1.1.Giriş

Bu doküman **Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğünün** hazırlamış olduğu Bilgi Güvenliği Politikaları Yönergesi ve kılavuzuna uyum çalışmaları kapsamında hazırlanmış olup, **Gölbaşı Şehit Ahmet Özsoy Devlet Hastanesi'nde** yürütülen Bilgi Güvenliği çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içermektedir. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

1.2.Tanım

Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır.

Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilginin yer aldığı belli başlı ortamlar;

•**Fiziksel ortamlar**; Kâğıt, tahta, pano, faks, Çöp/Atık kâğıt kutuları, Dolaplar vb

•**Elektronik ortamlar**; Bilgisayarlar, mobil iletişim cihazları, e-posta, USB, CD, Disk, Disket vb manyetik ortamlar.

•**Sosyal ortamlar**; Telefon görüşmeleri, kişiler arası iletişim, yemek araları, toplu tasıma araçları vb sosyal aktiviteler.

•**Tanıtım platformları**; internet siteleri, WEB, broşürle, reklamlar, sunular, eğitimler, video ya da görsel ortamlar.

Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür

1.3. Amaç

Bilgi Güvenliği Politikasının amacı; **bilginin gizlilik, bütünlük ve erişilebilirlik** kapsamında değerlendirilerek içeriden ve/veya dışarıdan gelebilecek, kasıtlı veya kazayla oluşabilecek tüm

tehditlerden korunması ve yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesini temin etmektir.

Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek 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.

Bilgi Güvenliğinin üç unsuru;

A-Gizlilik:
Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesi. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

B-Bütünlük:

Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz.

C-Kullanılabilirlik (Erişilebilirlik):

Yetkilendirilmiş kullanıcıların, gerek duyduklarında bilgiye ve ilişkili kaynaklara erişime sahip olabileceklerinin garanti edilmesi. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

1.4.Kapsam:

Bu politika Kurum Bilgi İşlem 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;

a. Veri dosyaları, sözleşmeler vb. den oluşan bilgi varlıkları,

b. 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 varlıklar,

d. Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,

e. Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıklarını kapsamaktadır.

1.5.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.

1.6.Bilgi Güvenlik 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 Bilgi Güvenliği Yetkilisine bildirmeli, raporlamalı ve bu ihlalleri engelleyecek önlemleri almalıdır.
- Kurum içi bilgi kaynakları (duyuru, döküman 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, prosedür ve talimatlarına uymakla sorumludur.

- 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

2. BİLGİ GÜVENLİĞİ ORGANİZASYONU

2.1. Bilgi Güvenliği Komisyonu:

Bilgi Güvenliği Yönetim Hizmet Kalite Standartlarının gerekliliklerini yürütmek üzere Gölbaşı Hasvak Devlet Hastanesi bünyesinde oluşturulmuştur.

Komisyon Başkanı:

Üyeler

1. Ali Niyazi KURTCEBE (Başhekim Yardımcısı)
2. Oktay ETYEMEZ (İdari ve Mali İşler Müdür Yardımcısı)
3. Dr. Mustafa YÜCE
4. Sermin Ulubey (Bilgi İşlem Sorumlusu)
5. Hatun AKDEMİR (Bilgi İşlem)
6. Hasan KARAHAN (Bilgi İşlem-Veri Tabanı görevli)

2.2. Bilgi Güvenliği Üst Yönetim Görev, Yetki ve Sorumluluklar:

- Bilgi Güvenliği altyapısını oluşturmak için sunulacak projelere ait yönetim temsilcilerini atamak ve yetkilendirmek.

- Bilgi Güvenliği Komisyonu tarafından hazırlanmış Bilgi Güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için Bilgi Güvenliği Komisyonu tarafından hazırlanmış projelere gerekli kaynağı sağlamak.

- Bilgi Güvenliği Komisyonu tarafından kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.

- Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanlar (Danışmanlar ve yüklenici firma personeli dahil) Bilgi Güvenliği farkındalığının artırılmasına yönelik planlanan çalışmaların etkinliğinin artırılması için teşvik edici faaliyetleri onaylamak.

- Bilgi Güvenliği konularında yapılacak olan çalışmalarına işlerlik kazandırmak, sürdürmek iyileştirmek ve gözden geçirmek için gerekli iç denetimlerin yapılmasına onay vermek.

2.4. Çalışan Görev, Yetki ve Sorumlulukları:
Bilgi Güvenliği Komisyonu tarafından hazırlanan ve üst yönetim tarafından onaylanan tüm bilgi güvenliği kurallarına kendi çalışma alanlarının gerektirdiği şekilde uymak.

3. BİLGİ GÜVENLİĞİ EĞİTİMLERİ

Günümüzde kurumlar ve bireylerin sahip olduğu en değerli varlıkları olan 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 yada 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 çesitli farkındalık programları uygulanması gerekmektedir. Bu programların en başında ise bilgi güvenliği eğitimi yer alır.

4. İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ

1.Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.

2.Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.

3.ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında (izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.

4.Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.

5.İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.)uygun şekilde imhası gerçekleştirilmelidir.

6.Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

10.Sistemlerde kullanılan şifreler, masa üstü veya ekran üstü gibi herkes tarafından görülebilecek yerlere yazılmamalı.

11.Personel, bilgisayarını belli bir süre kullanmadığı zaman otomatik olarak şifre ile oturum açmasını gerektirecek şekilde ayarlamalı.

12.Kullanıcı, gizli bilgi içeren evrakı ağ üzerinden paylaşmaz, gizli bilgi içeren atık evrakı imha eder.

13.Personel, bilgisayarındaki, USB belleğindeki, harici diskindeki ve benzeri veri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlüdür. USB veya harici diske gizli/önemli verilerin konulması gerekiyorsa kriptolanarak/şifrelenerek saklanır.

4.1. Bilgi Güvenliği İşe Başlama Ve İşten Ayrılma Süreç Prosedürü:

4.1.1 Amaç

Gölbaşı Şehit Ahmet Özsoy Devlet Hastanesi bünyesinde işe başlama ve işten ayrılma süreçlerinde uyulması gereken süreçleri ifade eder.

4.1.2 Kapsam

Gölbaşı Şehit Ahmet Özsoy Devlet Hastanesi Bilgi Güvenliği Politikası dokümanında kapsam maddesinde tanımlanmış alanlardır.

4.1.3 Uygulama

İşe Başlayış Prosedürü

- İşe başlayan her personele bilgi güvenliği ve sosyal mühendislik zafiyetleri konularında eğitim verilmelidir.

- Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

- Kullanacağı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri tanımlanmalıdır.

- EBYS tanımlaması için ilgili personellere *saglik.gov.tr* uzantılı e-mail adresi tanımlanmalıdır. İl içi yer değişikliklerinde ise sistem üzerinden kurum/birim değişikliği tanımlaması yapılmalıdır.

-Tüm personele kurum kimlik kartı çıkartılmalıdır.

İşten Ayrılış Prosedürü

-Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

-Görevden ayrılan personelin yaka kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

-Kullandığı bilgi sistemlerine yönelik (Tsim, Çkys, Ebys vb.) kullanıcı adı ve şifreleri sistem yöneticisi tarafından pasif hale getirilmelidir.

-Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.

-Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

-Görevden ayrılan personel işten ayrılma onay formunu doldurarak bağlı bulunduğu kurumun insan kaynakları birimine teslim etmelidir.

-İlgili form doldurulmadan personelin kurum ile ilişiği kesilmez.

5. PAROLA (ŞİFRE) GÜVENLİĞİ

1- Amaç

Bu politikanın amacı güçlü bir parola oluşturulması, oluşturulan parolanın korunması ve bu parolanın değiştirilme sıklığı hakkında standart oluşturmaktır.

2- Kapsam ve Sorumlular

Bu politika Gölbaşı Hasvak Devlet Hastanesi faaliyet gösteren tüm birimlerde çalışan ve bilgi sistemlerini kullanan kullanıcıları kapsamaktadır.

3- Politika Metni

Güvenli bir parola için aşağıdakiler yapılmalıdır.

- Parola en az 8 karakterden oluşmalıdır.
- Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içermelidir.
- Büyük ve küçük harfler bir arada kullanılmalıdır.
- Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

- Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi)
- Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.
- Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.

B yerine 8, Z yerine 2 gibi. Örnek: (Solaryum! = 501aryum!
S yerine 5, g yerine 9 gibi. (Kazak = Ka2ak)

- Basit bir cümle ya da ifade içerisindeki belirli kelimeler özel karakter veya rakamlarla değiştirilerek güçlü bir parola elde edilebilir.

Dün Kar Yağmış" : Dün*Yağm1$ ("kar", "yıldız" yerine '*')

- Parola iş arkadaşları, aile bireyleri ve tanımadığımız kişilerle paylaşılmamalıdır.
- Parola paylaşılmak zorunda kalınırsa vakit geçirmeden yenisiyle değiştirilmelidir.
- Kâğıtlara ya da elektronik ortamlara parola yazılmamalıdır.
- Parola her 6 ayda bir yukarıdaki kurallara göre yenisiyle değiştirilmelidir. Tavsiye edilen süre her üç ayda birdir.

6.BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ

6.1. Politika Metni:

- Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.
- Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.
- Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.
- İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
- Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.

- Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
- Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
- Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.
- Hacimsel küçültme işlemi için parçalanmalıdır.
- Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

6.1.2. Antivirüs Politikası:

- Bütün bilgisayarda kurumun lisanslı antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunma-malıdır.
- Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem birimine haber verilmelidir.
- Zararlı programları (örneğin, virüsler, solucanlar, truva atı, e-mail bombaları vb) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.
- Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını sisteme kuramaz.

6.1.3 Genel Kullanım Politikası:

- Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.
- Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
- Kurumda domain (çalışma alanı) yapısı varsa mutlaka login olunmalıdır. Bu durumda, domain' e bağlı olmayan bilgisayarların yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.
- Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimi' ne haber verilmelidir.
- Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur.
- Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.
- Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişmemelidir.
- Port veya ağ taraması yapılmamalıdır.

- Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.
- Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.
- Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
- Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.
- Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD' leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.
- Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
- Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, elektronik veya kâğıt ortamında üçüncü kişi ve kurumlara verilemez.
- Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü
- Bilgisayarlarındaki kurumsal bilgilerin güvenliği ile sorumludur.
- Bilgi İşlem birimi tarafından yetkili kişiler kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel kişisel bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.
- Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
- Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- Kurumda Bilgi İşlem biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb.) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.
- Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.
- Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisansız yazılımı bilgisayarında barından personel ilgili kanunlar karşısında kendisi sorumludur.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
- Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir.

7. İHLÂL BİLDİRİMİ VE YÖNETİMİ

- **7.1- Amaç**
- Gölbaşı Hasvak Devlet Hastanesi kapsamı dahilinde yaşanabilecek bilgi güvenliği ihlalleri noktasında durumun nasıl yönetileceğini ifade eder.
- **7.2- Kapsam ve Sorumlular**
- Gölbaşı Hasvak Devlet Hastanesi Bilgi Güvenliği Politikası dökümanında kapsam maddesinde tanımlanmış alanlardır.
- **7.3- Uygulama**

- Bilgi Güvenliği İhlal Olayları Gölbaşı Hasvak Devlet Hastanesi kapsamında aşağıdaki gibi yönetilmektedir.
- Bilgi güvenliği ile ilgili olaylar derhal rapor edilmelidir. Kurum politikalarına uymayan her tür davranış, kurum bilgi güvenliği prensipleri ve talimatlarına aykırı her tür bilgi paylaşımı, uygunsuz PC/Laptop kullanımı, yetkisiz girişler, uygun olmayan
- yerde yetkisiz personelin görülmesi, bilgisayar varlıkları ile ilgili arıza, hırsızlık, kaybolma vb. olumsuzluklar bilgi güvenliği olayı kapsamına girmektedir.

Bilgi güvenliği ihlâli oluşması durumunda kişilerin tüm gerekli faaliyetleri hatırlamasını sağlamak maksadıyla bilgi güvenliği olayı rapor formatı bir doküman halinde hazırlanmıştır. Olası bir tehdide meydan verecek bir zayıflığı tespit eden tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor etmelidir. Olay halinde müdahaleyi ilgili/yetkili birimler yaparlar.Olayı raporlayan kişinin müdahale etmemesi ve uzmanların müdahalesi için hiçbir şeye dokunmaması gerekmektedir.

Zayıflıklar şunlardan biri olabilir: politikaya direnen kullanıcılar, işletim sistemindeki eksik yamalar, epostalardaki spamın artması, sistemin yavaşlaması, cihazların fazla ısınması, giriş ve çıkışlarda tespit edilen yetkisiz girişe uygun alanlar ve durumlar, kapatılmayan kapılar, kilitlenmeyen dolaplar, kapatılmayan oturumlar (bilgisayarı açık bırakıp gitme), dağınık ve halka açık ortamlarda duran bilgiler ve bunun gibi konularda gözlemlenen ve Bilgi Güvenliği Komisyonunun dikkatinden kaçan konular.

7.4- Yaptırım

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği ve 657 sayılı Devlet Memurları Kanununun 125. Maddesi gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesi uygulayabilir:

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

Kurumsal Bilişim sistemlerinin güvenliğinde herhangi bir aksamaya mahal verilmemesi için genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında çalışanlarımızın da bu hususta titizlikle uyması gereken bu kurallara bütün kurum çalışanları uymak zorundadır.

8. İNTERNET VE ELEKTRONİK POSTA GÜVENLİĞİ

8.1. Amaç: Bu doküman, E-Posta mesajlarında alma, gönderme, yönlendirme ve otomatik gönderme kullanımına ait Gölbaşı Hasvak Devlet Hastanesi politikasını tanımlamaktadır.

8.2. Kapsam Bu politika, Gölbaşı Hasvak Devlet Hastanesi bünyesinde kurumun sağladığı resmi E-Posta kutusu olan tüm kullanıcılar içindir.

8.3. Politika Metni

1.Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.

2.İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.

3.Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.

4.Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.

5.İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta adresi bu mesajlarda kullanılamaz. Ancak iş gereği üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak Kurumun sağladığı resmi e-posta adresi kullanılabilir.

6.Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.

7.E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir.

8.Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.
9.E-postaya eklenecek dosya uzantıları “.exe”, “.vbs” veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip veya rar formatında) mesaja eklenmelidir.

10.E-postaya eklenecek dosya uzantıları “.exe”, “.vbs” veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip veya rar formatında) mesaja eklenmelidir.

11.Bakanlık ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

12.Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.

13.Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.

14.Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yönetimine haber verilmelidir.

15.Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmemelidir.

16.Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

17.Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.

18.Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.

19.Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.

20.Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

21.Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Sistem Yönetimine haber verilmelidir.

22.Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Bilgi Güvenliği Yetkilisine haber vermelidir.

8.4. Yaptırım

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla Bilgi Güvenliği Politikasında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

9. MAL VE HİZMET ALIM GÜVENLİĞİ

9.1.Amaç: Bu doküman mal ve hizmet alımlarında uyulması gereken Gölbaşı Hasvak Devlet Hastanesi politikalarını tanımlamaktadır.

9.2.Kapsam: Bu politika Kurum Bilgi İşlem 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 sağlayıcıları için hazırlanmış olup, mal ve hizmet alımında sorumluluğu olan tüm birim ve çalışanları kapsamaktadır.

9.3.Uyulması Gereken Kurallar:

1.Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.

2.Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

• Bilgi güvenliği politikası,

• Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,

• Gerekli fiziki koruma için kontrol ve mekanizmalar,

• Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,

• Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,

• Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,

• Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,

• Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,

• Kullanıcı ve yönetici eğitimlerinin methodu, prosedürü ve güvenliği,

Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,

• Uygun olduğu yerde personel transferi için hüküm,

• Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,

• Açık bir raporlama yapısı ve anlaşılan raporlama formatı,

• Değişim yönetimi sürecinin açıkça belirlenmesi,

• Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,

• İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,

• Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,

• Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,

• Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,

• Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,

• Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,

• Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,

• Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,

• Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,

• Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,

• Sorun çözümü için bir yükseltme sürecinin kurulması,

• Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dahil olmak üzere hizmet sürekliliği gerekleri,

• Anlaşmayla ilgili tarafların yükümlülükleri,

• Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak)

• Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,

• Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,

• Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,

• Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.

• Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi,

• Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

3.Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.

4.Bilgi güvenliği yönetimi dış kaynaklı ise anlaşmalarda üçüncü tarafın güvenlik garantisinin yeterliliğini nasıl ele alındığı anlaşmada belirtilmelidir. Risk değerlendirmede tanımlandığı gibi, risklerdeki değişiklikleri belirlemek ve başa çıkmak için güvenliğin nasıl adapte edileceği ve sürdürüleceği ele alınmalıdır.

5.Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesinti süresi, acil durum planlaması yönetmelikleri ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde; kuruluş değişiklikleri yönetmek için uygun süreçlere ve anlaşmaların yeniden müzakere edilmesi ya da fesh edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.

6.Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

7.Genellikle anlaşmaların esasları kuruluşlar tarafından geliştirilmiştir. Bazı durumlarda anlaşmaların üçüncü taraflarca geliştirilmesi ve kuruluşa empoze edilmesi durumu olabilir. Kuruluşlar, kendi yapılarına üçüncü taraflarca empoze edilecek anlaşmalarda kendi güvenliklerinin gereksiz yere etkilenmesini engeller.

9.4.Yaptırım: Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla Bilgi Güvenliği Politikasında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

10. SOSYAL MÜHENDİSLİK ZAFİYETLERİ VE SOSYAL MEDYA GÜVENLİĞİ

10.1. Sosyal Mühendislik Zafiyetleri

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaaflarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanırlar.

1.Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.
2.Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
3.Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.
4.Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.
5.Şifre kişiye özel bilgidir. Sistem yöneticiniz dahil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
6.Oluşturulan dosyaya erişecek kişiler ve hakları "bilmesi gereken" prensibine göre belirlenmelidir.
7.Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
8.Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
9.Kaza, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.
10.Sadece yetkili kişilerin kurum içersindeki sınırlı bölümlere erişim izni olduğundan emin olmak için uygun erişim kontrol mekanizmaları olması gerekir.
11.İnternette kurum ile ilgili paylaşılan bilgilere son derece dikkat edilmeli ve bu sürekli izlenmelidir.
12.'Bilmesi Gerektiği Kadar' prensibine göre hareket edilmelidir.

10.2. Sosyal Medya Güvenliği:

1.Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
2.Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
3.Kuruma ait hiçbir gizli bilgi, yazı, sosyal medyada paylaşılmamalıdır.