BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ ve KAPSAM

Bu politika, BİLGİ TEKNOLOJİLERİ VE HABERLEŞME KURUMU'nun iş sürekliliğini sağlamak ve güvenlik ihlal olaylarından doğan zararların ve riskin en aza indirilmesini amaçlamaktadır.

Bu politika BTHK'nın Bilgi Güvenliği Yönetim Sistemini, çalışanlarını ve iş fonksiyonlarını kapsar.

2. SORUMLULAR

- Bu politika BTHK Başkanı tarafından onaylanmıştır ve "Bilgi Güvenliği Politikası"nın uygulanmasının sağlanması, denetiminin yapılması ve güvenlik ihlallerinde gerekli yaptırımın uygulanması konusundaki desteğinin bir ifadesidir.

- Tüm BTHK çalışanları ve gerekli görüldüğü hallerde iş ortakları, tedarikçiler ve müşteriler bu politikadaki maddelere uymakla yükümlüdür.

- Bilgi güvenliğinin yönetiminden, denetiminden, politikaların oluşturulmasından ve onaylanmasından Bilgi Güvenliği Kurulu sorumludur.

- Güvenlik ihlal olaylarının araştırılması, soruşturulması ve gerekli önlemlerin alınması Bilgi Güvenliği Yöneticisi'nin (Yönetim Temsilcisi) sorumluluğundadır.

- Bilgi güvenliğini ilgilendiren tüm konularda politikaları, standartları ve kılavuzları oluşturmak, bunların uygulanmasını koordine etmek ve denetlemekten Bilgi Güvenliği Kurulu sorumludur.

- Politikaların uygulanması sırasında takip edilecek talimatları oluşturmak, süreçleri tasarlandığı şekliyle işletmek ve gerekli kurumsal kayıtları oluşturmak ilgili birimlerin görevidir ve çalışanların direkt sorumluluğudur.

3. REFERANSLAR

ISO 27001:2013

4. TANIMLAR VE KISALTMALAR

BGK: Bilgi Güvenliği Kurulu
BGYS: Bilgi Güvenliği Yönetim Sistemi
BTHK: Bilgi Teknolojileri ve Haberleşme Kurumu

5. UYGULAMA

5.1. Bilgi Güvenliği Tanımı

Bu politikada "Bilgi Güvenliği", Kurum'un bilgi varlıklarının aşağıdaki özelliklerinin korunması olarak tanımlanır:

- Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması.
- Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması.
- Erişebilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması.

5.2. Bilgi Güvenliği Politikasının Hedefleri

BTHK yönetimi, bu politikanın uygulanması ile

- Yasal zorunluluklara uymayı,
- Güvenlik olaylarından doğan her türlü gelir veya fırsat kaybını en aza indirmeyi,
- Kurumun imajını ve güvenilirliğini korumayı,
- Kendisi ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişim sağlamayı,
- Bilginin erişebilirliğini, bütünlüğünü ve gizliliğini korumayı,
- Kendisinin ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi,
- Bilgi güvenliği ihlali durumunda gerekli görülen yaptırımları uygulamayı,
- Tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, ilgili mevzuat ve standart gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimleri sağlamayı,
- İş/Hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmayı ve işin sürekliliği ve sürdürülebilirliğini sağlamayı,
- Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi,
- Bilgi güvenliği farkındalığını arttırmak amacıyla yetkinlikleri geliştirecek eğitimleri sağlamayı,

Hedeflemektedir.

5.3. Bilgi Güvenliği Politikası

- BTHK'da işlenen, saklanan ve taşınan her türlü bilginin bir sahibi olacaktır ve bu bilgiye erişim hakkı ve gizlilik derecesi sahibi tarafından belirlenecektir.
- Bilgi varlıkları ile bu bilgiyi işleyen, saklayan veya taşıyan tüm diğer varlıklara (donanım, yazılım, personel, altyapı ve destek hizmetler) ilişkin güncel bir Varlık Envanteri oluşturulacaktır.
- Varlık Envanteri'nde yer alan tüm bilgiler sınıflandırılacaktır.
- Bilgiye erişim, "en az erişim hakkı" prensibi ile sadece "bilmesi gerekene" verilecektir ve yetkisiz erişim engellenecektir.
- Çalışanlar veya ziyaretçiler, sahibinin onayı olmadan, hiçbir bilgiyi BTHK fiziksel veya mantıksal sınırları dışına çıkartamaz.

- BTHK'nin risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, Risk Değerlendirme prosedürü tanımlandığı şekilde yapılmasından Bilgi Güvenliği Kurulu sorumludur.
- Güvenlik ihlal olayları ve politikaların bilinçli veya bilinçsiz olarak uygulanmaması durumları Bilgi Güvenliği Kurulu'na bilgi güvenliği ihbar portalinden veya mail yoluyla bildirilecektir.
- İş sürekliliği ve felaketten kurtarma planlaması yapılacaktır.
- Kritik tüm sistemler ve BTHK için önemli olan bütün bilgiler düzenli olarak yedeklenecektir ve yedekleme talimatı ve ilgili geri dönüş planları oluşturulacaktır.
- Kapsam içindeki bilgi ve sistemleri barındıran tüm coğrafi lokasyonlar, barındırdıkları sistemlerin bilgi sınıflandırması ile doğru orantılı olarak fiziksel güvenlik önlemleri ile korunacaktır.
- Tüm personelin, görevinin gereği ölçüsünde bilgi güvenliği konusunda eğitim alması sağlanacaktır. Farkındalık ve bilinçlendirme eğitimleri düzenlenecektir.
- Bilgi güvenliği yönetim sistemi iç ve dış denetimi yılda en az bir kere, teknik güvenlik denetimleri ise ihtiyaç duyulan sıklıkta dış kaynaklarla gerçekleştirilecektir.
- BTHK bilgi güvenliği politikası ve diğer alt politikalar ISO/IEC 27001 doğrultusunda oluşturulacaktır.
- Tüm BTHK çalışanları, iş ortakları ve tedarikçileri, bilgi işlem kaynaklarını K.K.T.C yasalarına aykırı faaliyetler yürütmede kullanamaz ve yasalarda bilişim güvenliğine yönelik yer alan maddelere uymakla yükümlüdür.
- Bilgi güvenliği politika veya talimatlarına uyulmaması halinde disiplin süreci başlatılabilir. Disiplin sürecinin sonucunda, uyarı, kınama, para cezası ve sözleşme feshi gibi cezalar uygulanabilir.

6. İLGİLİ BELGELER

- ISO/IEC 27001:2013

Kadri BÜRÜNCÜK
Başkan