

Doküman Kodu: BGYS-0008

# BİLGİ GÜVENLİĞİ BİLİNÇLENDİRME SÜRECİ OLUŞTURMA KILAVUZU

SÜRÜM 1.00

22.02.2008

Hazırlayan: Dinçer Önel

## ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliđi, 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 güvenliđi, 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 Güvenliđi 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 Dođan Eskiörük'e teřekkürü borç biliriz.

## İÇİNDEKİLER

<b>1. GİRİŞ .....</b>	<b>5</b>
1.1 Amaç ve Kapsam.....	5
1.2 Hedeflenen Kitle.....	6
1.3 Kısaltmalar.....	6
<b>2. GÖREV VE SORUMLULUKLAR .....</b>	<b>7</b>
2.1 Üst yönetim.....	7
2.2 Bilgi Güvenliđi Yöneticisi.....	7
2.3 Bilgi Güvenliđi Bilinçlendirme Süreci Yürütücüsü .....	8
2.4 Bölüm Yöneticileri .....	8
2.5 Kullanıcılar .....	9
<b>3. SÜRECİN OLUŞTURULMASI.....</b>	<b>9</b>
3.1 Sürecin Planlanması ve Tasarlanması .....	10
3.1.1 Sürecin Yapılandırılması .....	10
3.1.2 İhtiyaç Analizi ve Deđerlendirmesi .....	12
3.1.3 Bilinçlendirme Strateji ve Planının Geliştirilmesi .....	14
3.1.4 Önceliklerin Belirlenmesi .....	15
3.1.5 İçeriklerin Bilgi Düzeyinin Belirlenmesi.....	16
3.1.6 Bilinçlendirme Programının Finansmanı.....	16
3.2 Bilinçlendirme ve Eğitim Materyalinin Geliştirilmesi .....	17
3.2.1 Bilinçlendirme Materyallerinin Geliştirilmesi.....	18
3.2.1.1 Bilinçlendirme Konularının Seçimi .....	18
3.2.1.2 Bilinçlendirme Materyali Kaynakları .....	19
3.2.2 Eğitim Materyallerinin Geliştirilmesi .....	19
3.2.2.1 Eğitim Materyali Kaynakları.....	19
3.3 Bilinçlendirme ve Eğitim Sürecinin Uygulanması .....	20
3.3.1 Bilinçlendirme Materyali Sunum Teknikleri .....	20
3.3.2 Eğitim Materyali Sunum Teknikleri .....	21
<b>KAYNAKÇA .....</b>	<b>22</b>

## 1. GİRİŞ

Bilgiyi işleme ve kullanma faaliyetlerinin büyük kısmının bilgi ağları üzerinde gerçekleştiđi günümüz iş dünyasında, kurumların sahip oldukları bilginin gizliliđini, bütünlüğünü ve kullanılabilirliğini koruyabilmeleri için BT kullanan ve yöneten kurum çalışanlarının:

- Kurumun misyonu doğrultusunda görev ve sorumluluklarını anlamaları
- Kurumun bilgi güvenliđi politika, prosedür ve uygulamalarını anlamaları
- Sorumlu oldukları bilgi (bilişim) kaynaklarını korumaya yönelik yönetimsel, operasyonel ve teknik açıdan gerekli asgari bilgi seviyesine sahip olmaları

gerekmektedir.

Bilgi Güvenliđi denetim raporları, makaleler veya konferans sunularında da ifade edildiđi ve BT güvenliđi uzmanlarınca da kabul edildiđi üzere, bilgi güvenliđinin sağlanmasındaki en zayıf halka insandır. İnsan faktörü uygun ve yeterli seviyede güvenliđin sağlanmasında anahtar role sahiptir. Bu sebeplerden ötürü bir kurum varlığı olarak insan üzerinde daha büyük bir dikkatle durulması gerekmektedir. Bu bağlamda, Bilgi Güvenliđi Yönetim Sistemi (BGYS) kapsamında her seviyedeki kurum çalışanın bilgi güvenliđi konusundaki sorumluluklarını kavramasını sağlayacak bir bilinçlendirme sürecinin oluşturulması zaruridir.

### 1.1 Amaç ve Kapsam

Bu doküman bir BGYS kapsamında bilgi güvenliđi bilinçlendirme ve eğitim süreci oluşturma ve yürütme konusunda yol gösterici bilgiler vermeyi hedeflemektedir. Bilinçlendirme süreci tasarlama (planlama), geliştirme, uygulama ve iyileştirme adımlarından oluşan bir yaşam döngüsü içinde sunulmaktadır. Bu doküman ayrıca bilinçlendirme süreci gereksinimlerinin nasıl belirleneceđi, bir eğitim planının nasıl geliştirileceđi ve süreç için finansal desteğin nasıl sağlanacağını anlatmaktadır. Bu dokümanda aşağıdaki hususlar da ele alınmaktadır:

- Bilinçlendirme ve eğitim konularının seçilmesi
- Bilinçlendirme ve eğitim materyalleri için kaynak bulunması
- Farklı metotlar izleyerek eğitim materyallerinin hazırlanması
- Bilinçlendirme sürecinin etkinliđinin değerlendirilmesi
- Deđişen teknoloji ve kurum öncelikleri karşısında güncel kalınması

## 1.2 Hedeflenen Kitle

Bu doküman öncelikli olarak BGYS kurulumu gerçekteřtiren veya gerçekteřtirmiş kurumların Bilgi Güvenliđi sorumluları, BT yöneticileri, sorumlu diđer yöneticileri ve bu kurumların hizmet aldıkları eğitim kuruluşları ve eğitimcileri için yol gösterici bir rehber olarak hazırlanmıştır.

## 1.3 Kısaltmalar

**BGYS** : **Bilgi Güvenliđi Yönetim Sistemi**

**BT** : **Bilgi Teknolojileri**

**UEKAE** : **Ulusal Elektronik ve Kriptoloji Arařtırma Enstitüsü**

## 2. GÖREV VE SORUMLULUKLAR

Başarılı ve etkin işleyen bir bilgi güvenliđi bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekmektedir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür. Bilgi güvenliđi bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir.

### 2.1 Üst yönetim

Üst yönetim bilgi güvenliđi bilinçlendirme sürecinden nihai olarak sorumlu olan taraftır. Kurumun üst yönetimi etkin bir bilinçlendirme süreci oluşturulmasına yönelik kararlılığını ortaya koymalıdır. Bilinçlendirme sürecinin başarıya ulaşmasında üst yönetimin tutum ve yaklaşımı son derece önemlidir. Bu alanda üst yönetime düşen görev ve sorumluluklar şu şekilde sıralanabilir:

- Kurum içinde bir Bilgi Güvenliđi Yöneticisi atanması
- Kurum çapında işleyen bir bilgi güvenliđi bilinçlendirme sürecinin oluşturulması, yeterli kaynak ve bütçe ile desteklenmesi
- Kurumun bilgi varlıklarının korunmasını sağlayabilecek seviyede bilinçli ve eğitimli bir personel kadrosunun bulunması

### 2.2 Bilgi Güvenliđi Yöneticisi

Bilgi Güvenliđi Yöneticisi kurum üst yönetimi tarafından bilgi güvenliđi bilinçlendirme sürecinin oluşturmasını yönetmekle görevlendirilen kişidir. Etkin bir bilinçlendirme süreci için Bilgi Güvenliđi Yöneticisinin, Bilgi Sistemleri Yöneticisi (BT Yöneticisi veya direktörü CIO) ile birlikte çalışması gerekmektedir. Bilgi Güvenliđi Yöneticisinin görev ve sorumlulukları şu şekilde sıralanabilir:

- Bilgi güvenliđi bilinçlendirme süreci için genel stratejinin belirlenmesi
- Kurum içinde bir bilgi güvenliđi bilinçlendirme süreci yürütücüsü atanması
- Üst yönetimin, bölüm yöneticilerinin, diğer seviyedeki yöneticilerin, çalışanların ve diğer personelin bilinçlendirme sürecinin temel kavramlarını ve hedeflerini anlamalarını sağlamak, onları sürecin gelişimi ve ilerlemesi konusunda bilgilendirmek
- Bilinçlendirme sürecinin yeterli seviyede finanse edilmesini sağlamak

- Kurum personeline bilgi güvenliđi sorumluluklarının eğitimler ile öğretilmesi
- Kurumun bilgi kaynaklarına erişen tüm kullanıcıların bilgi güvenliđi sorumluluklarını bildiklerinden emin olunması
- Bilgi güvenliđi bilinçlendirme sürecinin takip edilmesi ve uygunsuzlukları tespit edecek mekanizmaların devreye alınmış olması

### 2.3 Bilgi Güvenliđi Bilinçlendirme Süreci Yürütücüsü

Bilgi güvenliđi bilinçlendirme süreci yürütücüsü taktik ve uygulama seviyesinde bilinçlendirme sürecinin hayata geçirilmesinden sorumlu olan kişidir. Bu roldeki kişinin görev ve sorumlukları şu şekilde sıralanabilir:

- Her seviyedeki personel için uygun bilinçlendirme ve eğitim materyalinin zamanında geliştirilmiş olmasını sağlamak
- Her seviyedeki personel için uygun bilinçlendirme ve eğitim materyalinin planlanan kişilere etkin bir şekilde dağıtılmasını sağlamak
- Bilinçlendirme ve eğitim materyalleri ile bunların sunumları hakkında personel ve yöneticilerin görüşlerini iletebilmelerine imkan veren uygun bir geri besleme yönteminin sağlanması
- Bilinçlendirme ve eğitim materyallerinin periyodik olarak gözden geçirilmesini ve gereksinim halinde güncellenmesini sağlamak
- Bilgi güvenliđi bilinçlendirme sürecinin takip edilmesi ve uygunsuzlukların rapor edilmesinde Bilgi Güvenliđi Yöneticisine yardımcı olmak

### 2.4 Bölüm Yöneticileri

Yöneticiler bilgi güvenliđi bilinçlendirme ve eğitimi sürecinin gereklerine personelinin uymasını sağlamakla sorumludurlar. Diğer görev ve sorumlukları şu şekilde sıralanabilir:

- Bilgi güvenliđi bilinçlendirme süreci kapsamında ortak sorumlulukları yerine getirmek amacıyla Bilgi Güvenliđi Yöneticisi ve Bilgi Güvenliđi Bilinçlendirme Süreci Yürütücüsü ile birlikte çalışmak
- Bilgi güvenliđi alanında görev ve sorumluluđıya sahip personelinin mesleki anlamda bireysel gelişimine katkıda bulunmak

- Yarı zamanlı personel, stajyer çalışan ve yüklenici firma personeli dahil olmak üzere tüm kullanıcıların erişimde bulunmadan önce bilgi güvenliđi sorumluluklarını yerine getirebilmeleri için uygun eğitimleri almalarını sağlamak
- Yarı zamanlı personel, stajyer çalışan ve yüklenici firma personeli dahil olmak üzere tüm kullanıcıların kullandıkları sistem ve uygulamanın, ilgili politika veya prosedürle belirtilen kurallarını bilmelerini ve anlamalarını sağlamak
- Eğitim ve bilinçlendirme eksikliđi sebebiyle kullanıcıların yaptıkları hata veya ihmallerden kaynaklanabilecek, bilgi varlıklarındaki her türlü kayıp ve zararı azaltmaya çalışmak

## 2.5 Kullanıcılar

Kullanıcılar bilgi güvenliđi bilinçlendirme sürecindeki en büyük ve önemli hedef kitledir. Kurum içindeki işler yürütülürken istemeden yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir. Kurum çalışanları, yüklenici firma personeli, yarı zamanlı personel, stajyerler, diđer kurum çalışanları, ziyaretçiler, iş ortaklarının çalışanları, destek alınan firmaların personeli, kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir. Kullanıcıların sorumlulukları şu şekilde sıralanabilir:

- Güvenlik politika ve prosedürlerini anlamak, gereklerine uymak
- Erişim hakkının bulunduğu bilgi varlıklarının kullanım ve güvenlik kurallarını öğreten eğitimleri almak
- Bilinçlendirme ve eğitim ihtiyaçlarının giderilmesi için yönetimle birlikte çalışmak
- Kullandıkları yazılım ve uygulamaların güvenlik yamalarının güncel tutulmasını sağlamak
- Güçlü parola kullanımı, antivirüs yazılımı kullanılması, şüpheli olay ve ihlal durumlarının rapor edilmesi, veri yedeklemesi, sosyal mühendislik saldırılarına karşı koyulan kurallara uyulması vb. gibi kurum bilgisini daha iyi korumaya yönelik uygulama ve faaliyetlerin farkında ve bilincinde olmak

## 3. SÜRECİN OLUŞTURULMASI

Bilgi güvenliđi bilinçlendirme ve eğitim süreci oluşturulması üç ana adımda gerçekleşmektedir:

### 1. Sürecin planlanması ve tasarlanması

---

2. Bilinçlendirme ve eğitim materyalinin geliştirilmesi
3. Sürecin uygulanması

### 3.1 Sürecin Planlanması ve Tasarlanması

Bilgi güvenliđi bilinçlendirme programları tasarlanırken kurumun misyonu, stratejik hedefleri ve iş gereksinimlerine uyumlu olması sürekli göz önünde bulundurulmalıdır. Ayrıca bilinçlendirme sürecinin kurum kültürüne ve kurumun bilgiyi işleme yapısına uygun olması önemlidir. Başarılı bir bilinçlendirme programı kullanıcılara (katılımcılar) normal çalışma seyirleri içinde yaptıkları işlerle alakalı içerikler sunar.

Bilinçlendirme süreci oluşturulmasının planlama ve tasarlama aşamasında kurumun bilgi güvenliđi alanındaki eğitim ve bilinçlendirme ihtiyaçları saptanır, etkin bir eğitim ve bilinçlendirme planı geliştirilir, kurum içi finansman konusu sorgulanır ve öncelikler ortaya konur.

Bu bölümde:

- Bilinçlendirme ve eğitim faaliyetinin nasıl yapılandırılacağı
- İhtiyaç analizi ve değerlendirmesinin nasıl yapılacağı
- Bilinçlendirme ve eğitim planının nasıl geliştirileceđi
- Önceliklerin nasıl belirleneceđi
- İçeriklerin bilgi düzeyinin nasıl belirleneceđi
- Bilinçlendirme programının nasıl finanse edileceđi

anlatılacaktır.

#### 3.1.1 Sürecin Yapılandırılması

Bir bilgi güvenliđi bilinçlendirme süreci çok deđişik biçimlerde tasarlanıp geliştirilebilir. Bilinçlendirme süreci yapılandırılmasında yaygın olarak benimsenen üç farklı yaklaşım ve yönetim modeli bulunmaktadır. Bunlar:

- Model 1: Merkezi yönetim modeli
- Model 2: Yarı merkezi yönetim modeli
- Model 3: Dağıtık yönetim modeli

Seçilecek modelin ne olacağına karar verilirken aşağıdaki kriterlere bakılmalıdır:

- Kurumun büyüklüğü ve coğrafik dağılımı
- Tanımlı kurumsal rol ve sorumluluklar
- Ödenek ayrılması ve yetki

### **Model 1: Merkezi Program Yönetim Modeli**

Bu modelde bilgi güvenliđi bilinçlendirme ve eğitim programının tüm sorumluluđu ve bütçesi merkezi yönetime aittir. Bilinçlendirme süreci ile ilgili bütün politikalar, stratejiler, planlar, talimatlar ve yöntemler merkezi yönetim tarafından geliştirilir. Merkezde bulunan Bilgi Güvenliđi Yöneticisi ve Bilgi Güvenliđi Bilinçlendirme Süreci Yürütücüsü programın bütün aşamalarını koordine etmekle yükümlüdür. İhtiyaç analizinin yapılması ve gerekli eğitim materyallerinin geliştirilmesi ve sağlanması da yine merkezi yönetimin görevidir. Kurum içindeki organizasyonel birimler geliştirilen programa uymakla ve istenilen bilgileri merkezi yönetime sunmakla sorumludurlar. Bu modelde organizasyonel birimler ayrıca programın etkinliđi ve performansı ile ilgili değerlendirmelerini merkezi yönetime bildirirler.

Merkezi model şu özelliklere sahip kurumlar tarafından tercih edilmektedir:

- Nispeten küçük ve merkezi olarak yönetilen
- Gerekli kaynađı ve uzmanlıđı merkezi olarak sağlayabilen
- Birbirine benzer görevleri yürüten organizasyonel birimleri olan

### **Model 2: Yarı Merkezi Program Yönetim Modeli**

Bu modelde bilgi güvenliđi bilinçlendirme ve eğitim programı ile ilgili politika ve stratejiler merkezi yönetim tarafından geliştirilirken, programın uygulanması ve hayata geçirilmesi organizasyonel birimlerce bireysel olarak yürütülür. Bütçelendirme ve ihtiyaç analizi merkezi olarak gerçekleşir. Merkez tarafından belirlenen stratejiye uygun olarak organizasyonel birimler kendi eğitim planlarını oluştururlar. Bilinçlendirme ve eğitim materyallerinin geliştirilmesi ve sağlanması ile bunların kullanıcılara sunulması organizasyonel birimlerin sorumluluđundadır.

Bu modelde merkezi yönetim organizasyonel birimlerden yapılan harcamalar, eğitim planlarının durumu, bilinçlendirme faaliyetleri hakkında ayrıntılı bilgi içeren raporlar isteyebilir. Kısacası yarı merkezi modelde yönlendirme ve izleme merkezi olarak, geliştirme ve uygulama da birimlerce yapılır.

Yarı merkezi model:

- Nispeten büyük ve geniş bir coğrafik alana dağılmış olan
- Kurumsal rol ve sorumlulukların merkez ve birimler tarafından paylaşıldığı
- Birbirinden farklı görevleri yürüten organizasyonel birimlere sahip, bu sebeple de eğitim ihtiyaçlarının birimden birime farklılaştığı

gibi özelliklere sahip kurumlar tarafından tercih edilmektedir.

### **Model 3: Dağıtık Program Yönetim Modeli**

Bu modelde merkezi yönetim sadece genel bilinçlendirme politikasını ve beklentileri ortaya koyar. Bilinçlendirme programının planlanması, geliştirilmesi ve uygulamaya geçirilmesi ile ilgili bütün sorumluluklar organizasyonel birimlere bırakılmaktadır. Bu modelde bilinçlendirme süreci ile ilgili yetki dağılımı yapılmaktadır. Alt seviye Bilgi Güvenliđi Yöneticiliđi ve Bilinçlendirme Süreci Yürütücülüđü merkez dışındaki birimlerde de oluşturulur ve merkezdeki üstlerine bağlanırlar. İhtiyaç analizi organizasyonel birimlerce yapıldığından bilinçlendirme ve eğitimlerle ilgili stratejiler de buralarda geliştirilir. Ayrıca program için bütçenin belirlenmesi de birimlerin sorumluluğundadır. Kısacası bu modelde merkezi yönetim bilinçlendirme faaliyetiyle ilgili kurum misyonuna uygun genel çerçeveyi belirler, geri kalan adımlarla ilgili bütün sorumluluklar birimlere kalmaktadır.

Dağıtık modelin uygulanabileceđi kurumların:

- Uluslar arası seviyede faaliyet gösteren ve oldukça büyük
- Kurum idaresi ve yönetsel sorumluluklar açısından oldukça dağıtık bir yapıya sahip
- Birbirinden oldukça farklı alanlarda görevleri yürüten birimlere sahip

gibi karakteristik özellikleri bulunmaktadır.

### **3.1.2 İhtiyaç Analizi ve Deđerlendirmesi**

Kurumun bilgi güvenliđi bilinçlendirme ve eğitim ihtiyaçlarının belirlenmesi işlemidir. İhtiyaç analizi ve deđerlendirmesinden elde edilecek sonuçlar bilinçlendirme faaliyeti için gerekli kaynakların sağlanması konusunda üst yönetim onayının alınmasında yardımcı olur. Ayrıca ihtiyaç analizi, bilinçlendirme programı için izlenecek stratejinin de belirlenmesinde yol gösterici role sahiptir.

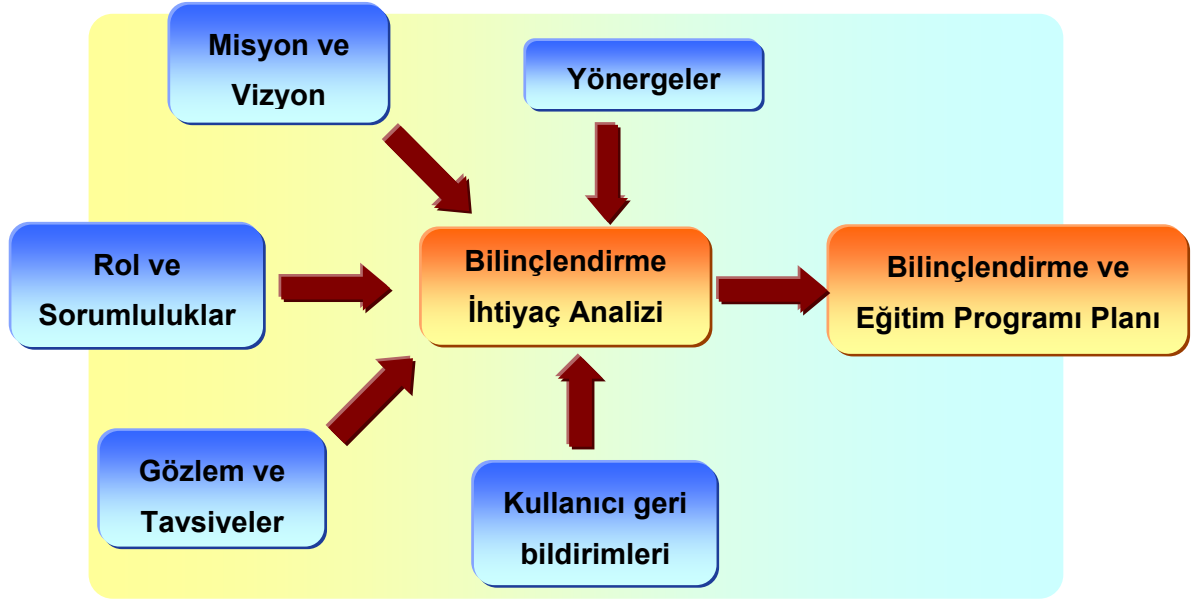
Bilgi güvenliđi bilinçlendirme ihtiyaçları belirlenirken personelin kurum içinde üstlenmekte olduđu farklı seviyedeki rol ve görevler dikkate alınması gerekir. Bilinçlendirme ihtiyaçları özellikle belirlenmesi gereken kritik personel şunlardır:

- Yöneticiler: İcraacı yönetim (executive management), bölüm (birim) yöneticileri, kısım amirleri vb.
- Güvenlik personeli: Bilgi Güvenliđi Yöneticileri, Bilinçlendirme Program Yürütücülerini
- Geliştiriciler: Sistem ve yazılım geliştiriciler
- Bilgi Sistemleri personeli: BT yöneticileri, sistem yöneticileri, sistem destek personeli
- İşletmenler ve kullanıcılar

İhtiyaçları kurum içindeki çalışanların görev ve sorumluluklarına uygun olacak şekilde belirleyebilmek için pek çok farklı kaynađa başvurulabilir. İhtiyaçları doğru tespit etme amacıyla bilgi toplamak için çeşitli yöntemler ve araçlar mevcuttur. Bunlardan bazıları şunlar olabilir:

- Kurumsal anketler
- Belirlenen tüm kritik personel gruplarıyla yüz yüze yapılacak görüşmeler ile personelin günlük görevleri kapsamında gerçekleştirdiđi aktivitelerin ve bilgi sistemini hangi amaçlarla kullandıklarının öğrenilmesi
- Kurum çapında bugüne kadar düzenlenmiş bilgi güvenliđi eğitim faaliyetlerinin gözden geçirilmesi, kullanılan materyallerin incelenmesi
- Geçmişte yaşanmış güvenlik ihlali olaylarının incelenmesi (servis dışı bırakılma, web sayfasının değiştirilmesi, sisteme yapılan yetkisiz girişler, başarılı virüs saldırıları vb.)
- Bilgi sistemine erişimi olan kullanıcı hesaplarının dökümünün alınması
- Geçmişte yapılmış denetimlere (iç denetim veya bağımsız denetim) ait raporlardaki bulguların incelenmesi
- Bilgi sisteminde yapılan teknik ve altyapısal deđişikliklerin sürekli takip edilmesi
- Akademik çevrelerde ve eğitim kurumlarındaki bilgi güvenliđi alanında takip edilen son gelişmelerden ve eğilimlerden haberdar olunması

Bu ve bunlara benzer yöntemlerle elde edilecek bilgiler ihtiyaçların detaylı bir şekilde ortaya çıkmasına ve stratejinin şekillenmesine yardımcı olur. Bunların yanında aşğıdaki şekilde gösterilen bilgiler de bu aşamada girdi olarak kullanılmalıdır.



Şekil 1 - İhtiyaç Analizi Girdileri

İhtiyaç analizi sürecinde toplanan bilgiler aşağıdaki şu sorulara cevap verebilmelidir:

- Ne tür bilinçlendirme ve eğitime ihtiyaç duyulmaktadır?
- Şu ana kadar bu ihtiyaçları karşılanması için neler yapılmıştır?
- Mevcut durumda bu ihtiyaçlar nasıl karşılanmakta?
- İhtiyaç duyulanla yapılan arasında hangi alanlarda ve ne seviye açıklık bulunmakta
- En kritik ihtiyaçlar hangileridir?

İhtiyaç analizinin önemli bir parçası bilinçlendirme ve eğitime programının uygulamaya konulmasına yönelik teknik gereksinimlerin ortaya çıkarılmasıdır. Örneğin, bilinçlendirme içerikleri bilgisayar ortamında sunulacak ise bunun için gerekli teknik altyapının özellikleri (yerel alan ağı, terminaller, grafik kartları, ses kartları, hoparlör vb.) önceden belirlenmelidir. Ayrıca sınıf eğitimleri için gereksinim duyulacak oda ve malzemenin özellikleri ve miktarı bu aşamada tespit edilmelidir.

### 3.1.3 Bilinçlendirme Strateji ve Planının Geliştirilmesi

İhtiyaç analizi tamamlandıktan sonra kurum, bilinçlendirme programının oluşturulmasında izlenecek plan ve stratejiyi belirlemelidir. Plan geliştirilirken belirlenen ihtiyaçların karşılandığından emin olunmalıdır. Program planı bilinçlendirme süreci geliştirme çalışmalarının başvuru dokümanı olacaktır. Bilinçlendirme planı aşağıdaki hususları ele almalıdır:

- Kurum bilgi güvenliđi politikasındaki bilinçlendirme ve eğitim programını ilgilendiren maddeler
- Bilinçlendirme ve eğitim programının kapsamı
- Bilinçlendirme materyallerini geliştirecek ve sunacak personel ile bilinçlendirme aktivitelerine katılacak personelin rol ve sorumlulukları
- Bilinçlendirme ve eğitim programıyla ulaşılmak istenen kurumsal hedefler
- Programın hedef kitlesi
- Her bir hedef kitle grubu için zorunlu veya isteđe bađlı kurs ve materyaller
- Her bir faaliyet ile ulaşılmak istenen bilgi ve farkındalık seviyesi
- Her bir eğitim ve bilinçlendirme aktivitesinde işlenecek konular
- Programı hayata geçirmede kullanılacak uygulama yöntemleri
- Dokümantasyon, geri bildirim ve bilgisel kazanımların takibi<sup>1</sup>
- Eğitim materyallerinin düzenli aralıklarla gözden geçirilmesi ve gerekirse güncellenmesi
- Her bir hedef kitle grubuna uygulanacak eğitim ve bilinçlendirme faaliyetlerinin tekrarlanma sıklığı<sup>2</sup>

#### 3.1.4 Önceliklerin Belirlenmesi

Bilinçlendirme planının hazırlandıktan sonra bir uygulama takviminin belirlenmesi gerekmektedir. Planı uygulamaya geçirme işlemi aşamalar halinde olursa nelerin önce nelerin sonra yapılacağı belirlenmesi gerekmektedir. Öncelikler belirlenirken dikkate alınması gereken faktörler aşağıda listelenmektedir:

- Eğitim materyallerinin durumu
- Kurumsal rol ve risk (yüksek sorumluluk ve yüksek risk alanlarında eğitime öncelik verilmesi)

---

<sup>1</sup> Bu madde, kurum içinde kimlerin bilgi güvenli konusunda başarıyla eğitildiđi, kimlerin hala eğitime ihtiyaç duyduđu, katılımcıların eğitim materyallerini nasıl değerlendireceđi ve kurumun katılımcıların eğitim ve diđer faaliyetlerden gerçekten bir kazanım sağlayıp sağlamadıklarını nasıl tespit edeceđi ile ilgilidir

<sup>2</sup> Hedef kitleye bilinçlendirme ve eğitim uygulaması yılda en az bir kere yapılmalıdır. Programın hedefine ulaşması açısından süreklilik gereklidir. Bilgi güvenliđi konusunda daha çok sorumluluđa sahip personel (sistem yöneticileri, ađ yöneticileri, bilgi güvenliđi sorumluları vb.) için bu periyot daha sık olmalıdır.

- Güvenlik bilincinin az olduđu birimlerde önceliđi arttırmak
- Eğitime ihtiyaç duyan kritik projeler

### 3.1.5 İçeriklerin Bilgi Düzeyinin Belirlenmesi

Eđitim materyallerinin içeriđi eğitimi alacak personele uygun seviyede ayarlanmalıdır. Personelin anlaması mümkün olmayacak derecede karmaşık bilgiler sunulması veya zaten bildiđi şeylerin verilmesi, eğitim materyallerinin bilgi düzeyinin yanlış ayarlanmasının sonucudur.

Eđitim materyalleri iki önemli kriter göz önünde bulundurularak geliştirilmelidir:

1. Eğitimi alacak hedef kitlenin kurum içindeki pozisyonu
2. Bu pozisyon için gerekli güvenlik bilgisinin seviyesi

Bilgi güvenliđi bilinçlendirme ve eğitim faaliyetlerinin temel amacı çalışanlara görev ve sorumluluklarıyla doğrudan alakalı ve sadece gerekli olan bilgi ve kabiliyetlerin kazandırılmasıdır. Bu bilgiler ışığında hazırlanacak bilinçlendirme materyalleri giriş seviyesi (göreve yeni başlayanlar için), orta seviye (alanında belli derece deneyim sahibi olanlar için) ve ileri seviye (yüksek güvenlik gereksinimli kritik görev ve sorumluluklara sahip personel için) gibi farklı düzeylerde olabilir.

### 3.1.6 Bilinçlendirme Programının Finansmanı

Bu aşamada bilinçlendirme programına yönelik bütçe gereksinimleri belirlenmeli ve bilinçlendirme süreci planına eklenmelidir. Bölüm 3.1.1’de bahsedilen uygulama modelleri temel alınarak gerekli finansmanın miktarı hakkında bir karar verilmelidir. Bilgi Teknolojileri Direktörünün (CIO) bu konuda beklentinin ne derece olduğunu üst yönetime açıkça sunması gerekmektedir. Belirlenen öncelikler dikkate alınarak mevcut ve öngörülen bütçe üzerinden finansman kaynaklarını belirlemeye yönelik yaklaşımlar ilgili birimlerce karşılanmaya çalışılmalıdır. Bilinçlendirme sürecine ait finansman kaynaklarının ve gereksinimlerin belirlenmesine yönelik yaklaşımlar:

- Toplam eğitim bütçesinin belli bir yüzdesi
- Toplam BT bütçesinin belli bir yüzdesi
- Rol tabanlı masraf ve bütçelendirme (yüksek güvenlik gereksinimli rollere verilecek eğitimler genel güvenlik eğitimlerinden daha masraflı olacaktır)

gibi olabilir.

### 3.2 Bilinçlendirme ve Eğitim Materyalinin Geliştirilmesi

Bilinçlendirme ve eğitim materyallerinin geliştirilmesi adımı geniş kapsamlı olarak anlaşılmalıdır. Bu adımda bilinçlendirme ve eğitim faaliyetleriyle verilecek içerik detaylarıyla belirlenir ve temin edilir. Bilinçlendirme ve eğitim materyalinin temin edilmesi farklı biçimlerde gerçekleşebilir:

- Kurum içinde kurumun kendi imkanlarıyla geliştirilebilir
- Diğer kurumların veya profesyonel kuruluşların çalışmalarından yararlanabilir
- Eğitim kuruluşlarından hazır olarak satın alınabilir

Hangi yolla temin edilirse edilsin materyaller geliştirilirken sürekli akılda tutulması gereken iki önemli husus bulunmaktadır:

- Personele nasıl bir davranış biçimi kazandırılmalıdır ? (Bilinçlendirme)
- Hedef kitleye hangi kabiliyetler kazandırılmalıdır ? (Eğitim)

Bilinçlendirme ve eğitim faaliyetleri içerik ve bilgi düzeyi anlamında birbirinden ayrılmaktadır. Bilinçlendirmenin amacı basitçe bilgi güvenliği konusuna dikkatlerin çekilmesidir. Bilinçlendirme faaliyetleri bireylerin bilgi güvenliğinin önemi anlamasını ve işinde buna uygun davranmasını sağlamaya çalışır. Bilinçlendirme, eğitim faaliyetlerine göre daha geniş bir kapsamda uygulanır. Eğitim ise daha çok belli bir kitleye işlerine yönelik özel alanlarda verilir. Eğitimde amaç, basitçe, belli özel güvenlik kabiliyetlerinin kazandırılmasıdır. Eğitimde katılımcılara görevlerini yerine getirirken bilgi güvenliği ile ilgili bilmesi gereken her şey verilir ve bunları uygulayabilmesi beklenir. Bu bağlamda materyal geliştirilmesi safhasında bunun bir eğitim materyali mi yoksa bir bilinçlendirme materyali mi olduğu iyi bilinmelidir.

Geliştirilen materyaller mutlaka hedef kitlenin görev ve sorumluluklarıyla doğrudan ilgili olmalıdır. Personel materyal ile verilen bilgiyi işi ile bütünleştirebilmelidir. Geniş kapsamlı ve genel konuların işlendiği sunumlar bireylerin ilgisini çekmede başarısız kalırlar. Bir bilinçlendirme ve eğitim süreci, hedef kitlenin ilgisini çekebildiği ve güncel konuları ele alabildiği takdirde başarılı olur.

### 3.2.1 Bilinçlendirme Materyallerinin Geliştirilmesi

Bilinçlendirme materyallerini geliştirmeye başlamadan önce şu sorunun cevaplanması gerekir: “Personelin bilgi güvenliđi ile ilgili nelerden haberdar olmasını istiyoruz?” Bilinçlendirme materyalinde kullanılacak konuların belirlenmesi gerekir. Bu konuda bilgi güvenliđi eğilimlerini takip eden web sayfalarından, dergilerden, e-posta bilgilendirmelerinden faydalanılabilir. Ayrıca kurum politikaları, düzenli yapılan denetimler ve iç kontroller de bilinçlendirmeye gereksinim duyulan alanları tespit etmede yardımcı olurlar.

#### 3.2.1.1 Bilinçlendirme Konularının Seçimi

Bir bilinçlendirme materyalinde veya oturumunda ele alınabilecek önemli pek çok farklı konu seçilebilir. Bu konular şunlar olabilir:

- Parola kullanımı ve yönetimi
- Virüsten, arka kapı programları ve zararlı yazılımlardan korunma
- Politikalar
- Bilinmeyen e-posta eklentileri
- Web kullanımı, uygunsuz kullanım şekillerine karşı uyarma
- Veri depolama ve yedekleme
- Sosyal mühendislik
- Acil durum müdahale
- Bilgi sisteminin tanıtımı
- El cihazları güvenliđi
- Gizli bilginin İnternet üzerinden iletimi (şifreleme)
- Dizüstü bilgisayar güvenliđi
- Yazılım yamalarının uygulanması
- Yazılım lisansı konuları
- Kurum sisteminde izin verilen yazılım türleri
- Erişim kontrolü konuları
- Ziyaretçi kontrolü ve fiziksel erişim kuralları

- Masaüstü güvenliđi, temiz ekran temiz masaüstü
- Baskı ve basılı doküman güvenliđi

### 3.2.1.2 Bilinçlendirme Materyali Kaynakları

Bir bilinçlendirme programı kapsamında başvurulabilecek pek çok kaynak bulunmaktadır. Bu kaynaklar belli bir güvenlik konusu hakkında olabileceđi gibi bilinçlendirme süreci oluşturmaya yönelik de olabilir. Kullanılabilecek güncel kaynaklar:

- Sektör ile ilgili haber gruplarının e-postaları, akademik enstitülerin yayınları
- Profesyonel eğitim ve bilgi güvenliđi kuruluşları
- Bilgi güvenliđi web siteleri
- Süreli yayınlar, dergiler
- Konferans, seminer ve kurslar

### 3.2.2 Eğitim Materyallerinin Geliştirilmesi

Eğitim materyallerini geliştirmeye başlamadan önce şu sorunun cevaplanması gerekir: “İlgili personele ne gibi bilgi güvenliđi yetenekleri kazandırmak istiyoruz?” Eğitim materyalinde kullanılacak konuların belirlenmesi gerekir. Ayrıca her materyalin hedef kitlesine uygun olması sağlanmalıdır. Seçilecek eğitim konularının daha çok belli bir alan üzerinde yoğunlaşmış olmasına, katılımcılara ihtiyaç duyulan konularda belli kabiliyetleri kazandırabilmesine dikkat etmek gerekmektedir.

#### 3.2.2.1 Eğitim Materyali Kaynakları

Bir eğitim programı kapsamında başvurulabilecek kaynakları tespit ederken atılacak ilk adım materyalin kurum içinde mi geliştirileceđi yoksa dışarıdan mı alınacağına karar verilmesidir. Eğer kurum eğitim materyalinin geliştirilmesi için gerekli kaynakları içeriden temin edebilecek yetkinliğe sahipse bunu kendisi yapabilir. Aşağıda eğitim materyali geliştirilmesi konusunda dış kaynak kullanımı kararının alınmasında değerlendirilmesi gereken kriterler verilmektedir:

- Kurum olarak yeterli kaynađa sahip miyiz? Uygun kabiliyet ve tecrübeye sahip personele sahip miyiz?
- Materyalin kurum içinde geliştirilmesi dış kaynak kullanımına oranla daha maliyet etkin bir çözüm mü?

- Eğitim materyali geliştirmenin maliyetini karşılamak için mevcut bir mekanizma var mı? Bu iş için ayrılan bütçe ne kadar olmalıdır?
- Eğitim materyali dışarıdan bir kuruluş tarafından geliştirilecekse, bunu takip ve kontrol edebilecek kaynaklara sahip miyiz?
- Geliştirilecek eğitim materyali içeriğinin gizlilik derecesi dış kaynak kullanımını engeller mi?
- Kritik eğitimlerin takvimi dış kaynak kullanımı ile geliştirilecek materyal ile planlanan zamanda sağlanabilir mi?

### **3.3 Bilinçlendirme ve Eğitim Sürecinin Uygulanması**

Sürecin uygulamaya konması aşamasında ilk olarak yeterli kaynak ve desteğın temin edilmesi amacıyla planın kuruma anlatılması ve ayrıntılı olarak açıklanması gerekir. Bilinçlendirme ve eğitim sürecine kurumun neden ihtiyacı olduđu yönetime izah edilmeli ve süreçten elde edilecek kazanımlara vurgu yapılmalıdır. Bütçe ile ilgili konuların mutlaka açıklıđa kavuşmuş olması sağlanmalıdır. Sürecin maliyeti hangi bütçe ile karşılanacağı belirlenmelidir. Sürecin uygulanmaya konmasında görev alacak personelin rol ve sorumlulukları net bir şekilde belirlenmeli ve ilgililere duyurulmalıdır.

Sürecin uygulanmasında izlenecek planın yönetim tarafından onaylanmasının ardından uygulama sürecine başlanabilir. Bilgi güvenliđi bilinçlendirme ve eğitim materyalinin kurum çapında nasıl sunulacağı ve dağıtılacağına ilişkin çok sayıda yöntem mevcuttur.

#### **3.3.1 Bilinçlendirme Materyali Sunum Teknikleri**

Bilinçlendirme materyalinin personele sunumunda başvurulabilecek pek çok farklı teknik ve yöntem bulunmaktadır. Bunlardan bazıları aşağıda verilmektedir:

- Kalem, not kağıdı, kahve fincanı, fare altlığı gibi nesnelere yazılabilecek uyarıcı mesajlar
- Uyarıcı ve bilgilendirici posterler (“şunu yapın”, “şunu yapmayın” içerikli mesajlar)
- Ekran koruyucularında veya sisteme girişte ekrana gelebilecek bilgi güvenliğine yönelik mesajlar
- Kurum gazetesi ve dergisinde yayınlanabilecek bilgi güvenliğine yönelik yazılar, yaşanmış öyküler

- Her masaya bırakılacak renkli kağıtlara basılı bültenler
- Belli zaman aralıklarında tüm kurum çapında gönderilecek e-postalar
- İnteraktif sunumlar
- Bilgi güvenliđi uzmanlarının vereceđi seminerler
- Bilgi güvenliđi günleri veya benzeri aktiviteler
- Ödül programları (bilgi güvenliđine teşvik edici davranışları ödüllendirme)

### **3.3.2 Eğitim Materyali Sunum Teknikleri**

Eđitim materyalinin personele sunumunda başvurulabilecek pek çok farklı teknik ve yöntem bulunmaktadır. Bunlardan bazıları aşağıda verilmektedir:

- İnteraktif video tabanlı eğitimler
- Web tabanlı eğitimler
- Bilgisayar tabanlı eğitimler
- Sınıf içi eğitimci önderliğinde eğitimler

## KAYNAKÇA

- [1]. NIST Special Publication 800-50 “Building an Information Technology Security Awareness and Training Program”
- [2]. NIST Special Publication 800-16 “Information Technology Security Training Requirements: A Role- and Performance-Based Model”
- [3]. Dancho Danchev, “Building and Implementing a Successful Information Security Policy“, <http://www.windowssecurity.com>
- [4]. Douglas Alfred, “Awareness, A Never Ending Struggle”, [http://www.sans.org/reading\\_room](http://www.sans.org/reading_room)
- [5]. Michelle Johnston, “Security Awareness Training and Privacy”, [http://www.sans.org/reading\\_room](http://www.sans.org/reading_room)
- [6]. David Sustaita, “Security Awareness Training Quiz - Finding the WEAKEST link!”, [http://www.sans.org/reading\\_room](http://www.sans.org/reading_room)
- [7]. Chris Garrett , “Developing a Security-Awareness Culture –Improving Security Decision Making”, [http://www.sans.org/reading\\_room](http://www.sans.org/reading_room)
- [8]. Chelsa Russell, “Security Awareness – Implementing an Effective Strategy”, [http://www.sans.org/reading\\_room](http://www.sans.org/reading_room)
- [9]. Fred Hinchcliffe, “Creating the effective Security Awareness Program and Demonstration”, [http://www.sans.org/reading\\_room](http://www.sans.org/reading_room)
- [10]. “Information Security and ISO27001 – An Introduction”, [www.itgovernance.co.uk/files/Infosec\\_101v1.1.pdf](http://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf)
- [11]. “How to Establish an ISMS Management Framework” , <http://www.isms.jipdec.jp/en/isms/frame.html>