HACETTEPE ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI

BGYS-PL-01
BİLGİ GÜVENLİĞİ POLİTİKASI

İlk Yayın Tarihi: 14.02.2014

KURUMA ÖZEL

** Sadece kurum çalışanlarının görebileceği, kurum dışı kişilerin görmemesi gereken dokümanlar bu sınıfta yer alır.*

*** Elektronik Nüsha, Çıktısı Kontrolsüz Dokumandır.*

REVİZYON KAYITLARI

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No
1	05.01.2018	BGYS Yöneticisi	ISO referansları başlığı ve tablosu kaldırıldı. /Sayfa 2 "ISO/IEC 27001:2005" ifadesi "ISO/IEC 27001:2013" olarak değiştirildi./ Sayfa 5,7
2			
3			
4			
5			
6			
7			
8			
9			
10			

İçindekiler

KISALTMALAR TABLOSU

Kısaltma	**Tanım**
Kurum	Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı
BGYS	Bilgi Güvenliği Yönetim Sistemi
Envanter	Kurum için önem arz eden her türlü bilgi varlığı
Üst Yönetim	Hacettepe Üniversitesi Yönetimi

1. Amaç

Kurum bünyesinde çalışanlar ve ilgili tarafların uyması gereken bilgi güvenliği şartlarının çerçevesini çizmek ve yazılı kuralları belirlemek.

2. Kapsam

Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde bulunan bilgi sistemleri varlıklarını ve bu varlıklara erişim sağlayan Bilgi İşlem Daire Başkanlığı birim çalışanları ve bu birimlerin iş süreçlerini kapsar.

Aşağıda verilen konumdaki çalışma ortamları BGYS sertifikası kapsamındadır.

Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı 06800 Beytepe / ANKARA
Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı Sıhhiye Birimleri 06100 Sıhhiye / ANKARA

3. Bilgi Güvenliği Nedir?

Bilgi, diğer önemli kurum varlıkları gibi, kurum için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği iş sürekliliğini sağlamak, kayıpları en aza indirmek için tehlike ve tehdit alanlarından korur.

Bilgi güvenliği, bu politikada aşağıdaki bilgi niteliklerinin korunması olarak tanımlanır:

Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek,

Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek,

Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

Bilgi güvenliği politikası dokümanı, yukardaki korumaları ve gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır. Bilgi Güvenliği Politikası ve Bilgi Güvenliği kapsamında hazırlanan her türlü doküman kapsam dâhilinde yer alan tüm kişilerin uyması gereken esasları içermektedir.

4. Bilgi Güvenliği Hedefleri

Bilgi Güvenliği Politikası, Kurum çalışanına, kurumun güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini artırmak ve bu şekilde kurumda

oluşabilecek riskleri minimuma indirmek, kurumun güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, teknik güvenlik kontrollerini uygulamak, kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla kurumun tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını korumayı hedefler.

5. Bilgi Güvenliği Organizasyonu

Bilgi Güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden BGYS Üst Yönetim Temsilcisi sorumludur. Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesinden BGYS Yöneticisi sorumludur. BGYS kapsamlı tüm görevlendirmeler, Üst Yönetim tarafından yapılmıştır.

Kapsam dâhilindeki birimlerde BGYS Sorumluları belirlenmiştir. BGYS Sorumluları kendi birimlerindeki Bilgi Güvenliği Yönetim Sistemi çalışmalarını takip etmek ve koordine etmekle yükümlüdürler.

BGYS'nin işletilmesi, sürdürülmesi gözden geçirilmesi, eylem planı oluşturulması, karar alınması ve uygulanması faaliyetleri komiteler ile yürütülmektedir. Bu anlamda BGYS Yürütme ve Yönetim Komitesi ile BGYS Komitesi oluşturulmuştur. BGYS Yürütme ve Yönetim Komitesi, BGYS Üst Yönetim Temsilcisi ile BGYS Yöneticisinden, BGYS Komitesi ise ilgili birimlerden seçilen BGYS Sorumlularından oluşur. Komite görev ve sorumlulukları "Roller ve Sorumluluklar Prosedürü" dokümanında anlatılmaktadır.

6. Risk Yönetim Çerçevesi

Kurumun ISO 27001 risk yönetim çerçevesi; Bilgi Güvenliği ve Hizmet Yönetimi risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi ve Risk İşleme Planı Bilgi Güvenliği ve Hizmet Yönetimi risklerinin nasıl kontrol edildiğini tanımlar. Risk İşleme Planının yönetiminden ve gerçekleştirilmesinden BGYS Komitesi sorumludur.

7. Sorumluluklar

BGYS Kapsamında oluşturulmuş roller ve sorumluluklar "Roller ve Sorumluluklar Prosedürü" dokümanında anlatılmaktadır.

8. Bilgi Güvenliği Politikası

8.1. Genel Esaslar

- Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, BGYS prosedürleri ile düzenlenir. Kurum çalışanları ve 3. taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.
- Bu kural ve prosedürlerin, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.
- Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001:2013 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler (Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir.
- Kurum tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya

sözleşmeler bulunmadıkça kuruma aittir.

8.2. Temel BGYS Prensipleri

- Çalışanlar ve üçüncü taraflarla kurumun gizlilik ihtiyaçlarını güvence altına almayı amaçlayan gizlilik anlaşmaları yapılır.
- Dış kaynak kullanım durumlarında oluşabilecek güvenlik gereksinimleri analiz edilerek güvenlik şart ve kontrolleri şartname ve sözleşmelerde ifade edilir.
- Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.
- Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.
- İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.
- Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.
- Kuruma ait bilgi varlıkları için kurum içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.
- Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.
- Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.
- Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
- Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
- Bilgi güvenliği ihlal olayları ve zayıflıklarının raporlanması için gerekli altyapı oluşturulur. İhlal olay kayıtları tutulur, gerekli düzeltici önleyici faaliyetler uygulanır ve düzenlenen farkındalık eğitimleri vasıtasıyla güvenlik olaylarından öğrenme sağlanır.
- Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
- Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.

8.3. Uyulması Gereken Kabul Edilebilir Kullanım Kuralları

Uyulması gereken kurallar BGYS Kapsamında hazırlanan prosedürlerde belirtilmiştir. Tüm kurallar esas olarak "Bilgi Sistemleri Kabul Edilebilir Kullanım Politikası" dokümanında yer almaktadır. BGYS kapsamı dâhilinde yer alan tüm çalışanlar ve 3. Taraflar belirtilen kurallara uymak zorundadır.

9. Yaptırım

Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı BGYS politika ve prosedürlerine uyulmadığının tespit edilmesi halinde, bu ihlalden sorumlu olan çalışan ya da 3. taraf için geçerli olan usul, esas ve sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır. Cezai yaptırımlarda öncelik hukuki, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere aittir.

10. Yönetimin Sorumluluğu

10.1. Yönetimin Taahhüdü

Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı, belirlediği hedef ve politikalarını gerçekleştirmek için Bilgi Güvenliği Yönetim Sistemini ISO/IEC 27001:2013'de belirtilen gereksinimleri yerine getirecek şekilde kurarak yürütür.

Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı Üst Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları tahsis edeceğini, etkinliğini, sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder. Bu taahhüdün sonucu olarak, kurum genelinde bilgi güvenliği farkındalık programları düzenler ve alt yapı yatırımlarını sürdürür.

BGYS Üst Yönetim Temsilcisi ve BGYS Yöneticisi değiştiğinde, işten ayrıldığında Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı Üst Yönetimi tarafından doküman revize edilerek atama tekrar yapılır.

Yönetim kademelerindeki yöneticiler güvenlik konusunda alt kademelerde bulunan çalışanlara sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan bir güvenlik anlayışıyla, kurumun en alt kademe çalışanına kadar inilmesi zorunludur. Bu yüzden kurumdaki yöneticilerin, gerek yazılı gerekse sözlü olarak güvenlik prosedürlerine uymaları, güvenlik konusundaki çalışmalara katılmaları konusunda güvenlik ile ilgili çalışmalarda bulunan çalışanlara destek olurlar.

Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı Üst Yönetimi, bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

11. Yönetim Gözden Geçirme

Yönetim Gözden geçirme toplantıları "Yönetimin Gözden Geçirmesi Prosedürü" 'ne uygun olarak yapılmalıdır.

12. Üçüncü tarafların yönetimi

Hacettepe Üniversitesi Bilgi İşlem Daire Başkanlığı çalışanı olmayıp bilgi sistemleri kaynaklarına erişim sağlayan her türlü kişi 3. Taraf olarak kabul edilir. 3. Tarafların uyması gereken kurallar ve yönetim şekli BGYS kapsamlı dokümanlarda 3. Taraf olarak ayrıca belirtilmiştir. 3. Taraf tanımına uyan her türlü kişi ya da kurumla yapılacak geçici ya da sürekli çalışma sözleşmelerin imzalanması güncel olarak takip edilmelidir. Sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları hazırlanıp Kurumlarla kurumsal gizlilik sözleşmesi 3. Taraf çalışanlarıyla bireysel gizlilik sözleşmesi yapılmalıdır. Gerektiği takdirde üçüncü taraf çalışanlarının politikaya uyması için süre tahsis edilmelidir.

13. Bilgi Güvenliği Politika Dokümanı Güncellenmesi ve Gözden Geçirilmesi

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yöneticisi sorumludur. Bilgi Güvenliği Politikası Dokümanı, en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa versiyon değişimi olarak kayıt altına alınmalı ve her versiyon BGYS Üst Yönetim Temsilcisine onaylatılmalıdır. Her versiyon değişikliği tüm kullanıcılara e-mail, sunucu üzerinden ya da yazılı olarak yayımlanmalıdır.

Gözden geçirmelerde;

- Politikanın etkinliği, kaydedilmiş güvenlik arızalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenmelidir.
- Politikanın güncelliği teknolojik değişimlerin etkisi vasıtasıyla gözlemlenmelidir.
- Bilgi Güvenliği Politikası organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından gözlemlenmelidir.
- Politika, sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra gözden geçirilmelidir.

14. İlgili Dokümanlar

14.1. İç Kaynaklı Dokümanlar

- Tüm BGYS Dokümantasyonu (BGYS Doküman Listesi)

14.2. Dış Kaynaklı Dokümanlar

Hacettepe Üniversitesi olarak, "Bilgi Güvenliği Politikası" 'nın Bilgi İşlem Daire Başkanlığında uygulanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederiz.