SGK BİLGİ TEKNOLOJİLERİ GENEL MÜDÜRLÜĞÜ
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

BİLGİ GÜVENLİĞİ POLİTİKASI

ONAYLAYAN
BTGM GENEL MÜDÜRÜ

DOKÜMAN KONTROL

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
BGYS Sorumlusu	Bilgi Güvenliği Yönetim Temsilcisi	Genel Müdür

DEĞİŞİKLİK KAYITLARI

Tarih	Hazırlayan	Sürüm	Değişiklik Referansı
23.11.2020	Oktay YILMAZ	2	Bilgi Güvenliği ilkeleri, sorumluluklar, eklenmiştir. Bilgi güvenliği ve güvenlik ihlali tanımı yapılmıştır

1. AMAÇ

- SGK Bilgi Teknolojileri Genel Müdürlüğü'nün bilgi güvenliğini yönetmekteki amacı; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden ve/veya dışardan gelebilecek, kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunması ve iş süreçlerinde etkin, doğru, hızlı ve erişim yetkileri gözetilerek güvenli bir biçimde kullanılmasıdır.

- Bilgi güvenliği politikasının amacı ise, iş sürekliliğini sağlamak ve potansiyel tehditlerin etkisini azaltmak için bilgi güvenliği olaylarını engellemek veya mevcut riskleri en aza indirmektir.

2. KAPSAM

- SGK Bilgi Teknolojileri Genel Müdürlüğü Bilgi Güvenliği Politikası, SGK Bilgi Teknolojileri Genel Müdürlüğünün uygulamalarını, hizmetlerini sunduğu Bilgi İşlem Merkezlerinin insan kaynaklarını, bilgi varlıklarını, fiziksel varlıklarını ve yazılım varlıklarını kapsar.

- SGK Bilgi Teknolojileri Genel Müdürlüğü kapsamındaki süreçlerde üretilen ve/veya kullanılan tüm bilgilerin her durumda mutlak bütünlüğünün sağlanacağını, ilgili tüm bilgilerin yönetileceğini ve uygun bir gizlilik prosedürü çerçevesinde korunacağını garanti eder.

3. POLİTİKA

- SGK Bilgi Teknolojileri Genel Müdürlüğü bilgiyi sahip olduğu varlıklar içerisinde en değerlisi olarak kabul eder. Bilgi; iş faaliyetlerimizin sürdürülebilmesi açısından kritik önem taşır ve uygun bir şekilde korunması gerekir.

- Bilgi Teknolojileri Genel Müdürlüğü, ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardını uygulayarak kurumsal biginin Gizlilik, Bütünlük ve Erişilebilirlik ile ilgili ortaya çıkabilecek riskleri belirlemeyi ve bu risklerin etkilerini en aza indirmeyi amaçlar.

- Bilgi Teknolojileri Genel Müdürlüğü için Bilgi Güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana gelir.

  - Gizlilik, SGK'da, sigortalı, emekli ve hak sahipleri, sağlık hizmet sunucuları ya da üçüncü taraflara ait olup olmasına bakılmaksızın üretilen ve/veya kullanılan her türlü bilginin gizliliğinin her durumda güvence altına alındığını ifade eder.

- Bütünlük, bilginin yetkisiz kişiler tarafından değiştirilmemesi, bilgilerin bütünlüğünün her durumda korunmasını ifade eder.

- Erişilebilirlik, iş süreçlerinin gereksinimi olarak her türlü bilginin, en az kesintiyle kapsam dahilindeki birimler, sigortalılar, emekliler, hak sahipleri, sağlık hizmet sunucuları ve gereken üçüncü taraflarca ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir olmasını ifade eder.

❖ SGK Bilgi Teknolojileri Genel Müdürlüğü tarafından kullanıcılara sağlanan sistemlere erişim esnasında kullanılan şifrelerle ilgili kriterler Şifre Kullanım Politikası ile belirlenir.

❖ Uygun erişim kontrolünün sağlanmasını ve bilginin yetkisiz erişime karşı korunması Erişim Politikası ile gerçekleştirilir.

❖ Risk Değerlendirme ve Yönetimi Prosedürü ile Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesinin takibi gerçekleştirilerek, bilgi varlıklarına yönelik risklerin tespiti ve sistematik bir şekilde yönetilmesi, mevcut risklerin kabul edilebilir düzeylere indirilmesi sağlanır.

❖ Kişisel Verilerin Korunması Yasasında belirtilen önlemler başta olmak üzere, Türkiye Cumhuriyeti yasaları, yönetmelikler, genelgeler, sözleşmeler ile belirlenmiş gereksinimler karşılanır, Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlanır.

❖ İş Sürekliliği Yönetimi ve İş Sürekliliği Planı ile kritik iş süreçlerini salgın, deprem, sel baskını vb. büyük felaketlerin ve işletim hatalarının etkilerinden korumak amaçlanır.

❖ Personelin bilgi güvenliği farkındalığını arttıracak ve sistemin işleyişine katkıda bulunmasını teşvik edecek eğitimler düzenli olarak verilir.

❖ Güvenlik ihlallerinin derhal rapor edilmesi, ihlal nedenlerinin araştırılarak gerekli önlemlerin alınması ve ihlal olaylarının en aza indirilmesi esastır. Bilgi Güvenliği İhlal Olaylarının Raporlanma Talimatı ile Bilgi güvenliğine dair gerçek ya da şüpheli tüm ihlallerin rapor edilmesi; tekrar etmesini engelleyici önlemlerin alınması amaçlanır.

❖ Çalışma alanlarında, “Temiz Masa/ Temiz Ekran” prensiplerine uygun olarak, tasnif dışı özellikteki bilgiler dışında bilgilerin, başkalarınca görülmesine imkan verilmeyecek şekilde önlemler alınması, bu konu ile ilgili gerçekleşebilecek zaafiyetin ortadan kaldırılması amaçlanır.

❖ Fiziksel ve Çevresel Güvenlik Prosedürü ile SGK Bilgi Teknolojileri Genel Müdürlüğü bünyesinde bulunan güvenli alanların ve hizmet binalarının fiziksel ve çevresel güvenliği sağlanır.

❖ E-posta Kullanım Politikası ile SGK çalışanları tarafından kullanılmakta olan eposta servisinin erişim ve kullanım yetkileri ile ilgili yazılı kural ve yöntemler tanımlanır.

03.02.2021 tarih ve E-41646129-020-19642054 sayılı Genel Müdürlük Oluru ile elektronik olarak imzalanmıştır.

- SGK BTGM tarafından kullanıcılara sağlanan tüm sistemlere erişim için kullanılan şifreler Şifre Kullanım Politikası ile belirtilen esaslara göre belirlenir ve kullanılır.

- Art Niyetli Yazılımlarla Mücadele Talimatı ile personelin olağandışı ya da şüpheli olan her konuyu "Bilgi Güvenliği İhlal Olaylarının Raporlanması Talimatı"na uygun olarak yetkililere bildirmesi sağlanır.

- Uzaktan Erişim Politikası ile SGK BTGM'nin ağına uzaktan erişim yapmakla yetkilendirilmiş kişilerin uyması gereken kurallar belirlenir.

- Bilgi varlıklarının, gizlilik derecelerine göre sınıflandırılması ile bilginin gizliliği ve bütünlüğü sağlanır.

- İnsan Kaynakları Güvenliği Prosedürü, SGK Bilgi Teknolojileri Genel Müdürlüğü bünyesinde görev yapan her statüdeki personelin, birimlerde geliştirilen uygulamaların bilgi güvenliği ihlaline ilişkin görev, yetki ve sorumluluklarını kapsar.

- BGYS politikasını desteklemek için, bilgi güvenliği ile sınırlı kalmayacak şekilde tüm politika, prosedür, talimat, form, liste ve sözleşmeler SGK Intranet portalında yer alacak ve elektronik ortamda bilmesi gereken prensibi çerçevesinde erişilebilir olacaktır. Tüm bu dokümanlar oluşturulurken yasalar, endüstri düzenlemeleri, uluslararası standartlar ve sözleşmeler dikkate alınacaktır.

BİLGİ GÜVENLİĞİ İLKELERİ

Bilgi Teknolojileri Genel Müdürlüğü,

- Vatandaşlara ve paydaşlarına sunduğu hizmetlere ilişkin faaliyetlerin güvenliğinin sağlanmasını

- Bilgi güvenliği kontrollerinin iş süreçleri ile entegre, uyumlu ve dengeli olmasını

- Vatandaşlara ve paydaşlarına sunduğu hizmetlerin gizlilik, bütünlük ve erişilebilirliğini tehdit edebilecek risklere karşı önleyici politikalar

- Bu politika ile uyumlu bilgi güvenliği hedefleri belirlemeyi ve düzenli aralıklarla uyumluluğunu ölçerek, sürekli iyileştirmeyi

İlke edinir.

SORUMLULUKLAR

03.02.2021 tarih ve E-41646129-020-19642054 sayılı Genel Müdürlük Oluru ile elektronik olarak imzalanmıştır.

- **İş Geliştirme Daire Başkanlığı (Bilgi Güvenliği Yönetim Temsilcisi),** Bilgi Güvenliği ile ilgili genel yönetim çerçevesinin oluşturulmasından ve sürekliliğinin sağlanmasından ve bu politikanın, güncel olarak yaşamasını ve Bilgi Teknolojileri Genel Müdürlüğü'nün işle ilgili gerekliliklerini veya bilgilerinin ve bilgi sistemlerinin karşı karşıya olduğu risk ortamındaki ya da tehditlerdeki değişimleri yansıtmaya devam etmesini temin edecek şekilde devamlı gözden geçirilmesinden sorumludur.

- Gerekli olduğunda bu politikanın ayrıntılı standartlar, prosedürler ve süreçlerle desteklenmesini ve bunların gerek doğdukça kullanıma hazır olmasını sağlayacaktır. Ayrıca bu politika gereklerinin tüm çalışanlara (daimi veya dönemsel) ve tüm yüklenici personeline aktarılmasını sağlamaktan sorumlu olacaktır.

- Bu politikanın ve tüm standartların ve diğer destekleyici belgelerin işlevsel sahipliği **İş Geliştirme Daire Başkanlığı (Bilgi Güvenliği Yönetim Temsilcisi)** tarafından yürütülecek ve bu yöneticilik, aynı zamanda politikanın tüm Bilgi Teknolojileri Genel Müdürlüğü bünyesinde uygulanmasıyla ilgili olarak tavsiye kaynağı ve rehber olacaktır.

- Bilgi Teknolojileri Genel Müdürlüğü Bilgi Güvenliği Politikaları, kadrolu ya da sözleşmeli olsun, kuruma ait bilgi veya iş sistemlerini kullanan tüm çalışanlar için geçerli ve zorunludur. Bilgi Teknolojileri Genel Müdürlüğü bilgilerine erişim gereği olan üçüncü taraf hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır.

ÇALIŞANLARIN SORUMLULUKLARI

- Bilgi Teknolojileri Genel Müdürlüğü personeli, konumları veya görevleri ne olursa olsun işlerini, bilgilerin Bilgi Teknolojileri Genel Müdürlüğü bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur.

- Bilgi Güvenliği Politikası ilkeleri, SGK Personel Yönetmeliği Kurallarıyla birlikte uygulanmalıdır. Çalışanlar ayrıca Bilgi Güvenliği Politikasının farkında olmaktan ve bu ilkelere uymaktan sorumludur.

DENETLEME VE POLİTİKALARA UYUM

- Daire Başkanları Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetlemekten birinci derece sorumludur.

- İş Geliştirme Daire Başkanlığı, başta Bilgi Güvenliği Politikası olmak üzere yayınlanmış olan tüm politika ve prosedürler ile ilgili standartlara uyumun periyodik olarak denetiminden ve ilgililere raporlanmasından sorumludur.

03.02.2021 tarih ve E-41646129-020-19642054 sayılı Genel Müdürlük Oluru ile elektronik olarak imzalanmıştır.

HEDEFLER

T.C. Sosyal Güvenlik Kurumu Bilgi Teknolojileri Genel Müdürlüğü'nün saygınlığının, güvenilirliğinin ve emanetinde bulunan bilgi varlıklarının korunması, mevcut iş ve işlemlerinin en az kesinti ile sürekliliğinin sağlanması amacıyla,

- Bilgi sistemleri faaliyetlerinin sürekliliğini tam olarak sağlamayı,
- Çalışanların Bilgi Güvenliği Konusundaki farkındalık düzeylerini en üst seviyeye çıkarmayı,
- Üçüncü taraflar ile yapılan sözleşmelere uygunluğun tam olarak tesis edilmesini sağlamayı,
- Bilgi güvenliği ihlal olaylarını en aza indirmeyi ve bunları öğrenme fırsatına çevirmeyi,
- Bilginin yasalara tam uyumlu üretilmesini, erişim sağlanmasını ve korunmasını,
- En güncel ve etkin teknik güvenlik kontrolleri uygulamayı hedefler.

Her bir SGK Bilgi Teknolojileri Genel Müdürlüğü çalışanı bu hedeflere katkı sağlamaktan sorumludur.

YAPTIRIM

- Bilgi Güvenliği Politikası ihlalleri, SGK'nın risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Dolayısıyla söz konusu ihlal aynı zamanda 657 sayılı Devlet Memurları Kanununun ihlali olup disiplin cezası sonucunu doğurabilir. Gerek gözetim, gerek denetim, gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlalleri uyarı, kınama cezalarına hatta Adli ve Cezai yasal işlemler başlatılmasına varıncaya kadar gidebilecek kurum içi disiplin cezaları ile sonuçlanabilecektir.

- Bu politikanın uygulanması konusunda hep birlikte çalışılması, bilgilerimizin ve itibarımızın sürekli olarak korunmasına ve işimizin başarısının devamlılığının sağlanmasına yardımcı olacaktır.

GÖZDEN GEÇİRME

- Bilgi Güvenliği Politikası yılda bir kez, Yönetimin Gözden Geçirme (YGG) toplantılarında gözden geçirilir. Gözden geçirme verileri Bilgi Güvenliği Yönetim Temsilcisi tarafından oluşturulur. Gözden geçirilen ve güncellenen Bilgi Güvenliği Politikası, SGK Bilgi Teknolojileri Genel Müdürü tarafından onaylandıktan sonra, SGK kurumsal web adresinde yayınlanır.

- Yeni riskleri ve risklerde meydana gelen değişiklikleri kontrol altında tutmak için Bilgi Güvenliği Yönetim Sistemi dokümanları güncellenerek, sürekli iyileştirilmektedir. Güncel Dokümanlar **SSOM platformunda "Bilgi Güvenliği Yönetim Sistemi (BGYS)" uygulaması** altında yayınlanmaktadır.

03.02.2021 tarih ve E-41646129-020-19642054 sayılı Genel Müdürlük Oluru ile elektronik olarak imzalanmıştır.