BGYS POLİTİKASI

BGYS Politikası, T.C. Sağlık Bakanlığı Gaziantep İl Sağlık Müdürlüğü ile Bağlı Tüm Birimler bünyesinde yürütülen Bilgi Güvenliği Yönetim Sistemi çalışmalarına ait kapsam, içerik, yöntem, BGYS Alt Komisyonu, ilgili komisyona ait görev ve sorumluluklar, uyulması gereken kurallar bütünü, kurumun bilgi güvenliği vizyonu, üst yönetimin ve komisyonun bilgi güvenliği taahhüdü ile bilgi güvenliği faaliyetlerinin nasıl yürütüleceği konularını içermektedir.

1. AMAÇ

Bu Bilgi Güvenliği Politikası, etkin ve yerleşmiş bilgi teknolojileri güvenlik süreçleri, politikaları, sözleşmeleri, formları, prosedürleri ve talimatları aracılığıyla sağlık hizmetlerinden faydalanan vatandaşa ait bilgilerin ya da kurumsal hizmetlerin icra edilmesi esnasında edinilen bilgi ve kaynakların güvenliğini, bütünlüğünü ve kullanılabilirliğini sağlamayı amaçlamaktadır.

2. KAPSAM

"Bilgi Güvenliği Yönetim Sistemi Politikası" dokümanında yer alan kriterler, İslahiye Devlet Hastanesi ve Bağlı Tüm Birimlerinde görevli tüm personel ile aşağıda belirtilen varlık ve teknoloji kategorilerini kapsamaktadır.

a) Veri dosyaları, sözleşmeler ve benzeri tüm bilgi varlıkları,
b) Tüm uygulama ve sistem yazılımları,
c) Güvenlik cihazları (Firewall), sunucular (Server), tüm personel bilgisayarları (Client), iletişim donanımları ile veri depolama ortamları,
d) Diğer fiziksel varlıklar (Aydınlatma, İklimlendirme, Kablolama vs.),
e) Kurum tarafından üretilen, kullanılan ve geliştirilen tüm yazılım ve verileri kapsar.

3. TANIMLAR VE KISALTMALAR

Varlık: İslahiye Devlet Hastanesi iş süreçleri için değeri olan, kaybı halinde iş ve işlemleri aksayacağı, insan, yazılım, donanım, itibar ve bilgi gibi unsurların tümünü ifade etmektedir.
Gizlilik: Bilginin yalnızca yetkili personel tarafından erişebilir olması durumunu ifade etmektedir. Bütünlük: Bilginin yetkisiz değiştirmelerden korunması, değişiklik durumunda farkına varılması ve tüm birimler ve personel için ortak anlam taşımasını ifade etmektedir.
Erişilebilirlik: Bilginin yetkilendirilmiş personel tarafından anlık olarak erişilebilmesini ifade etmektedir. Bilgi güvenliği ihlal olayı: İş operasyonlarını tehlikeye atma, bilgi akışını engelleme veya yavaşlatma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen/beklenmeyen olay ya da olayları ifade etmektedir.
Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, sözleşmeleri, talimatları, prosedürleri, prosesleri ve tüm kaynakları içerir.
SBSGM: T.C. Sağlık Bakanlığı Sağlık Bilgi sistemleri Genel Müdürlüğünü ifade etmektedir.

4. HEDEF VE PRENSİPLER

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak gerekli tüm önlemleri almak amacıyla aşağıda detayları verilen risk yönetimi faaliyetleri yürütülmektedir. Bu kapsamda her bir varlık için risk seviyesinin, kabul edilebilir risk seviyesinin altında tutulması hedeflenmektedir.

Kurumu içeriden veya dışarıdan gelebilecek tehditlere karşı korumak, üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak kurumun imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak ve risk yönetimi ile kontrollerinin uygulanması sürekli bir faaliyet olduğundan dolayı kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılmasını hedeflenmektedir.

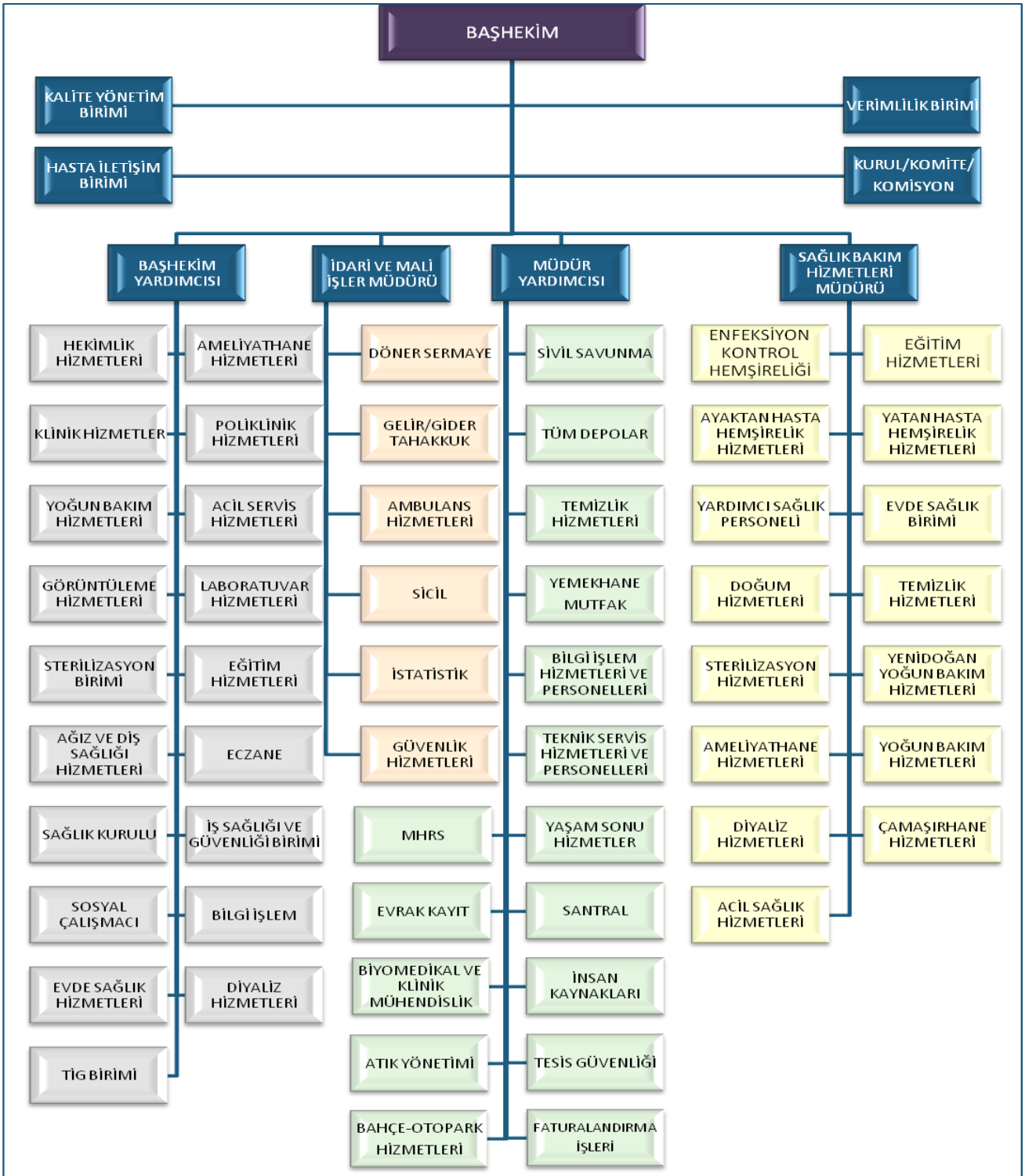
Temel prensiplerimiz; Bilgi güvenliği kapsamında yer alan basılı ve elektronik ortamdaki tüm bilgilerin, yasal mevzuat ışığında ve risk değerlendirme metotları kullanılarak "gizlilik, bütünlük ve erişilebilirlik" ilkelerine göre yönetilmesi amacıyla;

- Bilgi güvenliği standartlarının gerekliliklerini yerine getirmek,
- Bilgi güvenliği ile ilgili tüm yasal mevzuata BGYS kılavuzu çerçevesinde uyum sağlamak,
- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
- BGYS'yi sürekli gözden geçirmek ve iyileştirilmesi için BGYS'ye katkıda bulunmak,
- Bilgi güvenliği farkındalığını artırmak için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirme vizyon ve misyonuyla hareket etmektedir. Şeklinde sıralanabilir.

5. BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU

Bu politika metninde belirtilen 1. ve 2. Madde de tarifi yapılan kapsam dâhilinde TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Standartları gerekliliklerini yürütmek üzere T.C. Sağlık Bakanlığı Gaziantep İl Sağlık Müdürlüğü bünyesinde 65587614-719-E.499 sayılı Makam Oluru ile bir BGYS Alt Komisyonu kurulmuştur. Bu komisyon BGYS faaliyetlerini değerlendirmek üzere 6 (Altı) ayda bir toplanacaktır.

a) KURUM ORGANİZASYON ŞEMASI


BAŞHEKİM
KALİTE YÖNETİM BİRİMİ
HASTA İLETİŞİM BİRİMİ
VERİMLİLİK BİRİMİ
KURUL/KOMİTE/ KOMİSYON
BAŞHEKİM YARDIMCISI
İDARİ VE MALİ İŞLER MÜDÜRÜ
MÜDÜR YARDIMCISI
SAĞLIK BAKIM HİZMETLERİ MÜDÜRÜ
HEKİMLİK HİZMETLERİ
KLİNİK HİZMETLER
YOĞUN BAKIM HİZMETLERİ
GÖRÜNTÜLEME HİZMETLERİ
STERİLİZASYON BİRİMİ
AĞIZ VE DİŞ SAĞLIĞI HİZMETLERİ
SAĞLIK KURULU
SOSYAL ÇALIŞMACI
EVDE SAĞLIK HİZMETLERİ
TİG BİRİMİ
AMELİYATHANE HİZMETLERİ
POLİKLİNİK HİZMETLERİ
ACİL SERVİS HİZMETLERİ
LABORATUVAR HİZMETLERİ
EĞİTİM HİZMETLERİ
ECZANE
İŞ SAĞLIĞI VE GÜVENLİĞİ BİRİMİ
BİLGİ İŞLEM
DİYALİZ HİZMETLERİ
DÖNER SERMAYE
GELİR/GİDER TAHAKKUK
AMBULANS HİZMETLERİ
SİCİL
İSTATİSTİK
GÜVENLİK HİZMETLERİ
MHRS
EVRAK KAYIT
BİYOMEDİKAL VE KLİNİK MÜHENDİSLİK
ATIK YÖNETİMİ
BAHÇE-OTOPARK HİZMETLERİ
SİVİL SAVUNMA
TÜM DEPOLAR
TEMİZLİK HİZMETLERİ
YEMEKHANE MUTFAK
BİLGİ İŞLEM HİZMETLERİ VE PERSONELLERİ
TEKNİK SERVİS HİZMETLERİ VE PERSONELLERİ
YAŞAM SONU HİZMETLER
SANTRAL
İNSAN KAYNAKLARI
TESİS GÜVENLİĞİ
FATURALANDIRMA İŞLERİ
ENFEKSİYON KONTROL HEMŞİRELİĞİ
AYAKTAN HASTA HEMŞİRELİK HİZMETLERİ
YARDIMCI SAĞLIK PERSONELİ
DOĞUM HİZMETLERİ
STERİLİZASYON HİZMETLERİ
AMELİYATHANE HİZMETLERİ
DİYALİZ HİZMETLERİ
ACİL SAĞLIK HİZMETLERİ
EĞİTİM HİZMETLERİ
YATAN HASTA HEMŞİRELİK HİZMETLERİ
EVDE SAĞLIK BİRİMİ
TEMİZLİK HİZMETLERİ
YENİDOĞAN YOĞUN BAKIM HİZMETLERİ
YOĞUN BAKIM HİZMETLERİ
ÇAMAŞIRHANE HİZMETLERİ

b) BGYS KOMİSYONU GÖREVLENDİRME TABLOSU

ADI	SOYADI	UNVANI	GÖREVİ
MUSTAFA	YILDIZ	UZMAN HEKİM - BAŞHEKİM	BAŞKAN
FATMA	ŞAHİN	SAĞLIK BAKIM HİZMETLERİ MÜDÜRÜ	ÜYE
AHMET	YILMAZ	İDARİ VE MALİ İŞLER MÜDÜRÜ	ÜYE
MUHARREM	ÇİL	MÜHENDİS	ÜYE
FERİHA	DURAN	MEMUR	ÜYE
FERUZ	BOZGEYİK	SBYS SORUMLUSU	ÜYE
MURAT	KAPLAN	GÜVENLİK HİZMETLERİ SORUMLUSU	ÜYE

c) BGYS GÖREV, YETKİ VE SORUMLULUKLARI

Komisyon üyelerinden biri sekreter olarak belirlenir.

Düzenli aralıklarla toplanır. Ekip bilgi güvenliği ile ilgili mevcut durum tespitini yapar ve olası riskleri belirler. Tanımlı kullanıcılar için yapılan yetki değişikliklerini izler. Çalışanlar tarafından bilgi güvenliği açısından karşılaşılan olaylar hakkında iletilen sorunlar ve gündem maddelerini görüşür, takip eder ve gerektiğinde düzeltici önleyici faaliyetleri başlatır. Donanım ile ilgili cihaz ve malzeme istemlerini görüşerek değerlendirir. BYS'de yapılan güncellemelerin değerlendirilmesi, onayı ve çalışanlara duyurulmasından sorumludur. Hastanede kullanılan veri tabanlarında yedekleme, bilişim güvenliği alt yapısını denetler. BYS'ye entegre edilecek modüllerin seçilmesi, entegrasyonların yapılması ve kontrolünün yapılmasını sağlar. Bilgi yönetim sistemi personelinin çalışma düzenini planlar ve denetler. Hizmette gereken sarf malzemenin gerekliliğini değerlendirerek teminini sağlar.

f) BİLGİ GÜVENLİĞİ YETKİLİSİ GÖREV, YETKİ VE SORUMLULUKLARI

1. BGYS Alt Komisyonundan aldığı yetkiye dayanarak SBSGM ile koordineli bir şekilde ve İslahiye Devlet Hastanesi ve bağlı birimler bünyesinde bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek.
2. Ana ilkeler doğrultusunda SBSGM tarafından aldığı eğitimler ile BGYS Komisyonunu yönlendirmek ve İslahiye Devlet Hastanesi'nde bilgi güvenliği ile ilgili konulardaki SBSGM'nin icra organı olarak hareket etmek.
3. BGYS komisyonundan aldığı yetkiye dayanarak bilgi güvenliği ile ilgili faaliyetleri yürütürken kurumda görev yapan tüm personel ile uygun yöntemlerle iletişim kurmak, personeli yönlendirmek.

1. BGYS İLKELERİ

1. Bilgi güvenliği ilkeleri, kurumdaki bilgi güvenliği ile ilgili genel kuralları koyar. Bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlar.
2. Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:
   a) Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
   b) Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
   c) Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,
   d) Bilgi güvenliği ihlal olaylarını Bilgi Güvenliği Yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.
3. Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.
4. Kurum bilişim kaynakları, T.C. Yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacı ile kullanılamaz.
5. Kurumun tüm çalışanları; bu politika ile diğer desteklenen politikalara, prosedürlere, ve talimatlarına, formlar ve sözleşme gerekliliklerine uymakla sorumludur.
6. İş süreçlerinin gereksinimi olarak her türü bilgi, en az kesintiyle kapsam dâhilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.
7. Bilgilerin bütünlüğü her durumda korunacaktır.
8. Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.
9. Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.
10. Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.

6. BİLGİ HASSASİYETİ VE RİSKLER

a) BİLGİ VARLIKLARIMIZ

İslahiye Devlet Hastanesi ve Bağlı Kuruluşlar bünyesinde bu politika metninin 3. maddesinde belirtilen kapsam dâhilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları iş ve işlemlerde üretilen bilgiler envantere kayıtlı olup olmadıklarına bakılmaksızın bilgi varlıklarımızın bütünüdür.

Masaüstü bilgisayarlar, laptoplar, tabletler, telefonlar, CD, DVD ve USB Bellek ortamındaki tüm veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (İnternet, Email, Telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

b) VARLIKLARIN KATEGORİLERİ

İş Süreçleri: Kurumsal bilgi varlıklarının kullanıldığı, çeşitli vasıtalarla hassas bilgilerin yoğun olarak işlendiği iş süreçleri (hasta kabul, heyet işlemleri, tıbbi kayıt arşiv vb.).

Kurumsal Bilgi Varlıkları: Elektronik veya kâğıt ortamda tutulan hasta kayıtları, personel kayıt ve dosyaları, kurumsal evraklar, bilgisayarlarda saklanan ve kurum için değeri olan veriler, raporlar, listeler, çizimler, veri tabanları, veri tabanı yedekleri, faturalar, sözleşmeler, teklifler, telifler, lisanslar vb.

Yazılımlar: İşletim sistemleri, ofis uygulamaları, HBYS yazılımları, laboratuvar yazılımları, tıbbi görüntüleme yazılımları, kurumsal yazılımlar (EBYS, ÇKYS, KPS, HİTAP vb.) vb.

Fiziksel varlıklar: Sunucular, masaüstü bilgisayarlar, taşınabilir bilgisayarlar, depolama birimleri, yedekleme birimleri (kasetler, hard diskler vb.), aktif cihazlar (anahtarlama cihazı, güvenlik duvarı, yönlendirici, ağ erişim cihazı, anahtar, modem, erişim noktası vb), fakslar, fotokopiler, yazıcılar, santraller, telefonlar, evrak imha cihazları, ağa bağlı olarak çalışan veya ağa bağlanma arayüzleri olan tıbbi cihazlar vb.
İnsan Kaynakları: Çalışanlar. Altyapı: Yapısal ve elektrik kablolama altyapısı, UPS, jeneratör, iklimlendirme, giriş/çıkış kontrol sistemleri, kamera sistemleri, yangın, duman uyarı sistemleri, yangın söndürme sistemleri, destek teçhizatı vb.
Mekânlar: Yönetim ve hizmet odaları, sunucu odaları, arşiv odaları, tıbbi kayıt saklama odaları vb.

c) VARLIK SINIFLANDIRILMASI

BİLGİ SINIFLANDIRMA KILAVUZU		**SAKLANMA YERİ VE ŞEKLİ**
GİZLİ ÇOK GİZLİ ÖZEL HİZMETE ÖZEL	Bilgi varlıklarına (resmi yazılar dâhil) verilecek gizlilik dereceleri için 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe giren "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar" ile 2017/21 sayılı "e-Yazışma Projesi" isimli genelge dikkate alınır. Bu tür bilgiler kurum için en kritik bilgilerdir ve sadece yetkili personelin erişim izni vardır. Çok gizli gizlilik dereceli evrak ve dokümanlar, Kurumun en üst düzey yöneticisi tarafından belirlenen ve yazılı olarak görevlendirilen kişi veya kişiler tarafından hazırlanır ve özel usullere göre dağıtımı yapılır. Gizlilik ön plandadır.	Bu tip evrak ve dokümanlar korumalı-kilitli odalarda, kasa, çelik masa veya diğer tipte çelik dolaplar içinde ve/veya parola ve erişim politikalarına uyumlu olacak şekilde güvenliği sağlanmış olan kişisel bilgisayarlarda muhafaza edilir. Hizmete özel evraklar ise masa gözlerinde kilitli olmak şartıyla muhafaza edilir.
İÇ KULLANIM	Sadece birimlere özel bilgilerdir. Birim çalışanları haricinde yetkisiz duruma bulunan hiç kimsenin veya kurumun-kuruluşun görmemesi gereken bilgilerdir. Gizlilik ön plandadır.	Birimlere ait korumalı dolaplarda ve/veya parola ve erişim politikalarına uyumlu olacak şekilde güvenliği sağlanmış olan kişisel bilgisayarlarda muhafaza edilir.
KİŞİSEL	Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kuruma ait iş ve işleyişler için yapılan kişisel çalışmalar bu	Çalışma masalarına ait korumalıkilitli çekmecelerde muhafaza edilir.

	kapsama girmektedir. Kurum iş ve işleyişine ait olmayan bilgiler bilgisayarlar veya dolaplarda tutulmamalıdır. Erişilebilirlik ön plandadır.	
KURUMA AÇIK	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Aynı ya da farklı birimlerde görevli personelin ortak kullanım amacıyla erişebildikleri bilgilerdir.	Birimlere ait kilitli dolaplar ya da politikalara uygun bir şekilde oluşturulmuş parola korumalı sunucu/bilgisayarlarda muhafaza edilir.
HALKA AÇIK	Bu bilgiler T.C. Sağlık Bakanlığı iznine tabi olan ve bağlı Genel Müdürlükler/Birimler ile Taşra Teşkilatına ve tedarikçiler ile halka açık olan bilgilerdir. Erişilebilirlikleri ve süreklilikleri ön plandadır.	Dolaplar, bilgisayarlar, internet ortamı vb. ortamlarda muhafaza edilir.

Sağlık verilerinin korunmasına yönelik risk analizi yapılırken, kişisel verilerin hassasiyeti ve kanuna aykırı bir şekilde ifşası halinde uygulanacak ağır idari ve cezai yaptırımlar nedeniyle en üst düzeyde özen gösterilmelidir.

7. BİLGİ GÜVENLİĞİ EĞİTİMLERİ

a) BGYS EĞİTİMLERİ

Hastanemiz ile bağlı kurumlar ve personelin sahip olduğu en değerli varlıkları olan kurumsal ya da kişisel bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli korunması gerekmektedir. Koruma bir takım fiziksel ve sistemsel önlemlerin yanında bireylerin bilgi güvenliğine ilişkin tehdit ve risklerden, kurum bilgi güvenlik politika ya da kurallarından haberdar olması, bu tehditlere nasıl karşı koyabileceği, olası riskleri mümkün olabilecek en düşük risk düzeyinde nasıl tutabileceği konusunda bilgilenmesiyle mümkün olabilir. Güvenliğin en zayıf halkası olarak da kabul edilen insan faktörü üzerinde çeşitli farkındalık programları uygulanması gerekmektedir. Bu programların en başında ise bilgi güvenliği eğitimi yer alır. Kurumumuzda gerekli görüldüğü hallerde görevli tüm personele belirli zaman dilimlerinde aşağıdaki eğitim verilecektir.

b) EĞİTİM İÇERİKLERİ

1. Bilgi Güvenliği Yönetim Sistemi Standardı ve Farkındalık Eğitimi
2. Adli Bilişim ve BGYS Hukuksal Boyutu Eğitimi
3. BGYS Siber Güvenlik Eğitimi
4. BGYS Son Kullanıcı Güvenlik Eğitim
5. Sosyal Medya Eğitimi
6. E-Posta Güvenliği Eğitimi