KALİTE YÖNETİM SİSTEMİ

Bilgi Güvenliği

Bilgi Güvenliği Yönetim Sistemi Politikası

Sürüm No: 8.0

Yayın Tarihi: 09.04.2018

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

444 0 545

Standartlar

ISO 27001: Bilgi Güvenliği Yönetimi Sistemi Standardı

ISO 22301: İş Sürekliliği Yönetimi Sistemi Standardı

ISO 20000: Bilgi Teknolojileri Hizmet Yönetim Sistemi Standardı

CMMI Level 3: Bütünleşik Yetenek Olgunluk Modeli - Seviye 3

© 2012 Kamu İhale Kurumu

Tüm hakları saklıdır. Bu dokümanın hiçbir bölümü Kamu İhale Kurumu'nun izni alınmadan, hiçbir biçimde ve hiçbir yöntemle çoğaltılamaz ve dağıtılamaz, veri tabanı ya da başka bir sistemde saklanamaz.

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

ONAY

09 / 04 / 2018

Cevat ASLANBAŞ

Elektronik İhale Dairesi Başkanı

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

İÇİNDEKİLER

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

1. GİRİŞ

1.1 Amaç ve Hedef

Bu dokümanın amacı Kamu İhale Kurumu'nda uygulanan Bilgi Güvenliği Yönetim Sisteminin (BGYS) oluşturulması için genel çerçevenin çizilmesidir.

Bu doküman BGYS'deki tüm doküman ve aktiviteler için kaynak niteliğindedir.
BGYS Kapsam dokümanında tanımlanan, Elektronik İhale Dairesi (EİD) tarafından sağlanan bilişim hizmetlerindeki tüm elektronik ve fiziksel varlıkların bilgi güvenliğini aşağıda belirtilen maddeler doğrultusunda sağlamayı hedefler.

- Kurum tarafından üretilen, kullanılan, geliştirilen ve EİD tarafından yönetilen bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak.
- Kurumun sunmuş olduğu elektronik platformlar üzerinden gerçekleşen tüm ihale süreçlerinin şeffaflığını ve güvenirliliğini sağlamak.
- Kurumun temel ve destekleyici iş faaliyetlerinin güvenli ve en az kesinti ile devam etmesini sağlamak.
- Temsil ettiği makamın güvenilir imajını korumak.
- Kurumun tabi olduğu mevzuat, yasa ve yönetmeliklere uyumluluğu sağlamak.
- Paydaşlar ve üçüncü taraflarla yapılan sözleşmelere uygunluğu sağlamak.

1.2 Kapsam

Bilgi Güvenliği EİD bilgi varlıklarının aşağıdaki özelliklerinin korunması olarak tanımlanır:

Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması,

Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması,

Erişilebilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması.

Kamu İhale Kurumu Türkiye'de kamu ihale süreçlerinin tümünü elektronik ortama taşıyarak ihale süreçlerini şeffaflaştırmayı ve süreçleri kolaylaştırmayı amaçlamaktadır. Bu nedenle Kurum bünyesinde kullanılan ve kullanılması planlanan elektronik ortamdaki bütün bilgiler değer kazanmaktadır. Bu bilgilerin güvenliğinin sağlanması Kurum, ihaleye teklif veren istekli ve idareler için yüksek önem arz etmektedir. Bu bilgilerin yetkisiz kişilerin eline geçmemesi, ilgili bilginin değiştirilmemesi ve ihtiyaç halinde sadece yetkili kişiler tarafından erişilebilir olması bir zorunluluktur.

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

BGYS, EİD tarafından yönetilen tüm iç ve dış uygulamalar ile Elektronik Kamu Alımları Platformu (EKAP) projelerini ve bu projelerde kullanılmakta olan tüm bilgi varlıklarını kapsamaktadır. BGYS Kapsamı, BGYS Kapsam dokümanında detaylandırılmıştır.

1.3 Geçerlilik ve Yürürlük

Bu doküman Kurum Yönetimi tarafından onaylandığı tarihten itibaren geçerlidir.

Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler dokümanın gözden geçirilmesini gerektirir.

1.4 Kısaltmalar ve Tanımlar

BGYS: ISO/IEC 27001 standardına uygun olarak yürütülen Bilgi Güvenliği Yönetim Sistemi

EİD: Elektronik İhale Dairesi

KİK: Kamu İhale Kurumu

EKAP: Elektronik Kamu Alımları Platformu

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

2. GENEL BİLGİLER

Uygulanabilir Değil

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

3. ESASLAR/İLKELER

3.1 Risk Yönetim Çerçevesi

Bilgi güvenliği, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik boyutları açısından korunmasıyla sağlanmaktadır. Bilgilerin etkileşimde bulunduğu varlıklar ile ilgili açıklıklar, bu açıklıklara yönelik tehditler ve bu tehditlerin gerçekleşme olasılığı ile gerçekleşmesi sonucunda oluşacak zararın önlenmesi veya en aza indirilmesi için yapılacakların planlanması EİD risk yönetim yaklaşımı olarak tanımlanır. Risk yönetimi, EİD bilgi varlıkları için geçerli olan risklerin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Bilgi Güvenliği Yönetim Sistemi; Risk Değerlendirme Kılavuzu, Risk Değerlendirme Raporu Dokümanı, Risk İşleme Planı Dokümanı, Risk Yönetimi Kural Dokümanı ve Uygulanabilirlik Bildirgesi Dokümanı bilgi güvenliği risklerinin nasıl kontrol edileceğini tanımlar. Risklerin yönetimi ve işlenmesinin takibinden Bilgi Güvenliği Koordinasyon Kurulu sorumludur.

3.2 Yönetimin Bilgi Güvenliğini Sağlama Sözü ve Politika Dokümanının Onayı

Kurum Yönetimi, EİD tarafından oluşturulmuş olan Bilgi Güvenliği Politikasının ve diğer BGYS kurallarının uygulanmasını, devamlılığının sürdürülmesini ve denetlenmesini desteklemektedir. Bu politikaya personel, paydaş ve üçüncü taraflarca uyulmaması durumunda, "Kamu İhale Kurumu Disiplin Amirleri Yönetmeliği" dokümanında ve/veya sözleşmelerde belirtilen yaptırımlar uygulanacaktır.

3.3 Roller/Görevler ve Sorumluluklar

BGYS kapsamındaki temel rol ve sorumluluklar aşağıda tanımlanmıştır:

- Kapsam dâhilindeki tüm Kurum personeli, paydaş ve üçüncü taraflar Bilgi Güvenliği Politikasına ve BGYS'de tanımlanan kural ve süreçlere uymak zorundadır.
- Kapsam dâhilindeki tüm personel güvenlik olaylarını, fark edilen güvenlik açıklıklarını ve güvenlik kuralları ihlallerini en kısa sürede Bilgi Güvenliği Yöneticisine raporlamaktan sorumludur.
- BGYS'nin yönetiminden Bilgi Güvenliği Yöneticisi, devamlılığının sağlanmasından ve gözden geçirilmesinden Bilgi Güvenliği Koordinasyon Kurulu ve Kurum Yönetimi sorumludur.
- Bilgi Güvenliği Koordinasyon Kurulu bilgi güvenliği politikasının uygulanmasını sağlar ve gözden geçirir.
- Kurum Yönetimi çeşitli kurallar ve süreçler ile bu politikanın uygulanmasını destekler.
- Bilgi varlıklarının gizlilik, bütünlük, erişilebilirliğinin korunmasından varlık sahipleri sorumludur.

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

- Bilgi varlıklarının gizlilik, bütünlük, erişilebilirlik ve sınıflandırma ile ilgili gereksinimleri varlık sahipleri tarafından belirlenir.
- EİD'nin bilgi kaynakları izinsiz olarak paydaş ve üçüncü kişiler ile paylaşılamaz.
- Tüm çalışanların bilgi güvenliği bilincini arttırmak için belirli aralıklarla proje ekibince farkındalık eğitimlerinin verilmesi sağlanır.

3.4 Politikanın İhlali ve Yaptırımlar

BGYS kapsamında oluşturulmuş kural ve süreçleri ihlal eden personel, paydaş ve üçüncü taraflar için ilgili sözleşmelerde yer alan ve "Kamu İhale Kurumu Disiplin Amirleri Yönetmeliği" dokümanında uygulamaları belirtilen aşağıdaki yaptırımlardan bir veya birden fazlasının uygulanması önerilebilir. Bu uygulamanın yürütülmesinden Bilgi Güvenliği Koordinasyon Kurulu sorumludur.

- Uyarma
- Kınama
- Para cezası
- Sözleşme Feshi

3.5 Bilgi Güvenliği Politikası Gözden Geçirme Kuralları

Bilgi Güvenliği Politikası, periyodik olarak yılda bir kez Bilgi Güvenliği yönetim Temsilcisi ve ilgili taraflar ile gözden geçirilir ve üst yönetimin onayı ile yayımlanır. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Bu tür durumlarda periyodik gözden geçirme tarihi beklenmeden politikanın gözden geçirmesi gerçekleştirilir. Gözden geçirilen ve güncellenen politika Kurum Yönetimi tarafından onaylanır. Onaylanan politika Kurum internet sitesi ve intranet sitesinde yayımlanır.

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

4. KAYNAKLAR/REFERANSLAR

- ISO/IEC 27001, ISO 22301 standartları
- Mevzuat ve Kanunlar

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA

5. EKLER

Uygulanabilir Değil

Hacettepe Üniversitesi Teknokent Yerleşkesi,
Kamu İhale Kurumu Binası 1596. Cadde, No:8
06800 Beytepe/Çankaya / ANKARA