tedbirler alınır.
- Ağdaki bilgi ve bilgi varlıklarını korumak amacıyla yetkili personel tarafından ağ kontrolleri yapılır. Sisteme erişim sağlayan personelin yetkileri aylık periyotlar ile varlık sahibi tarafından kontrol edilir ve gerekli güvenlik önlemleri alınır.
- Dış varlıklarla yapılan bilgi transferleri, politika ve prosedürlere göre kontrol altına alınır. Dış taraflar ile **"BGYS-TAH-01 Gizlilik Anlaşması**" ve "**BGYS-TAH-02 Bilgi Koruma Taahhütnamesi**" imzalanır.
- Bilgi güvenliği kapsamında bilginin oluşumu, transferi, işlenmesi ve saklanması süreçlerinde uçtan uca gizlilik, bütünlük ve ulaşılabilirlik daimi olarak sağlanır.
- Tedarikçiler tarafından erişilen bilgi varlıklarının güvenliği karşılıklı imzalanacak **"BGYS-TAH-01Gizlilik Anlaşması"** ile güvence altına alınır.
- Bilgi Güvenliği ihlal olayları raporlanır, değerlendirilir, ihlal olup olmadığına karar verilir ve koruyucu, önleyici, tekrar etmesini engelleyici tedbirler alınır.
- BİGM çağrı hizmetleri **"BGYS-P-19 Çağrı Merkezi Bilgi Güvenliği Prosedürüne"** uygun olarak hizmet verir.
- Kurum içerisinde oluşturulan tüm yazılımlara ait kaynak kodları sadece yetkili kişilerin erişim sağlayabildiği, parola ile korunan dijital veri kasasında saklanır.

- BİGM bünyesindeki alt birimlerce uygulanmakta olan prosedürlerin bilgi güvenliği politikalarına uygun olup olmadığı ilgili yöneticiler tarafından denetlenir.
- Bilgi güvenliği politikaları, belirli aralıklarla veya önemli değişiklikler ortaya çıktığında sürekli uygunluk ve etkinliği sağlamak amacıyla gözden geçirilir.