1. AMAÇ

Bu politikanın amacı; Kurumun sahip olduğu veya sorumluluğunda bulunan bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin korunması, bilgi güvenliği risklerinin etkin şekilde yönetilmesi, bilgi güvenliği ihlallerinin önlenmesi ve kurumsal faaliyetlerin güvenli ve sürdürülebilir şekilde yürütülmesine ilişkin temel ilke ve esasları belirlemektir.

Bu Politika, Kurumun Bilgi Güvenliği Yönetim Sisteminin (BGYS) temel çerçevesini ve bilgi güvenliğine ilişkin yönetim yaklaşımını ortaya koyar.

2. KAPSAM

Bu politika; Kurumun merkez ve taşra teşkilatını, Kurum personelini, Kurumun sahip olduğu veya sorumluluğunda bulunan her türlü bilgi ve belgeyi, bilgi sistemlerini, uygulamaları ve bilişim altyapısını, fiziksel ve elektronik bilgi işleme ortamlarını, Kurum bilgi varlıklarına erişim sağlayan yüklenici, tedarikçi, danışman, stajyer ve diğer ilgili tarafları kapsar.

3. SORUMLULUKLAR

Üst Yönetim: Bu politikanın onaylanmasından, bilgi güvenliği yönetiminin desteklenmesinden ve BGYS' nin etkin şekilde yürütülmesi için gerekli kaynakların sağlanmasından sorumludur.

Bilgi Güvenliğinden Sorumlu Birim: BGYS faaliyetlerinin koordinasyonu, bilgi güvenliği risk ve kontrollerinin takibi, ilgili dokümanların güncelliğinin izlenmesi, farkındalık faaliyetlerinin yürütülmesi ve bilgi güvenliği performansının takip edilmesine ilişkin görevleri yürütür.

Birim Yöneticileri: Sorumluluk alanlarındaki bilgi varlıklarının korunmasını, erişimlerin görev ve yetkilerle uyumlu olmasını ve personelin bilgi güvenliği gerekliliklerine uygun hareket etmesini sağlar.

Tüm Personel ve İlgili Taraflar: Kendilerine bildirilen bilgi güvenliği politika, prosedür, talimat ve kurallarına uymak, kendilerine tahsis edilen bilgi varlıklarını korumak ve bilgi güvenliği olaylarını belirlenen yöntemlerle bildirmekle yükümlüdür.

4. TANIMLAR VE KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi’ni,

Kurum: Gençlik ve Spor Bakanlığı’nı,

TS EN ISO/IEC 27001: Kuruluşların bilgi varlıklarını güvenli bir şekilde yönetmesini ve korumasını sağlayan uluslararası Bilgi Güvenliği Yönetim Sistemi standardını,

YGG: Yönetimin Gözden Geçirmesini ifade eder.

5. UYGULAMA

5.1. Bilgi Güvenliği Yaklaşımı

Kurum, bilgi güvenliğini; kurumsal faaliyetlerin ve hizmetlerin güvenli, etkin ve sürdürülebilir şekilde yürütülmesinin temel unsurlarından biri olarak kabul eder.

Bilgi güvenliğinin sağlanmasında bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması esastır. Bilgi güvenliği; insan, süreç ve teknoloji unsurlarını kapsayan, risk temelli ve bütüncül bir yaklaşımla yönetilir.

Bu kapsamda Kurum;

- Bilgi varlıklarını ve bunlara ilişkin güvenlik gereksinimlerini belirlemeyi,
- Bilgi varlıklarının uygun şekilde sınıflandırılmasını ve korunmasını,
- Bilgi güvenliği risklerini sistematik olarak belirlemeyi, değerlendirmeyi ve yönetmeyi,
- Risklerin kabul edilebilir seviyelere indirilmesi amacıyla uygun teknik ve idari güvenlik kontrollerini uygulamayı,
- Bilgiye erişimi görev, yetki, bilmesi gereken ve en az ayrıcalık prensipleri doğrultusunda sınırlandırmayı,
- Görevler ayrılığı ilkesini gözetmeyi,
- Bilgi güvenliği olaylarını önlemeye, tespit etmeye, müdahale etmeye ve etkilerini azaltmaya yönelik mekanizmalar oluşturmayı,
- Bilgi sistemlerinin ve kritik hizmetlerin sürekliliğini sağlamayı,
- İlgili mevzuat, standart, rehber ve sözleşmesel yükümlülüklere uymayı,
- Personelin ve ilgili tarafların bilgi güvenliği farkındalığını geliştirmeyi,
- Bilgi Güvenliği Yönetim Sisteminin uygunluğunu, yeterliliğini ve etkinliğini izlemeyi ve sürekli iyileştirmeyi

bilgi güvenliği yönetiminin temel esasları olarak benimser.

5.2. Bilgi Güvenliği Temel İlkeleri

Kurumda bilgi güvenliğinin sağlanmasında aşağıdaki temel ilkeler esas alınır:

Gizlilik: Bilginin yalnızca yetkili kişiler, süreçler ve sistemler tarafından erişilebilir olması sağlanır.

Bütünlük: Bilginin doğruluğu, tamlığı ve güvenilirliği korunur; bilginin yetkisiz veya kontrolsüz şekilde değiştirilmesi önlenir.

Erişilebilirlik: Bilginin ve bilgi sistemlerinin ihtiyaç duyulduğu zamanda yetkili kullanıcılar tarafından erişilebilir ve kullanılabilir olması sağlanır.

Bilmesi Gereken Prensibi: Bilgiye erişim, kişinin görev ve sorumluluklarını yerine getirebilmesi için ihtiyaç duyduğu bilgi ile sınırlandırılır.

En Az Ayrıcalık Prensibi: Kullanıcılara görevlerini yerine getirebilmeleri için ihtiyaç duydukları asgari erişim yetkisi verilir.

Görevler Ayrılığı: Hata, yetkisiz işlem ve kötüye kullanım risklerini azaltmak amacıyla kritik görev, yetki ve sorumlulukların mümkün olduğu ölçüde ayrıştırılması sağlanır.

5.3. Bilgi Güvenliği ve Risk Yönetimi

Kurum, bilgi güvenliğinin sistematik ve sürdürülebilir şekilde yönetilmesi amacıyla Bilgi Güvenliği Yönetim Sistemini kurar, uygular, sürdürür ve sürekli iyileştirir.

Bilgi güvenliği riskleri; Kurumun faaliyetleri, bilgi varlıkları, teknolojik altyapısı, yasal ve düzenleyici yükümlülükleri ile ilgili tarafların gereksinimleri dikkate alınarak belirlenir, analiz edilir, değerlendirilir ve işlenir.

Risklerin değerlendirilmesinde bilginin gizlilik, bütünlük ve erişilebilirlik gereksinimleri ile tehditler, zafiyetler, gerçekleşme olasılığı ve muhtemel etkiler dikkate alınır.

Risklerin kabul edilebilir seviyelere indirilmesi amacıyla uygun teknik ve idari kontroller belirlenir, uygulanır ve etkinlikleri izlenir.

5.4. Bilgi Güvenliği Kontrolleri ve Alt Düzenlemeler

Bu politika, Kurumun bilgi güvenliği yönetimine ilişkin çatı politika niteliğindedir.

Politikada belirlenen temel ilke ve esasların uygulanmasına yönelik ayrıntılı düzenlemeler; ilgili riskler, mevzuat, standartlar ve kurumsal ihtiyaçlar doğrultusunda oluşturulan alt politikalar, prosedürler, talimatlar, planlar, rehberler, formlar ve diğer tamamlayıcı dokümanlarla belirlenir.

Bu kapsamda ihtiyaçlar doğrultusunda gerekli tamamlayıcı düzenlemeler oluşturulur. Alt düzenlemeler bu politika ile uyumlu olmak zorundadır.

5.5. Bilgi Güvenliği Farkındalığı

Bilgi güvenliğinin sağlanması tüm çalışanların ortak sorumluluğudur.

Kurum personelinin ve gerekli görülen ilgili tarafların bilgi güvenliğine ilişkin görev ve sorumluluklarını bilmesi ve güvenlik farkındalığının geliştirilmesi amacıyla eğitim, bilgilendirme ve farkındalık faaliyetleri gerçekleştirilir.

Personel, kendisine bildirilen bilgi güvenliği politika, prosedür, talimat ve diğer kurallara uymak ve karşılaştığı veya şüphelendiği bilgi güvenliği olaylarını belirlenen yöntemlerle bildirmekle yükümlüdür.

5.6. Mevzuat ve Diğer Gerekliliklere Uyum

Bilgi güvenliği faaliyetlerinin ilgili mevzuata, TS EN ISO/IEC 27001 gerekliliklerine, Bilgi ve İletişim Güvenliği Rehberine, sözleşmesel yükümlülüklere ve Kurumun iç düzenlemelerine uygun şekilde yürütülmesi esastır.

Bilgi güvenliğine ilişkin mevzuat, standart, rehber ve diğer gerekliliklerde meydana gelen değişiklikler takip edilir ve gerekli durumlarda BGYS ve ilgili dokümanlar güncellenir.

5.7. Yönetimin Taahhüdü

Üst Yönetim; BGYS' nin kurulmasını, uygulanmasını, sürdürülmesini ve sürekli iyileştirilmesini, bilgi güvenliği amaçlarının Kurumun amaçları ve faaliyetleriyle uyumlu olmasını, bilgi güvenliği

risklerinin sistematik şekilde yönetilmesini, bilginin gizlilik, bütünlük ve erişilebilirliğinin korunmasını, ilgili yasal, düzenleyici ve sözleşmesel yükümlülüklere uyulmasını, BGYS' nin etkin şekilde işletilmesi için gerekli kaynakların sağlanmasını, bilgi güvenliği görev, yetki ve sorumluluklarının belirlenmesini, bilgi güvenliği farkındalığının geliştirilmesini, BGYS performansının izlenmesini, değerlendirilmesini ve sürekli iyileştirilmesini taahhüt eder.

5.8. İzleme, Gözden Geçirme ve Sürekli İyileştirme

Bilgi Güvenliği Yönetim Sisteminin uygunluğu, yeterliliği ve etkinliği; bilgi güvenliği hedefleri, risk değerlendirmeleri, iç ve dış denetimler, bilgi güvenliği olayları, performans sonuçları, test ve kontroller ile yönetimin gözden geçirme faaliyetlerinden elde edilen sonuçlar doğrultusunda izlenir ve değerlendirilir.

Tespit edilen uygunsuzluklar ve iyileştirme ihtiyaçları için gerekli faaliyetler planlanır ve takip edilir.

Bu politika yapılan işe uygunluk açısından sürekli olarak, her halükârda yılda bir kez YGG toplantısından önce gözden geçirilir. Mevzuat ve standart değişiklikleri, önemli organizasyonel veya teknolojik değişiklikler, risk değerlendirme sonuçları, önemli bilgi güvenliği olayları ve denetim bulguları politikanın gözden geçirilmesinde dikkate alınır.

Kurum, Bilgi Güvenliği Yönetim Sisteminin uygunluğunu, yeterliliğini ve etkinliğini sürekli iyileştirmeyi esas alır.

5.9. Duyuru

Bu politika, üst yönetim tarafından onaylanmasının ardından Kurum personeline ve gerekli görülen ilgili taraflara uygun iletişim kanalları aracılığıyla duyurulur ve erişilebilirliği sağlanır.

6. UYUM VE YAPTIRIM

Bu politika ile politika kapsamında oluşturulan alt politika, prosedür, talimat ve diğer bilgi güvenliği düzenlemelerine uyulması zorunludur.

Bilgi güvenliği kurallarına aykırı davranışlar ve bilgi güvenliği ihlalleri; olayın niteliği, kapsamı ve ilgili kişinin hukuki statüsü dikkate alınarak ilgili mevzuat, sözleşmeler ve Kurum içi düzenlemeler çerçevesinde değerlendirilir.

İhlalin niteliğine göre gerekli idari, disiplin, hukuki veya sözleşmesel işlemler uygulanabilir.

7. İLGİLİ DOKÜMANLAR

- TS EN ISO/IEC 27001:2022 BİLGİ GÜVENLİĞİ YÖNETİM STANDARDI
- BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ