

Döküman No	DBY.PR.01
Yayın Tarihi	01.01.2015
Revizyon No	01
Revizyon Tarihi	01.01.2020
Sayfa No	1/3

1. AMAÇ:

Bilgi Yönetim Sistemi Politikası (BYSP), Uzmandent Diş Hastanesi bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır. Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi diğer kıymetli varlıklarımızın içinde en çok ihmal edilen fakat kurum açısından en önemli varlıklardan biridir. Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilir bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir.

2. KAPSAM:

Bu politika kurum bilgi işlem altyapısını kullanmakta olan tüm birimleri ve bağlı kuruluşları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamakla birlikte;

- Veri dosyaları, sözleşmeler vb. den oluşan bilgi varlıkları,
- Uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları, c) Yönlendirici cihazları, güvenlik cihazları, sistem yönetim sunucuları, yasal yükümlülükler kapsamında kurulmuş sunucu sistemleri, bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıkları,
- Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,
- Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıklarını kapsamaktadır.

3. KISALTMALAR:

BYSP: Bilgi Yönetim Sistemi Politikası

4. SORUMLULAR:

Üst yönetim ve Bilgi İşlem Birim Personelleri Sorumludur.

Hazırlayan :
Kalite Yönetim Direktörü

Onaylayan:
Başhekim

Döküman No	DBY.PR.01
Yayın Tarihi	01.01.2015
Revizyon No	01
Revizyon Tarihi	01.01.2020
Sayfa No	1/3

5. FAALİYET AKIŞI:

5.1. BİLGİ GÜVENLİĞİ HEDEFLERİ VE PRENSİPLERİ

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesinin kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir.

- Kurumu içeriden veya dışarıdan gelebilecek tehditlere karşı korumak,
- Üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak kurumun imajını korumak,
- Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak
- Bilgi Güvenliği Prosedürlerini yerine getirerek personelin bilgi güvenliği farkındalıklarını artırmak amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

5.1.1.HEDEF ;

- Kurumu içeriden veya dışarıdan gelebilecek tehditlere karşı korumak,
- Üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak kurumun imajını korumak,
- Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak
- Bilgi Güvenliği Prosedürlerini yerine getirerek personelin bilgi güvenliği farkındalıklarını artırmak Amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

5.1.2.BİLGİ GÜVENLİĞİ İLKELERİ :

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,

Hazırlayan :
Kalite Yönetim Direktörü

Onaylayan:
Başhekim

Döküman No	DBY.PR.01
Yayın Tarihi	01.01.2015
Revizyon No	01
Revizyon Tarihi	01.01.2020
Sayfa No	1/3

- Bilgi güvenliği ihlal olaylarını bilgi güvenliği yetkilisine bildirmeli, raporlamalı ve 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 amacı kullanılamaz.
- Kurumun tüm çalışanları; bu politikaya, izlek ve talimatlarına uymakla sorumludur. h- İş süreçlerinin gereksinimi olarak her türü bilgi, en az kesintiyle kapsam dâhilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.
- Bilgilerin bütünlüğü her durumda korunacaktır.
- Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.
- Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.
- Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.

Hazırlayan :
Kalite Yönetim Direktörü

Onaylayan:
Başhekim