

Doküman Kodu: BGYS-0005

BİLGİ GÜVENLİĞİ POLİTİKASI OLUŞTURMA KILAVUZU

SÜRÜM 1.00

21 Mart 2008

Hazırlayan: Günce Öztürk

P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE
Tel: (0262) 648 1000
Faks: (0262) 648 1100
<http://www.bilgiguvenligi.gov.tr>
bilgi@bilgiguvenligi.gov.tr

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman, BGYS (Bilgi Güvenliği Yönetim Sistemi) kurmak isteyen kurumlar için yardımcı kaynak olarak hazırlanmıştır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda anlatılanlar tamamen tavsiye niteliğindedir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geçen Ağ Güvenliđi personeline ve dokümanı gözden geçirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Ali Dinçkan ve Fikret Ottekin'e teşekkürü borç biliriz.

İÇİNDEKİLER

1. GİRİŞ	5
1.1 Amaç ve Kapsam.....	5
1.2 Hedeflenen Kitle.....	5
1.3 Kısaltmalar.....	5
2. BİLGİ GÜVENLİĞİ POLİTİKALARI	6
3. BİLGİ GÜVENLİĞİ POLİTİKASININ BİLEŞENLERİ.....	6
3.1 Bilgi Güvenliğinin Tanımı.....	7
3.2 Bilgi Güvenliği İhtiyacı ve Bilgi Güvenliği Kapsamı	8
3.3 Bilgi Güvenliği Hedefleri	8
3.4 Risk Yönetim Çerçevesi	9
3.5 Yönetimin Bilgi Güvenliğini Sağlama Sözü ve Politika Dokümanının Onayı	9
3.6 Bilgi Güvenliği İlkeleri.....	10
3.7 Roller/Görevler ve sorumluluklar.....	10
3.8 Politikanın İhlali ve Yaptırımlar	10
3.9 Atıflar (Diğer kural, yönerge, standart ve süreçlere atıflar)	11
3.10 Bilgi Güvenliği Politikası Gözden Geçirme Kuralları.....	11
4. BİLGİ GÜVENLİĞİ POLİTİKASI'NI YAZARKEN.....	12
KAYNAKÇA	13

1. GİRİŞ

Bir kurumda, bilgi güvenliğini etkin bir şekilde sağlamak amacıyla çeşitli kurallar ve metotlar uygulanabilir. Bu kural ve metotlar, kurumun tehdit ve açıklarını analiz ederek, risklerinin farkına varmasından, teknik güvenlik çözümlerini sisteme entegre etmesine, sözleşmelerde bilgi güvenliğini de ele alan düzenlemeler yapmasından, kullanıcıların bilgi güvenliği farkındalığını arttırmaya kadar çok çeşitli alanlarda uygulanabilir.

Bu metotlardan en önemlisi, kurumun bilgi güvenliği hedefini ve bu hedefe ulaşmak için uygulanacak kural ve metotların çerçevesini çizen bilgi güvenliği politikalarının oluşturulması ve uygulanmasıdır.

1.1 Amaç ve Kapsam

Bu dokümanda ISO/IEC 27001 standardına uygun olarak Bilgi Güvenliği Yönetim Sistemi (BGYS) kurma çalışması planlayan kurumlara Bilgi Güvenliği Politikası'nın yazılması konusunda yol gösteren bilgilere yer verilmiş, politikada bulunması gereken hususlar örneklerle açıklanmıştır.

1.2 Hedeflenen Kitle

Bu doküman, Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulumu gerçekleştirecek kurum ve kuruluşlara yönelik olarak hazırlanmıştır.

1.3 Kısaltmalar

BGYS : Bilgi Güvenliği Yönetim Sistemi

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

2. BİLGİ GÜVENLİĞİ POLİTİKALARI

Bilgi güvenliği politikaları, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür.[1]

Bu kural ve uygulamaları tanımlayan politikalar çeşitli seviyelerde yazılabilir. Politikalar, genel bir Bilgi Güvenliği Politikası ve belirli alanlara ait politikalardan (erişim kontrol politikası, uzaktan erişim politikası, kullanıcı politikası, e-posta kullanım politikası vb.) oluşur ve uygulamaları tanımlayan prosedür ve talimatlarla tamamlanır.

Her seviyedeki politikanın tek bir dokümanda bulunması yerine, en üst seviyede temel ilkeleri barındıran bir Bilgi Güvenliği Politikası'nın oluşturulması ve bu dokümanla diğer ayrıntılı politikaların ilişkilendirilmesi tavsiye edilmektedir.[2]

Bilgi güvenliği politikası, bu politikalar doğrultusunda uygulanacak prosedürlerin amaçlarını tanımlayan en üst düzey doküman olacaktır. Yeni bir ürünü tanımlayan teknik özellikler gibi, genel bir güvenlik programının planlarını oluşturacaktır.

Makalenin devamında, Bilgi Güvenliği Politikası olarak bu üst seviye politikayı adlandıracağız.

3. BİLGİ GÜVENLİĞİ POLİTİKASININ BİLEŞENLERİ

Bilgi Güvenliği Politikası, kurumun bilgi güvenliği ihtiyacını ve bilgi güvenliği kavramını kurumun bilgi kaynaklarını kullanan her kişiye anlatma amacıyla hazırlanır. Kurumdaki bilgi güvenliği ihtiyacı, kurumun yaptığı işin gereği olarak ortaya çıkmış veya ilgili kanunlar ve düzenlemelerle belirlenmiş olabilir. Bu iş gerekleri ve varsa yasal zorunluluklar bu dokümanda net bir biçimde ortaya konmalıdır.

Bilgi güvenliği politikası, kurum yönetiminin bilgi güvenliğine dair sözünü ve desteğini gösterir ve bilgi güvenliğinin, kurumun belirlemiş olduğu misyonuna ulaşabilmesindeki destekleyici rolünü tanımlar.

Bilgi Güvenliği Politikası ile ilgili ISO/IEC 27001 standardı A.5.1 maddesi için, BGYS Kontrolleri Gerçekleştirilmesi ve Denetlenmesi Kılavuzu'na göre bir Bilgi Güvenliği Politikası'nda en azından aşağıdaki hususlar yer almalıdır:[3]

- a) Bilgi güvenliğinin tanımı, genel kapsamı ve hedefi,
- b) Bilgi güvenliğinin kurum için neden önemli olduğu, bilgi güvenliği sağlanmasının amacı ve bilgi güvenliği ilkeleri, bu amaç ve ilkeler için yönetim desteği,
- c) Kontrol hedefleri ve kontrollerin seçimi için risk değerlendirmesi ve risk yönetimini de içeren bir çerçevenin ortaya konulması,
- d) Güvenlik politikaları, ilkeleri, standartları ve uyum gereksinimlerinin özet bir açıklaması,
- e) Bilgi güvenliği ile ilgili tüm görev ve sorumlulukların tanımı,
- f) Diğer ayrıntılı politikalar ve belirli bilgi sistemleri için prosedürler veya kullanıcıların uyması gereken kurallar gibi politikayı destekleyen dokümanlara atıflar

Bu bilgiler ışığında, bir bilgi güvenliği politikasında bulunması gereken ifadeleri birer örnek ile aşağıdaki gibi sıralayabiliriz:

3.1 Bilgi Güvenliğinin Tanımı

Bilgi güvenliği politikası kurumun geneline hitap eder. Kurum içinde farklı görevlerde birçok çalışan olduğu için bilgi güvenliği kavramı bazı çalışanlar için yabancı veya yeni bir kavram olabilir. Bilgi güvenliği dendiğinde herkes tarafından aynı kavramın anlaşılmasını sağlamak için, politikada bilgi güvenliğinin açık ve anlaşılır bir tanımının bulunması gereklidir.

Bu politikada Bilgi Güvenliği kurumun bilgi varlıklarının aşağıdaki özelliklerinin korunması olarak tanımlanır:

- a) Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması,*
- b) Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması,*
- c) Kullanılabilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması.*

3.2 Bilgi Güvenliği İhtiyacı ve Bilgi Güvenliği Kapsamı

Kurumun bilgiye, dolayısıyla bilgi güvenliğine olan bağımlılığını vurgulayan bir ifadeden oluşur. Bir kurumda neden bilgi güvenliği politikasına ihtiyaç duyulduğu sorusunun temelini oluşturur.

Kurumumuz, satış hizmetlerinin tümünü elektronik ortamda gerçekleştirmektedir.

Bilgi güvenliği kapsamı ile kurumda hangi yönetsel birimlerin ve aktivitelerin bilgi güvenliği yapısı içinde değerlendirileceği belirtilmelidir.

Bu politika, kurum Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

3.3 Bilgi Güvenliği Hedefleri

Bilgi güvenliği hedefleri, bilgi güvenliğinin yönetimi ile ulaşılabilecek amaç hakkında okuyucuyu bilgilendirmek için özet olarak tanımlanmalıdır. Bu hedefler kurumun iş gerekleri ve stratejileri ile ilişkilendirilmelidir.

Kurum yönetimi:

- *Kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak,*
- *Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,*
- *Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak*

Amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

3.4 Risk Yönetim Çerçevesi

Kurumun, bilgi güvenliği risklerini nasıl yönettiğine dair bir çerçeve ortaya koymalıdır. Bilgi güvenliğini sağlamak için uygulayacağı kontrolleri ve bu kontrolleri hangi risklerle ilintili olarak uyguladığını ortaya koyduğu bir metodolojisi bulunmalıdır.

Kurumun risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk değerlendirmesi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Bu planın yönetiminden ve gerçekleştirilmesinden Bilgi Güvenliği Koordinasyon Kurulu sorumludur.

3.5 Yönetimin Bilgi Güvenliğini Sağlama Sözü ve Politika Dokümanının Onayı

Kurum yönetiminin, kurumda bilgi güvenliğini sağlama niyeti, politikada bulunması gereken en önemli ifadedir. Bu ifade olmadan, bilgi güvenliği personelinin yapmaya teşebbüs ettiği herhangi bir faaliyet etkin şekilde gerçekleşmeyecek ve kurum içinde ciddiye alınmayacaktır. Yönetim, bu söz ile, bilgi güvenliği amaçlarına ulaşma konusunda kararlılığını ve bu iş için gereken desteği sağlayacağını ifade ederken, kurum çalışanlarının bilgi güvenliğine önem vermesini de sağlamaktadır. Onay imzası, kurumda bilgi güvenliğinin sağlanmasının desteklendiğini gösterir. Genellikle kurumdaki en yüksek makam tarafından imzalanır.

Kurum yönetimi olarak, "Kurum Bilgi Güvenliği Politikası"nın uygulanmasının sağlanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.

Genel Müdür

3.6 Bilgi Güvenliği İlkeleri

Bilgi güvenliği ilkeleri, kurumdaki bilgi güvenliği ile ilgili genel kuralları koyar. Bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlar.

- *Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:*
 - *Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,*
 - *Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,*
 - *Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,*
 - *Bilgi güvenliği ihlal olaylarını raporlamalı ve Bilgi Güvenliği Birimi'ne bildirmeli, bu ihlalleri engelleyecek önlemleri almalıdır.*
- *Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.*
- *Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.*

3.7 Roller/Görevler ve sorumluluklar

Bu kısım, kurumda bilgi güvenliği ile ilgili, tam olarak ne beklendiğini anlatır. Görev ve sorumluluklar, kurumun bilgi kaynaklarını kullanan tüm tarafların sorumluluklarını ve bilgi güvenliğinin her alanını kapsamalıdır.

Kurumun tüm çalışanları ve BGYS de tanımlanan dış taraflar, bu politikaya ve bu politikayı uygulayan BGYS politika, prosedür ve talimatlarına uymakla yükümlüdür.

Birimlerin güvenlik sorumlularından oluşan Güvenlik Koordinasyon Kurulu, BGYS altyapısını desteklemek ve işleyişini devam ettirmekle sorumludur.

3.8 Politikanın İhlali ve Yaptırımlar

Bir kullanıcının politikaya uymadığı ve politikayı ihlal ettiği durumlarda o kullanıcıya yaptırım uygulanabileceğini belirten ifadedir. Kurumun genel disiplin politikasıyla ilişkilendirilmelidir.

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

- *Uyarma,*
- *Kınama,*
- *Para cezası,*
- *Sözleşme feshi.*

3.9 Atıflar (Diğer kural, yönerge, standart ve süreçlere atıflar)

Bilgi güvenliği politikası tek başına bir doküman değildir. Bilgi güvenliği amaçlarının gerçekleşmesi için hazırlanan başka ilgili politikalarla, standartlarla, prosedür ve talimatlarla desteklenecektir. Okuyucunun zihninde tam bir bilgi güvenliği resmi oluşturabilmesini sağlamak için bu dokümanlara da işaret edilmelidir.

Ayrıca, kanun, mevzuat vb. ile belirtilmiş, kurumun uygulaması gereken belirli kontrol ve önlemler varsa, bu kontrol ve önlemlere politikada referans verilir.

İş Sürekliliği ve Acil Durum Planları, Veri Yedekleme Prosedürleri, Virüs ve Saldırılarından Korunma, Sistemlere Erişim Kontrolü, Bilgi Güvenliği Olayları Prosedürleri bu politikayı destekler. Bu alanlarla ilgili işleyiş özel olarak dokümante edilmiş politika ve prosedürlerle tanımlanır.

3.10 Bilgi Güvenliği Politikası Gözden Geçirme Kuralları

Kurumda bilgi güvenliğinin sağlanması için, uygulamaya konulan kurallar ve alınan önlemlerin uygulanabilirlik ve etkinlik açılarından kontrol edilmesi ve gerekli gözden geçirme ve güncellemelerin yapılması gerekir. Bilgi Güvenliği Politikası da buna dâhildir.

Politika ile ilgili gözden geçirme, geliştirme ve değerlendirmelerin kimin tarafından, hangi aralıklarla yapılacağı belirlenmeli ve dokümanda yer almalıdır. Bu periyodik gözden geçirmeler dışında, bilgi güvenliği uygulama süreçlerinde değişiklikler, ortaya çıkabilecek yeni yasal düzenlemeler, teknik değişikliklere göre de politikanın düzenlenmesi gerekebilir.

Her iki durumda da, yapılan gözden geçirme ve güncellemelerin kayıtlarının da tutulması ve geliştirilen politikanın tekrar onaylanıp, yürürlüğe konması gerekir.

Bu politika, Güvenlik Koordinasyon Kurulu tarafından periyodik olarak 6 (altı) ayda bir gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika Kurum Başkanı tarafından onaylanır. Onaylanan politika kurum web sayfasında yayınlanır.

Bu ifadelere ek olarak, dokümanda, bilgi güvenliği politikasını hazırlayanların isimleri, politikanın yayınlanma ve gözden geçirme tarihleri bulunmalıdır.

4. BİLGİ GÜVENLİĞİ POLİTİKASI'NI YAZARKEN

Bilgi Güvenliği Politikası kurumda bilgi güvenliğine yön veren temel dokümandır. Bu doküman, kurumun tüm paydaşları tarafından erişilebilen ve bilinen bir doküman olacaktır. Bu nedenle, politikayı yazarken, dikkat edilmesi gereken ilk konu, politikanın kısa ve anlaşılabilir olmasıdır.

Politika çok uzun olursa, kurum kullanıcıları tarafından okunmayacaktır. Bunu göz önüne alarak, bilgi güvenliği politikasına ek olarak, tamamen kurum kullanıcıları hedeflenerek, bilgi güvenliği politikasının özetlenmiş bir sürümü hazırlanabilir. Böylece, kullanıcıların tüm dokümanı okumaları ve kendilerinden beklenenleri daha iyi anlamaları mümkün olabilir. Bu hazırlanan sürüm, Bilgi Güvenliği Politikası'nın ekinde veya ayrı bir doküman olarak yayınlanabilir ve paydaşlar ve kurum arasında bir sözleşme olarak kullanılabilir. Örneğin, bir kullanıcıya elektronik bilgiye erişim izni verilmeden önce, bu kullanıcının bilgi güvenliğine ilişkin sorumluluklarını okuyup anladığını/bildiğini onaylaması istenebilir. Bu belgenin ayrıca, kurumdaki bilgi güvenliği varlıklarının korunmasındaki sorumluluklarını anımsatmak amacıyla kullanıcılar tarafından –örneğin her yıl- okunması ve tekrar imzalanması sağlanabilir.

Politika, tüm kullanıcılar tarafından anlaşılır ve net olmalıdır; teknolojik terimlerin kullanılmasından da mümkün olduğunca kaçınılmalıdır.

Bilgi güvenliği politikası kurum çalışanları tarafından uygulanması beklenen bir politikadır. Politikanın gerçekçi olması önemlidir. Uygulanması zor veya imkânsız ifadeler yer verilmemelidir.

KAYNAKÇA

- [1]. Tuğkan Tuğlular, “Üniversitelerde Bilgi Güvenliği Politikaları“, Ulaknet Sistem Yönetimi Konferansı – Güvenlik, Ekim 2003.
- [2]. Scott Barman, Writing Information Security Policies, New Riders Publishing, 2001.
- [3]. Ted Humphreys and Angelika Plate, Guide to the Implementation and Auditing of ISMS Controls based on ISO/IEC 27001, British Standards Institution, 2005.
- [4]. Karin Höne and J.H.P. Eloff, “Information Security Policy- What do international security standards say?”, Computer and Security, Vol.21 No.5, 1 October 2002, s.402-409 (8).
- [5]. Alan Calder, Nine Steps to Success: An ISO 27001 Implementation Overview, IT Governance Institute, Jan 2006.