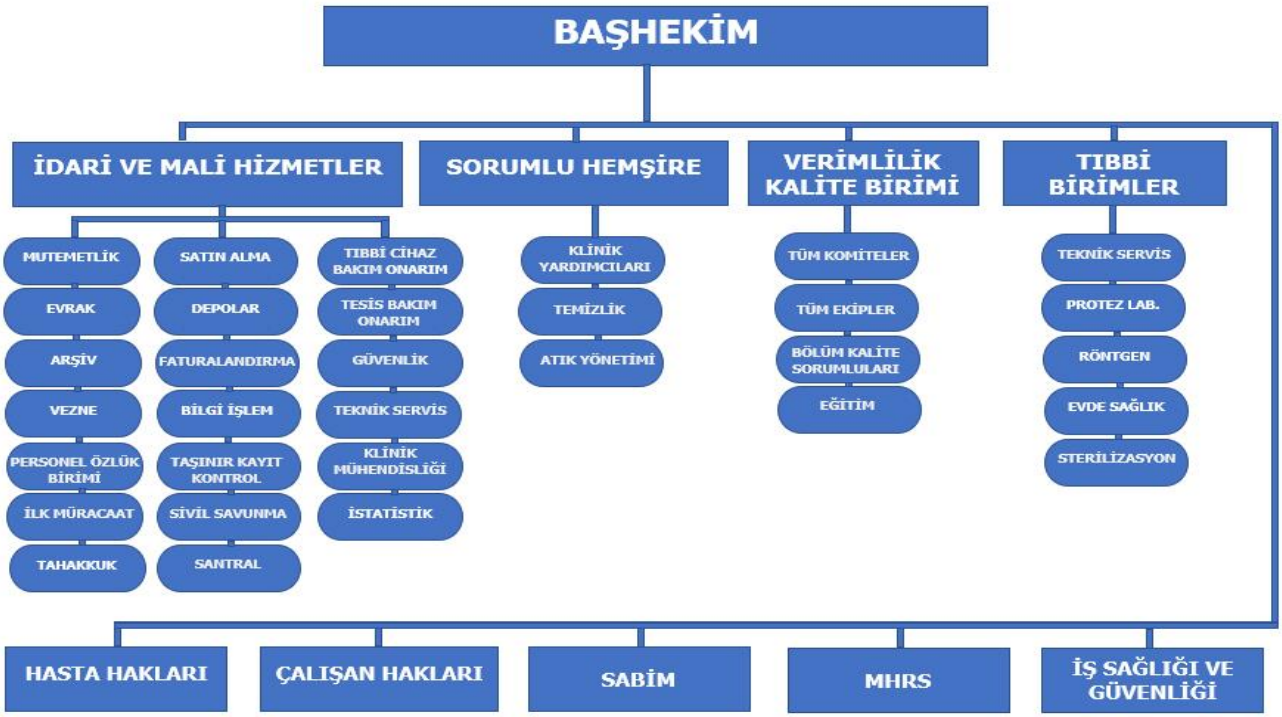
BİLGİ GÜVENLİĞİ:
Bilgi güvenliği; elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikasının belirlenmesi ve uygulanması gereklidir.

1.AMAÇ:
Yalova Ağız Ve Diş Sağlığı Merkezi görevleri kapsamında bilginin toplanması, değerlendirilmesi, raporlanması ve paylaşılması süreçlerinde güvenliğin sağlanmasına yönelik tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içerden veya dışarıdan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlamaktır. Ayrıca bilgi güvenliği farkındalık, duyarlılık ve teknik bilgi düzeylerinin artırılması ile sistemsel güvenlik açıklarının ortadan kaldırılmasını sağlayarak, insan kaynaklı zafiyetlerin önlenmesi ve gizliliği, bütünlüğü ve erişilebilirliği sağlanmış bilişim alt yapısının kullanılması ve sürdürebilirliğinin temin edilmesi sureti ile; veri ve bilgi kayıplarının önlenmesi, bu yolla ekonomik zarara uğranılmaması ve kurumsal prestij kaybı yaşanmamasıdır.

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

3. HEDEF:
Bilgi güvenliği temelde gizlilik, bütünlük, kullanılabilirlik unsurlarını hedefler. Gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesi, bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunması, kullanılabilirlik ise bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir.

4.ORGANİZASYON ŞEMASI:



5.TANIMLAR:

ÇKYS: Çekirdek Kaynak Yönetimi Sistemi

BYS: Bilgi yönetim sistemi

6.POLİTİKALAR

6.1-Bilgi Güvenliği:

6.1.1-Merkezimizde Bilgi Güvenliği Ekibi oluşturulmuş olup, görev -yetki ve sorumlulukları tanımlanmıştır. (KKU02.YD.36-Bilgi Güvenliği Ekibi Görev Yetki Ve Sorumlulukları)

6.1.2-Yıllık planlar çerçevesinde bilgi güvenliği teknik ve farkındalık eğitimleri gerçekleştirilmektedir.

6.2-Gizlilik Sözleşmeleri:

6.2.1-Merkezimizde çalışan ve herhangi bir modülde kullanıcı olarak tanımlanan tüm çalışanlar, personel gizlilik sözleşmesini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Merkezimizde göreve yeni başlayan bir personel özlük birimi tarafından kendisine verilen HBYS Kullanıcı Yetkilendirme ve Gizlilik Formu'nu doldurarak, Otomasyon Görevlisine yönlendirilir, otomasyon görevlisi tarafından BYS üzerinde aktifleştirilerek kendisine erişim yetkisi verilir.

Merkezimizden istifa, emeklilik ya da benzeri nedenlerle ayrılan bir personel, özlük birimi tarafından Otomasyon Görevlisine yönlendirilir, HBYS Kullanıcı Yetkilendirme ve Gizlilik Formu üzerinde ayrıldığı tarih ve saat belirtilir ve o andan itibaren BYS üzerinde

inaktifleştirilerek erişim yetkisi iptal edilir. Çalışanlara ait rol grupları ve yetkileri Kullanıcı Bilgi Yetkilendirme Envanteri Listesi'nde belirtilmiştir.

BİLGİ SINIFLANDIRMA KLAVUZU		Saklama Yeri Dolap
Gizli	En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır.	
İç Kullanım	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görememesi gereken bilgilerdir. Gizlilik ön plandadır.	Departmanın kilitli dolapları, kişisel bilgisayarlar
Kişisel	Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, laptop veya dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır.	Çalışma masalarının kilitli çekmeceleri.
Kuruma Açık	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın kilitli ortak dolapları
Halka Açık	Bu bilgiler T.C. Sağlık Bakanlığı' na bağlı tüm teşkilatına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Dolaplar ve dolap dışlarında

6.3-İnsan Kaynakları ve Zafiyetleri Yönetimi

6.3.1- Çalışan personele ait şahsi dosyalar ve gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.

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

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

6.3.4- İmha edilmesi gereken müsvedde halini almış ya da iptal edilmiş yazılar vb. imha edilmelidir.

6.3.5-Çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

6.3.6- Görevden ayrılan personel, zimmetinde bulunan malzemeleri ve elindeki bilgi, belgeleri teslim etmeli; personel kimlik kartı idareye yazıyla iade edilmelidir.

6.4-Parola Güvenliği

6.4.1- Parola en az 8 karakterden oluşmalıdır. Büyük ve küçük harfler bir arada kullanılmalı; harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler de içermelidir.

6.4.2- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar, sözlükte bulunabilen kelimeler veya kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi)

6.4.3- Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.

6.5-İhlal Bildirim ve Yönetimi:

6.5.1-Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar değişikliğe uğraması ve başkaları tarafından ele geçirilmesi gibi güvenlik ihlali durumları mutlaka kayıt altına alınmalıdır.

6.5.2-Bilgi güvenliği ihlâli oluşması durumunda; Bilgi Güvenliği İhlal Bildirim Formu doldurularak olay anında raporlanmalı, olay anında ihlali yapan kullanıcı tespit edilip ihlalin suç unsuru içerip içermediği belirlenmelidir.

6.5.3-Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurur.

6.5.4-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 etmelidirler.

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

Uyarma
Kınama
Para cezası
Sözleşme feshi,

6.6-İnternet ve Elektronik Posta Güvenliği

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

6.6.2-Kurumun e-posta sunucusu; kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz; herhangi bir kullanıcı ya da gruba küçük düşürücü, hakaret edici, zarar verici mesajlar göndermek için kullanılamaz.

6.6.3- 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.

6.6.4-Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz; e-posta gönderirken konu alanı boş bırakılamaz ve de konu alanı boş, kimliği belirsiz hiçbir e-posta açılıp ve silinemez.

6.6.5-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.

6.6.6-Kurum ile ilgili olan gizli bilgi, gönderilen mesajlarda ya da ekinde yer almamalıdır.
6.6.7-Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.
6.6.8-Kullanıcı; kurumun e-posta adresi üzerinden taciz, suiistimal veya alıcının haklarına zarar vermeye yönelik öğeleri içeren ve de e-posta ile uygun olmayan içerikleri (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemeli bu tür mesajlar aldığında Sistem Yönetimine haber vermelidir. 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.)
6.6.9-Kullanıcı hesapları; doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmayıp diğer kullanıcılara da bu amaçla e-posta gönderilmemelidir.
6.6.10-Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yönetimine haber verilmelidir. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmemelidir.
6.6.11-Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermeli; gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.
6.6.12-Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı; tehdit unsuru olduğu düşünülen ve kullanıcı kodu/parolasını girmesini isteyen e-postalar geldiğinde ise herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.
6.6.13-Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.
6.6.14-Kullanıcı, güvenlik zafiyetlerine sebep olmamak için bilgisayar başından ayrılırken mutlak ekranını kilitlemelidir.
6.6.15-Kullanıcı bilgisayarlarında güncel antivirüs bulunmalıdır.

6.7-Mal ve Hizmet Alımları Güvenliği

6.7.1- 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.
6.7.2- 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 metodu, 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 dâhil 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.

6.7.3-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.

6.7.4-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.

6.7.5-Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; sorumluluk, geçiş durumu planlama ve işlemler 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.

6.7.6- 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.

6.7.7- 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.

6.8-Sosyal Mühendislik Zafiyetleri:

İnsanların 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.

- ✓ Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.
- ✓ Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
- ✓ Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.
- ✓ Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgiler (Sistem yöneticiniz dahil) paylaşılmamalıdır. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
- ✓ Oluşturulan dosyaya erişecek kişiler ve hakları “bilmesi gereken” prensibine göre belirlenmelidir.
- ✓ Verilen haklar yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalı; belirli zamanlarda kontrol edilerek değişiklik gerekiyorsa yapılmalıdır.
- ✓ Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.
- ✓ Kazaa, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.

6.9-Sosyal Medya Güvenliği:

6.9.1-Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.

6.9.2-Kuruma ait hiçbir bilgi, yazı sosyal medyada paylaşılmamalıdır.

6.9.3-Kimlik bilgilerinin herkese açık görünür şekilde yer almasına izin verilmemelidir.

6.10-Uzaktan Erişim:

Sisteme erişim kontrolü ilgili başhekim ve bilgi işlem sorumlusu tarafından kişilerin yetki ve sorumlulukları dikkate alınarak düzenlenir. Bu şartlar uzaktan erişim içinde geçerlidir. Sistemde herhangi bir arıza durumunda HBYS firması tarafından uzaktan bakım için bağlantı şifresi verilir. Bu bağlantı ekstra programlar aracılığı ile yapılır. Ve her bağlantıdan sonra program kapatılır. Uzaktan erişimlerde otomasyon birim çalışanı tarafından Uzaktan Erişim Bildirim Formu doldurulur. Süreçlerde karşılaşılan sorunlar Bilgi Yönetim Sistemi Hata Bildirim Formu ile kayıt atına alınarak, gerektiğinde iyileştirme çalışmaları başlatılır.

Sisteme erişim ve yetkilendirme Sağlık Bakanlığı tarafından belirlenmiş olan esaslara göre düzenlenir.

Yazılım -donanım destek birimi 24 saat kesintisiz hizmet sunmakta olup, çalışanların güncel iletişim bilgileri bilgi-işlem ve otomasyon sorumlusunda bulunmaktadır.

6.11-Kablosuz Erişim :

Hastanemizde kullanılan otomasyon sistemine kablosuz erişim mümkün değildir.

6.12-Yedekleme:

- ✓ Veri yedekleme işlemi bilgi işlem işletimini yapan firma elemanlarınca yapılmaktadır.
- ✓ Hastane verileri her gün saat 06:00, 13:00 ve 18:00 olmak üzere günde üç defa yedek server üzerinde yedeklenmektedir.
- ✓ Hastane verileri her gün saat 06:00, 13:00 ve 18:00 olmak üzere günde üç defa Otomasyon firmasının serverlarında yedeklenmektedir.
- ✓ Hastane verileri haftada bir gün taşınabilir cihazda yedeklenerek hastane idaresine teslim edilmektedir.

6.13-Sunucu Odaları:

- ✓ Merkezimizde bulunan bütün sunucuların kayıtları tutulmakta olup, sadece sunuculara tahsis edilmiş bağımsız bir oda bulunmaktadır.
- ✓ Yetkisiz personelin girişini engellemek amaçlı kapıları kilitlidir. Ayrıca sunucu odasının bulunduğu koridorda güvenlik kamerası mevcuttur.
- ✓ Sıcaklık ve nem kontrolleri ısı-nem ölçer ile düzenli yapılmakta olup, normal sınırlardadır. (Sıcaklık: 18-22 nem oranı:30-60)
- ✓ Merkezimiz iklimlendirmesine ek olarak ayrıca bir klima bulunmaktadır.

- ✓ Acil durum kapsamında odada bir yangın tüpü bulunmakta olup, şu basmalarına karşı sunucular zeminden belirli bir yükseklikte tutulmaktadır.

6.14-Eğitim:

Merkezimizde kullanılan BYS'de kullanılabilirlik açısından gerekli düzenlemeler yapılmış olup, çalışanlar da etkin kullanımı ve uygulamalara ilişkin güncellemeler hakkında bilgilendirilmektedir Yedekleme işlemlerinden Başhekim ve Hastane Müdürü sorumludur.BYS'de farklı hizmet süreçlerine yönelik gerekli modüller bulunmakta ve aktif olarak kullanılmaktadır. Kullanılan modüller;

- ✓ Hasta kayıt
- ✓ Poliklinik
- ✓ Protez laboratuvarı
- ✓ Radyoloji
- ✓ Depo
- ✓ Satın alma
- ✓ Ayniyat
- ✓ Vezne
- ✓ Faturalandırma
- ✓ Personel
- ✓ İstatistik