1. **AMAÇ**: Hastanemiz bilgi güvenliği politikası (bilgi yönetim prosedürü); etkin ve yerleşmiş bilgi teknolojileri güvenlik süreçleri ve prosedürleri aracılığıyla sağlık

hizmetlerinden faydalanan vatandaşa ait bilgilerin ya da kurumsal hizmetlerin icra edilmesi esnasında edinilen bilgi ve kaynakların güvenliğini, bütünlüğünü ve erişebilirliğini

sağlamayı, ayrıca var olan bilginin kaybolmasını, zarara uğramasını, yok olmasını, yetkisiz ve kötü niyetli kişilerin eline geçmesini engellemek amacıyla oluşturulmuştur. Bu dokümanda, bilgi güvenliğine ilişkin korumalar ve gereksinimler belirlenmiş ve

denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtilmiştir.

1. **KAPSAM**: hastanemizin, bilgi kaynaklarını kullanmakta olan tüm birimleri, bilgi sistemlerine teknik destek

sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

# TANIMLAR:

* 1. **Bilgi Güvenliği: Bilgi**, diğer önemli ticari ve kurumsal varlıklar gibi, bir işletme ve kurum için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği; bilgiyi, yetkisiz kişilerin görmesinden, değiştirmesinden, bilgilerin silinmesinden korumaktadır. Bilgi güvenliği, bu politikada aşağıdakilerin korunması olarak tanımlanır:
		+ .**Erişilebilirlik:** Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek;
		+ . **Bütünlük**: Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek;
		+ .Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.
	2. **Varlık**: Kurum içi değeri olan her türlü unsur olarak tanımlanabilir. BGYS kapsamında Varlıklar:
* İş süreçleri; Kurumsal bilgi varlıklarının kullanıldığı, çeşitli vasıtalarla hassas

bilgilerin yoğun olarak işlendiği iş süreçleri (hasta kabul, heyet işlemleri, tıbbi kayıt arşiv vb.). V

* 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, laboratuar yazılımları, tıbbi görüntüleme yazılımları, kurumsal yazılımlar (EBYS, ÇKYS, KPS, HİTAP vb.) vb.
* Fiziksel varlıklar (Sunucular, masaüstü bilgisayarlar, taşınabilir bilgisayarlar,

taşınabilir ortamlar, 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 ara yüzleri olan tıbbi cihazlar vb.

* İnsan kaynakları: Çalışanlar
* Alt yapı: Yapısal ve elektrik kablolama altyapısı, UPS, jeneratör, iklimlendirme, giriş/çıkış kontrol sistemleri, kamera sistemleri, yangın, duman uyarı sistemleri, yangın söndürme sistemleri, destek teçhizatı vb
* Mekanlar: Yönetim ve hizmet odaları, sunucu odaları, arşiv odaları, tıbbi kayıt saklama odaları vb. dir.
	1. Taşınabilir ortam: CD/DVD, USB girişli hafif taşınabilir bellekler, taşınabilir diskler, hafıza kartları, teyp kartuşları vb.) ve basılı evraklar (yazılar, dosya klasörleri, etüdler, çizimler, krokiler, proje evrakları vb.)

3.4. Gizlilik: Bilgiye sadece erişme izni olan yetkili kişiler ya da sistemlerin erişmesini sağlamaktır.

* 1. Bütünlük: Bilginin yetkisiz kişi ya da işlemler tarafından değiştirilmemesini sağlamaktır. Böylece bilginin tutarlılığı sağlanmış olur.
	2. Erişilebilirlik: Bilgiye doğru zamanda erişimin ve erişim sürekliliğinin sağlanmasıdır.
	3. Bilgi Güvenliği İhlal Olayı: Bilgi Güvenliği Politikalarının ve prosedürlerinin dışında

işlem tesis edilmesi ile iş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen Bilgi Güvenliği olayıdır.

* 1. Bilgi Sistemleri: Donanım, yazılım, bilgisayar ağları ve insan unsurlarından oluşan, veri ve bilgileri toplayan, kaydeden, işleyen, dönüştüren ve yayan sistemler bütününü ifade eder.
1. KISALTMALAR:
	1. SBYS: Sağlık Bilgi Yönetim Sistemleri

 HBYS: Hastane bilgi yönetim sistemi

* 1. BG: Bilgi Güvenliği
	2. BGYS: Bilgi Güvenliği Yönetim Sistemi,
	3. VTYS: Veri Tabanı Yönetim Sistemi
	4. SBA: Sağlık Bilişim Ağı
	5. KVKK: Kişisel Verilerin Korunması Kurulu
1. **SORUMLULAR**: Hastane yönetimi, bilgi yönetim sistemi ekibi, tüm hastane çalışanları, bilgi sistemlerine

teknik destek sağlayan firma elemanları, HBYS ile entegre çalışan laboratuar, görüntüleme firması elemanları.

# FAALİYET AKIŞI: .

* 1. Bilgi Güvenliği Ekibi hastane yönetimi tarafından oluşturulur. Oluşturulan bu ekibin görevi BGYS

faaliyetlerini yürütmektir. BGYE'ne, BGYS'nin tüm süreçleri için gerekli yönetimsel destek ve kaynaklar sağlanır.

* + 1. Bilgi Güvenliği Ekibi, İdari ve Mali İşler Müdürü başkanlığında yılda en az 2 (iki) kez toplanır.
		2. BGYS Ekibi Görev, Yetki ve Sorumlulukları:
			- Kurum düzeyindeki Bilgi Güvenliği Politika ve stratejilerini belirler; kurum bünyesinde uygulanacak
			- BGYS'ye yönelik çalışmaları koordine eder
			- İl Sağlık Müdürlüğü tarafından yayımlanan eylem planında yer alan hususların gerçekleştirilmesini sağlar.
	1. **İnsan Kaynakları ve Son Kullanıcı Güvenliği**: Bilgi işleme tesislerine erişim izni verilecek tüm personel için (kamu personeli, tam zamanlı ya da yarı zamanlı olarak

çalışan sözleşmeli personel, yüklenici firma çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli vb.) işe alma öncesinde/alım yapılırken aşağıdaki hususların dikkate alınması gerekir. İşe alma öncesinde yapılacak güvenlik kontrollerinin amacı,

çalışanların kendilerinden beklenen sorumlulukları anlamalarını sağlamak ve düşünüldükleri roller için uygun olmalarını temin etmektir.

* + 1. İşe Başlayış:
			- İşe alınacak 657 sayılı kanuna tabi personellerin eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilmesi Bakanlığımızca yapılıyor olup, İl Sağlık Müdürlüğünce kurumumuza atanan personelin personel servisi tarafından kimlik kontrolleri yapılır.
			- İşe alınacak Yüklenici personeli, destek personeli vb. statüde çalışacak

personelin adli sicil kayıtları istenir ve ilgili komisyon tarafından incelenir.

* + - * İşe başlamadan önce tüm personel ve yükleniciler ile kişisel ve/veya kurumsal gizlilik sözleşmesi imzalanacağı ilgili taraflara bildirilir.

İmzalatılacak sözleşmelerin içeriği ve ilgililerin yükümlülükleri detaylı olarak açıklanır.

* + - * Kurumun güvenlik gereksinimleri dikkate alınmadığında, çalışanlar ve yükleniciler için yürütülecek işlemler (disiplin kurallarının uygulanması, gerekiyorsa iş akitlerinin sonlandırılması, tedarik sözleşmesinin feshi vb.) önceden belirlenir ve taraflara duyurulur.
			* Göreve başlayan personel, bilgi güvenliği sözleşmesini/bilgi güvenliği farkındalık bildirgesini okur, ilgili alanları eksiksiz olarak doldurur ve imzalar.
			* Göreve başlayan personele genel oryantasyon sorumlusu tarafından Bilgi

Güvenliği ve Sosyal Mühendislik zafiyetleri konularında eğitim verilir. Verilen eğitim, genel ve mesleki oryantasyon eğitim formuna kaydedilir.

* + - * Görev alanı belirlenen personel, görev alanı doğrultusunda HBYS kullanıcı talep formunu doldurur. HBYS kullanıcı şifresi bilgi işlem sorumlusu tarafından verilir ve sisteme kaydedilir.
			* Göreve başlayan personelin kimlik kartı personel servisi tarafından düzenlenir. Eğer personel EBYS kullanacak ise ©saglik.gov.tr uzantılı kurumsal posta adresi personel servisi tarafından temin edilir.
		1. Çalışma Esnasında Uyulacak Kurallar: Çalışma esnasında uygulanacak güvenlik kontrollerinin amacı, çalışanların işlerini yaparken bilgi güvenliği ile ilgili

sorumluluklarının farkında olmalarını ve beklenen şekilde yerine getirmelerini

sağlamaktır. Hastanemiz Yönetimi, bilgi güvenliği politikalarını, prosedürlerini ve kontrollerini desteklediğini her fırsatta örnek teşkil edecek şekilde gösterir. Bu

suretle, diğer çalışanların bilgi güvenliği ile ilgili motivasyonları üst düzeyde tutulur. Bilgi güvenliği ile ilgili beklentiler ve sorumluluklar, çalışanların görev tanımlarına eklenir.

* Bilgi güvenliği kontrolleri, İl Bilgi Güvenliği Komisyonu/Hastanemiz Bilgi Güvenliği Ekibi tarafından yapılır. Çalışanların kurumun bilgi güvenliği politikasına uyumu izlenir.
* Bilgi güvenliği farkındalık eğitimleri bilgi güvenliği ekibi tarafından hazırlanır. Belirlenen eğitim planına göre yapılır. Eğitim Kayıtları eğitim birimi tarafından muhafaza edilir.
* Çalışan personele ait şahsi dosyalar, gizlilik ihtiva eden yazılar, ilgili birimlerde kilitli dolaplarda muhafaza edilir.
* Bilgisayar ekranında kişisel bilgi içeren bir işlem yapıldığında (izin kâğıdı gibi) ekranda bulunan kişisel bilgilerin bilgi sahibi dışında diğer kişi veya kişilerce görülmesi engellenir.
* Diğer kişi, birim veya kurumlardan telefonla ya da sözlü olarak hastalar ve çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmez.
* İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) okunmayacak şekilde yırtılarak imha edilir.
* Tüm çalışanlar, çalıştıkları süre içerisinde kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmak zorundadır.
* BGYS politikalarına ve sır saklama yükümlülüğüne uymayanlar hakkında “657 sayılı Devlet Memurları Kanunu'nun veya iş sözleşmesinin ilgili hükümleri ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ilgili hükümleri” uyarınca işlem yapılır.
* Bilgi güvenliği ihlali yapan personele, uygulanan yaptırımlar (kişi kimlik bilgisi

verilmeden) diğer çalışanlara duyurulur ve onlar için de örnek teşkil etmesi sağlanır.

* + 1. Görev Değişikliği ve İşten Ayrılışta Yapılacak İşlemler: Görev değişikliği veya işten ayrılma ile ilgili güvenlik kontrollerinin amacı, ayrılma işlemleri esnasında yapılması

gereken bilgi güvenliği ile ilgili tedbirlerin ortaya konulması ve çalışanların görevleri sona erse dahi bilgi güvenliği ile ilgili devam eden sorumlulukları hakkında bilgilendirilmesidir.

* + - * İşten ayrılan veya Görev değişikliği yapılan personel üzerindeki görev ve evrakları birim sorumlusunun belirlediği personele devreder. Devir teslim işleminin tamamlandığına dair Görev Devir-Teslim Formunu doldurup birim sorumlusuna teslim eder. Görevi devralan personelin göreve dair oryantasyon eğitimi birim

sorumlusu tarafından yapılır. Yapılan eğitim genel ve mesleki oryantasyon eğitim formuna kaydedilir.

* + - * Kurumdan ayrılan personelin ayrılma işlemleri; ilgili tüm devir teslimler

yapılmadan ve ilişik kesme formu tüm ilgili sorumlular tarafından doldurulmadan yapılmaz. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi ile personel birimi müştereken sorumludur.

* + - * şten ayrılan veya görev yeri değişen personelin eski görevi ile ilgili bilgisayar

hesapları ve uzaktan erişim için kullandıkları hesaplar kapatılır veya erişim yetkileri yeni görev yerinin gereksinimlerine göre yeniden düzenlenir. Personele teslim

edilmiş tüm bilgi varlıkları (bilgisayarlar, yazılı ortamda saklanan bilgi ve belgeler, bilgisayar ortamında tutulan dosyalar, lisans belgeleri, CD'ler vb.) sayım yapılarak iade alınır.

* Ayrılan kişiden teslim alınan bilgisayarlar güvenli silme işlemi yapılmadan bir başka kullanıcıya teslim edilemez.
* Ayrılan veya görev yeri değişen personel tarafından yürütülen faaliyetlerin aksamaması için birim sorumlusu tarafından gerekli tedbirler alınır, gerekirse ayrılan personel ile yeni katılan personelin geçici bir süre birlikte görev yapması sağlanır.
* Görev değişikliklerinde, HBYS kullanıcı iptal formu doldurulur. Eski görevine ilişkin kullanıcı yetkileri bilgi işlem sorumlusu tarafından iptal edilir. Yeni göreve ilişkin yetkiler personel tarafından HBYS kullanıcı talep formu doldurularak talep edilir. 6.2.1. maddesine göre işlem yapılır.
* İşten ayrılan veya Görev değişikliği yapılan personel, görevi esnasında edinmiş olduğu bilgileri, görev yeri değişmesi veya ayrılması durumunda dahi sır olarak saklamaktan ve hiçbir şekilde yetkisiz olarak ifşa etmemekten sorumludur. Sır saklama yükümlülüğü süresizdir.

# İnternet Kullanım Kuralları:

* + 1. Hastanemizde görev yapan personel, İnternet hizmetini yalnızca iş faaliyetlerini destekleyecek şekilde

kullanmalıdır. Bunun dışındaki kişisel kullanımda aşağıdaki hususlar çerçevesinde;

* + - * Görev amaçlı kullanılabilecek kaynaklar az miktarda kullanılıyorsa,
			* Çalışanların verimliliğini engellemiyorsa,
			* Herhangi bir iş faaliyetini aksatmıyorsa,
			* Kullanıcıların bazı kişisel işlerini daha hızlı yerine getirmesini sağlıyorsa İzin verilebilir.
		1. Internet kullanımı, İl Sağlık Müdürlüğü tarafından yönetilen Güvenlik Duvarı

kullanılarak sınırlandırılmaktadır. Kullanıcılar, bu kontrollerin yapıldığını bilerek Internet'i kullanmalı, güvenlik amacıyla konulan önlemleri devre dışı bırakmaya çalışmamalıdır.

# E-Posta Kullanım Kuralları:

* + 1. Hastanemizde görev yapan personel tarafından görevleri gereği yürütülen kurumsal iş ve işlemlerde©saglik.gov.tr uzantılı kurumsal veya tüzel e-Posta hesabı kullanılır.

Kurumsal iş ve işlemler, kişilerin özel işleri için (Gmail, Hotmail gibi) internet hizmet sağlayıcılarından alınan hesaplar üzerinden yürütülmez.

* + 1. KVKK tarafından yayınlanan 2018/10 sayılı karar ile; 6698 sayılı kişisel verilerin korunması kanununda yer alan “özel nitelikli verilerin işlenmesi sırasında veri

sorumlularınca alınması gereken yeterli önlemler” belirlenmiştir. e-Posta ile aktarılacak verilerin özel nitelikli kişisel veri statüsünde olması durumunda aktarma işlemlerinin kurumsal e-Posta veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak yapılması kanuni zorunluluktur.

* + 1. Hastanemizde görev yapan 657 sayılı Kanuna bağlı tüm kamu personeli, talep etmeleri halinde https://eposta.saglik.gov.tr adresinden kurumsal e-Posta hesabı açabilir.
		2. Çeşitli sözleşmeler kapsamında hastanemizde görev yapan ve yaptıkları iş gereği e-

Posta hesabı olması gereken personele, sıralı yöneticileri tarafından onay verilmesi halinde resmi yazıyla Sağlık Bilgi Sistemleri Genel Müdürlüğü'nden kurumsal e-Posta hesabı talebi yapılabilir.

* + 1. Hastanemizde yer alan birimler için ihtiyaç olması halinde, tüzel e-Posta hesapları resmi yazıyla Sağlık Bilgi Sistemleri Genel Müdürlüğü'nden talep edilir. Tüzel e-Posta hesapları, Kurumun adı \* “.” # ilgili birimin adı veya yürüttüğü işlev ile alakalı olarak belirlenir. ( (torosdh.kalite©saglik.govitr, torosdh.personel ©saglik.gov.tr gibi).
		2. Kurumsal ve tüzel e-Posta kullanım kayıtları Bakanlıkça tutulur. Bu kayıtlar 6698

sayılı kanunun 28 inci maddesinin birinci ve ikinci fıkralarında yer alan şartlar kapsamında; yalnızca yetkili kişi, kurum ve kuruluşlar tarafından, yine aynı Kanun'un 4'üncü

maddesinde yer alan genel ilkelere uymak kaydıyla incelenebilir.

* + 1. Kurumsal ve tüzel hesapların kullanımında dikkat edilmesi gereken hususlar:
			- Kullanıcılar, kendilerine tahsis edilen e-Posta hesabını bir başka kişiye kullandıramaz veya devredemez. Kullanıcılar, parolalarını Kurum Parola Politikasında uyarınca oluşturur ve kullanır.
			- Kullanıcılar, kendilerine ait parolanın güvenliğinden ve söz konusu parola kullanılarak gönderilen e- Postalardan doğacak hukuki işlemlerden sorumludur.
			- Kurumsal e-Posta hesabı yalnızca kurumsal süreçlere ilişkin iş ve işlemlerde kullanılabilir. Kurumsal e-Posta hesaplarının, idari ve hukuki düzenlemelere aykırı ya da şahsi iş ve işlemlere ilişkin kullanımından kaynaklanan her türlü adli, idari, mali ve cezai sorumluluk ilgili hesap kullanıcısına aittir.
			- Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-Posta hesapları kullanılamaz. Aksine durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.
			- Konusu suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira

içeren, ahlaka aykırı mesajların içeriğinden ve sahip olduğu görev kapsamı içindeki iş ve işlemler dışındaki e-Posta hesabının kullanımından kullanıcı sorumludur.

* + - * Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-Posta gönderilemez.
			* Kurumsal e posta hesabından Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları

gönderilemez.

* + - * İnternet haber gruplarına üyelik için kurumun sağladığı e-Posta hesapları kullanılmaz. Ancak iş gereği üye olunması yararlı internet haber grupları için

yöneticisinin onayı alınarak kurumun sağladığı resmi e-Posta adresi kullanılabilir.

* + - * Kullanıcılar, e-Posta hesaplarında hukuki açıdan suç teşkil edecek materyal ve belgeleri bulunduramaz. Kullanıcılar, kendi kullanıcı hesaplarında barındırdıkları içeriklerden ve gerçekleştirilen tüm elektronik posta işlemlerinden sorumludur.
			* e-Posta gönderimlerinde, mesajın en alt kısmına gönderen kişinin kimlik ve iletişim bilgileri yazılır, konu alanı boş bir e-posta mesajı göndermez.
			* Konu alanı boş ve kimliği belirsiz veya kaynağı bilinmeyen e-Posta ve ekinde gelen hiçbir e-posta açılmamalı ve hemen silinmelidir. Spam, zincir, sahte vb. zararlı

olduğu düşünülen e-Postalara yanıt verilmez. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmez.

* + - * Tanınmayan elektronik postaların açılması, eklentilerinde bulunan dosya veya programların indirilip çalıştırılmasından kaynaklanabilecek güvenlik sorunlarının sorumluluğu kullanıcıya aittir.
			* Kurumsal e-posta adresi, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.
			* Kurumsal e-posta adresi ile; taciz, suiistimal veya herhangi bir şekilde alıcının

haklarına zarar vermeye yönelik öğeleri içeren mesajlar, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) gönderilmez.

* + - * Kullanıcılar, gelen veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemek için her türlü tedbiri alır, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.
			* 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.
			* Kurum 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.

* + - * Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e- postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.
	1. **Sosyal Mühendislik ve Sosyal Medya Güvenliği**: Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı

olarak tanımlanır. Başka bir tanım ise insanoğlunun zaaflarını kullanarak istenilen bilgiyi, veriyi elde etme sanatıdır. Sosyal mühendislik yapan kötü niyetli kişiler, sosyal medya ve analiz yöntemlerini kullanarak hedef kişiler hakkında bilgi toplarlar. Sonrasında sosyal mühendislik tekniklerini kullanarak insanların zaaflarından faydalanıp istedikleri bilgilere ulaşmak için çalışma yaparlar.

* + 1. Sosyal mühendislik saldırılarından korunmak için kişisel olarak dikkat edilmesi gereken hususlar:
			- Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunuz.
			- Bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket ediniz.
			- Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.
			- Parola kişiye özel bilgidir. Özellikle telefonda, e-Posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi; Sistem yöneticiniz de dâhil olmak üzere kesinlikle hiç kimseyle paylaşmayınız.
			- Oluşturulan dosyaya erişecek kişiler ve haklarını, “bilmesi gereken” prensibine göre belirleyiniz ve erişim kontrol tedbirleri uygulayınız. Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.
			- Çöpe atılan kâğıtlara dikkat ediniz. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtları, kâğıt kırpma makinesinden geçirerek ya da okunmayacak şekilde

yırtarak imha ediniz.

* + - * Çok acele bilgi istendiği zaman istenen bilginin niteliğine göre teyit mekanizması kullanınız.
			* Bilgisayarınızı yabancı bir kişiye kullandırmayınız. Bu kişiler tarafından

bilgisayarınıza takılacak olan USB depolama aygıtları ya da harici disklerden bilgisayarınıza zararlı yazılım bulaştırabilir.

* + - * Hediye olarak verilen USB depolama aygıtlarını kullanmadan önce mutlaka virüs taramasından geçiriniz.

# Kurum tarafından sosyal mühendislik alanında alınan önlemler:

* + - * Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınır.
			* Telefon ile hasta hakkında bilgi almak isteyen kişilere, hastanın kişisel bilgileri ile ilgili açıklama yapılmaz.
			* Hasta dosyaları ilgili doktor ve hemşire dışında kimseyle paylaşılmaz. Kolay ulaşılır yerlere konulmaz.
			* Hastaya ait bilgiler ve belgeler, hasta ve ve ya vasii/velisi dışında hiç kimse ile paylaşılmaz. Ortak alanlarda hastaya ve hastalığına ait konuşma yapılmaz.
			* SBYS/HBYS programlarında kullanılan parolalar kimseyle paylaşılmaz.
			* Eğitimlerde sosyal mühendislik zafiyetleri ve sosyal medya güvenliği ile ilgili hususlara yer verilir.

# Kişisel Sosyal Medya Güvenliği:

* + - * Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalar farklı seçilir.
			* Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.
			* Kuruma ait gizli bilgiler, resmi yazılar, çeşitli gelişmeler sosyal medya ortamında yayımlanamaz.

# Varlık Yönetimi:

* + 1. İş süreçleri ve kurumsal bilgi varlıklarının yönetimi:
			- İş süreçleri ve Kurum bilgi varlıkları, içerdikleri verilerin hassasiyeti, kurum için taşıdıkları önem ve yasal zorunluluklar dikkate alınarak uygun bir şekilde

sınıflandırılır/gizlilik derecesi verilir.

* + - * 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” dikkate alınır.
			* Gizli, özel ve hizmete özel evrakların gizlilik derecesi, yazıyı hazırlayan makam tarafından tayin edilir. Gizli ve özel evraklar kilitli çelik dolaplarda, hizmete özel evraklar ise masa gözlerinde kilitli olmak şartıyla muhafaza edilir.
			* Gizlilik derecelerinden hiçbirisi ile sınıflandırılmayan ve özel bir koruma

gerektirmeyen evrak ve dokümanlar, **“tasnif dışı”** olarak kabul edilir. Tasnif dışı belgeler için herhangi bir erişim kısıtlaması yoktur

* + - * Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, elektronik ortamda hazırlanması ve dağıtılması ile ilgili hususlar için Sağlık Bakanlığı Elektronik Belge Yönetim Sistemi Yönergesinde belirtilen kurallar uygulanır.
			* Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, kâğıt ortamda hazırlanması ve manuel (elektronik olmayan) yöntemlerle dağıtılması için Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelikte belirtilen kurallar uygulanır.
			* Gerekelektronik ortamda, gerekse basılı ortamda saklanan bilgilerin;
				+ Bilgiye erişimin kayıt ve kontrol altına alınması,
				+ İzinsiz kopyalamanın önlenmesi,
				+ E lektronik veya basılı olarak depolama süresi ve koşullarının tanımlanması,
				+ İletim hassasiyetinin belirlenmesi,
				+ Gerektiğinde kanıt olarak kullanılmak üzere bütünlüğünün sağlanması,
				+ İhtiyacın sonlanması durumunda imha edilmesi süreçlerinin tanımlanması

için uygun şekil ve yöntemlerle etiketlenmesi gerekir. Tasnif dışı bilgiler için etiketleme yapılmasına gerek yoktur

* + - * + İlgili mevzuat tarafından verilen yetkiye dayanılarak Bakanlığımıza bağlı

sağlık hizmet sunucuları tarafından işlenen kişisel sağlık verileri; verinin ait olduğu kişi, ne maksatla istendiği vb. özel durumlar da dikkate alınmak

suretiyle yukarıda tanımlanan gizlilik derecelerinden en az “ÖZEL” gizlilik derecesi ile etiketlenir.

# Taşınabilir Ortam Yönetimi:

**Personellerin Taşınabilir Ortamların kullanımında dikkat etmesi gerekenler:**

* + - * Kaybolma, kolayca çoğaltma vb. nedenlerden dolayı, özellikle elektronik medya (CD/DVD, USB girişli hafif taşınabilir bellekler, taşınabilir diskler, hafıza kartları, teyp kartuşları vb.) ve basılı evraklar (yazılar, dosya klasörleri, etüdler, çizimler,

krokiler, proje evrakları vb.) olmak üzere taşınabilir ortamlarda saklanan her türlü bilginin korunması ve yetkisiz kişilerin eline geçmemesi için özel önlemler alınmalıdır.

* + - * Taşınabilir cihazlardaki bilgileri üçüncü taraflarla paylaşımında da gerektiği kadar bilgi verme prensibi göz önünde bulundurulmalıdır.
			* Personelin kullanımı için tahsis edilmiş olan taşınabilir ortamlar sadeci yetkilendirilmiş personel tarafından ve veriliş amaçları doğrultusunda kullanılmalıdır.

# Elektronik medya kullanımı ile ilgili dikkat edilmesi gerekenler:

* + - * Kuruma ait veriler, kişilere ait medyalar üzerinde saklanamaz. Verilerin bir taşınabilir ortama aktarılması ihtiyacı kaçınılmaz ise bu maksatla kuruma ait medyalar kullanılır.
			* Kuruma ait medyalar varlık envanteri içinde listelenir ve kimler tarafından kullanıldığı kayıt altına alınır. Görev devir teslimlerinde veya işten ayrılışlarda, kişilere teslim edilmiş olan medyaların iade edilmesi istenir veya ne şekilde sarf edildiği bilgisi sorgulanır.
			* Özellikle eski SBYS/HBYS verileri ve SBYS/HBYS yedeklerinin saklandığı medya ortamlarının mutlak surette envanter listesi oluşturulur, 6 (altı) aydan az olmayacak

şekilde belirlenecek sürelerde sayım işlemleri yapılır ve sayım sonuçları kayıt altına alınır.

* + - * ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL veriler, taşınabilir ortamda saklanamaz. Özellikle bu tür ortamlarda saklama zorunluluğu var ise şifreli olarak saklanır.
			* Bir bilgi sadece taşınabilir medya ortamında saklanıyorsa, bozulma/kaybolma gibi ihtimallere karşı bir başka medya ortamında da yedeklenmelidir. Veriler çok

kıymetli ise yedeklenen medya ortamı, doğal afet vb. tehditlere karşı önlem olmak üzere fiziksel olarak farklı bir yerde muhafaza edilir.

* + - * Yeni medya teknolojilerinin ortaya çıkması nedeniyle üç yıldan uzun süredir eski teknolojilerin kullanıldığı bir medya ortamında saklanan verilerin daha yeni bir medya ortamına taşınması tavsiye edilir.
			* Gizlilik derecesi taşıyan kurumsal verilerin saklandığı medya ortamları, kişisel (şahsın kendisine ait) bilgisayarlarda kullanılamaz. Bu tip veriler kişisel

bilgisayarlarda işlenemez.

* + - * VTüm ortamlar üretici talimatında belirtildiği şekilde toz, nem vb. çevresel şartlardan etkilenmeyecek şekilde güvenli bir ortamda saklanır.
			* Elektronik medya da dâhil tüm taşınabilir ortamlar, kullanılmadığı zamanlarda

içinde bulunan verilerin gizlilik derecesi dikkate alınarak fiziki güvenlik tedbirleri alınmış kasa, dolap, çekmece gibi ortamlarda saklanmalıdır.

**Taşınabilir ortamların bir yerden başka yere taşınması:** taşınma esnasında yetkisiz erişim, kötüye

kullanım ve bozulmaya karşı gerekli önlemler alınmalıdır. Bu çerçevede;

* + - * Güvenilir kargo/taşıma şirketleri ya da kuryeler kullanılır,
			* V Yönetim tarafından yetkili kurye listeleri oluşturulur.
			* V Paketleme ve taşıma sırasında ortaya çıkabilecek herhangi bir fiziksel hasardan korumak için üreticinin belirlediği teknik özelliklere uygun önlemler (ısı, nem ya da elektromanyetik alanlara maruz kalma gibi çevresel faktörlere karşı koruma vb.) alınır.

# Bilgi Saklama Ortamları Yok Etme Kuralları:

* + 1. Basılı Ortamlar ve bilgi işlem cihazlarında saklanan bilgiler de dahil olmak üzere; her türlü ortamda saklanan bilgilerin silinmesi, anonim hale getirilmesi ve imha edilmesi ilgili

mevzuatlar doğrultusundahastanemiz tarafından belirlenen kurallar çerçevesinde gerçekleştirilir.

* + 1. Basılı ortamda tutulan bilgilerin yok edilmesi:
* Hastanemizin genel ve birim arşivlerinde bulunan dökümanlar, arşiv işleyiş prosedürü'ne göre muhafazaedilir. Arşivlerde bulunan dökümanların saklama süreleri Arşiv bekleme süreleri tablosunda belirtilmiştir.
* Genel arşivde bulunan ve Yasal bekleme süreleri sone eren dökümanların imhası; Devlet Arşiv HizmetleriYönetmeliği doğrultusunda oluşturulan Evrak İmha Komisyonu tarafından yapılır.
* Özel ve Çok Gizli evraklar kırpılarak imha edilir. Tasnif dışı evraklar geri dönüşümlü atık kapsamındadeğerlendirilerek imha edilir.
	+ 1. Elektronik ortamda bulunan bilgilerin yok edilmesi:
			- Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik veya fiziki nedenlerlekullanılmasında yarar görülmeyerek hizmet dışı bırakılmasına karar

verilen bilgi sistem cihazları ile ilgilikayıt silme işlemleri 2006/11545 sayılı Taşınır Mal Yönetmeliğinde belirtilen usul ve esaslar çerçevesince, ilgili birimler ve komisyonlar tarafında yapılır.

* + - * Kaydı silinen bilgi sistem cihazlarına ait veri depolama üniteleri, içerisinde gizlilik dereceli bilgibulundurma ihtimali nedeniyle usulüne uygun olarak imha edilir veya güvenli silme işlemi yapılır.
			* Kaydı silinen bilgisayarların sabit diskleri, ilgili teknik birimlerden destek alınmak suretiyle sökülür.
			* Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) imhası, Katı Atıkların Kontrolü Yönetmeliğine ve Basel Sözleşmesine göre yapılır.
			* İmha edilecek elektronik ortamların imha usulleri ve imhanın yapılacağı alanlar; materyalin özellik ve cinsine göre, imha Komisyonca belirlenir. İmha yöntemine göre Uygun koşulların sağlanmasından imha komisyonu sorumludur.
			* Yeniden kullanılmayacak olan elektronik ortamlar; parçalama, yakma, kimyasal maddeler ile eritme, delme kesme makinesi ile kullanılamaz hale getirme vb.

yöntemlerle imha edilir.

* + - * İmha işleminden önce elektronik ortamda bulunan veri ünitelerinin seri numaraları ve adet bilgileri alınarak data imha tutanağına kaydedilir.
			* İmha edilen parçaların fiziksel muayene ile tamamen tahrip edilip edilmediği kontrol edilir. Son ürünlerin gruplar halinde fotoğraflanarak data imha tutanağı ile birlikte

ilgili kişi ve/veya kuruma iletilir.

* + - * Çıkan maddeler sınıflarına göre ayrılarak, Endüstriyel Atık Yönetim Planı doğrultusunda bertaraf edilir.
			* Yeniden kullanılması planlanan disklere, içlerinde yer alan bilgilerin yetkisiz

kişilerin eline geçmesini engellemek maksadıyla “güvenli sil” (üzerine yazma) işlemi yapılır.

* + - * Güvenli silme işlemi, manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez O ve Vlerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu iş için uygun bir yazılım (DBAN, Kill Disk, Eraser, Disk Wipe, HDShredder gibi) veya donanım kullanılır.

# Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi:

* + - * İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan veriler bilgi işlem sorumlusu tarafından güvenli olarak silinir.
			* Güvenli silmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortam sökülerek bilgi işlem sorumlusu tarafından saklanır,
			* Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, hassas verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için bakım ve onarım işlemleri bilgi işlem teknik personeli gözetiminde yapılır.

# ERİŞİM KONTROLÜ

* + 1. Erişim Kontrol Politikası: hastanemizin bilgi ve bilgi işleme sistemlerine yapılacak olan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin oluşturulmasıdır.
			- Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı gizlilik

dereceli) bilgiler için özel bir erişim kontrol tedbiri alınmasına gerek yoktur. Bu tür bilgiler, hastanemizin İnternet sitesinin vatandaşlara açık bölümlerinde, duyuru panosu vb. ortamlarda yayınlanabilir.

* + - * Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir
			* Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.
				+ “Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin

gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak, bir kişinin kendi başına tüm bilgi

varlıklarına erişimi engellenir. Teknik nedenlerle görev ayrımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır.

* + - * + “Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve

kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.

* + - * Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik

sistemler için farklı kimlik doğrulama yöntemleri (akıllı kart, tek kullanımlık parola, elektronik imza, mobil imza vb.) kullanılabilir.

* + - * Bilgi varlıklarına yapılan erişimler için iz kayıtları bilgi işlem sorumlusu tarafından oluşturulur.
			* Sağlık Bilişim Ağı dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.
			* Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. Veri tabanı yönetim sistemi sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.
			* Bilgi varlıklarına fiziksel olarak yapılacak erişimler için gerekli önlemler bilgi işlem sorumlusu tarafından alınır.
			* Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için KVKK'nun 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir.
			* Bakanlığımız ortak uygulamalarına erişim, SBSGM Bilgi Güvenliği Politikaları Kılavuzuna uygun şekilde yapılır
		1. **Kullanıcı Erişimlerinin Yönetimi:** sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek, sadece yetkili kullanıcıların erişimlerini temin etmek için yapılır.
			- Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir.

Bilmesi gereken prensibi uyarınca, gereksiz olarak verilmiş yetkilerin kaldırılması

sağlanır. İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en fazla altı aylık aralıklarla yapılır.

* + - * Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında bilgi işlem sorumlusu tarafından gözden geçirilir.
			* Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili incelemeler, üç ayı aşmayacak şekilde daha sık yapılır.
			* 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır. Ayrıcalıklı erişim hakkı verilen kullanıcı sayısı (etki alanı

yöneticisi, veri tabanı yöneticisi vb.) asgari düzeyde tutulur.

**6.8.3. Uzaktan Erişim Kuralları:** Kurumumuz bünyesindeki bilgi kaynaklarına (sunucu ve hizmetlere) uzaktan erişim için alınması gereken tedbirler ve uyulması gereken kurallardır.

* Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahiptir.
* İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar SSL VPN teknolojisini kullanmalıdırlar. SSL VPN Kullanıcısı İl Sağlık Müdürlüğü Bilgi İşlem Biriminden talep edilecektir.
* SSL VPN bağlantılarına ilişkin kayıtlar İl Sağlık Müdürlüğü loglama sisteminde loglanmaktadır.
* SSL VPN Kullanıcı şifresi Kurum Parola Politikası ile uyumludur.
* SSL VPN Kullanıcısı bağlantı bilgilerini hiç kimse ile paylaşmaz.
* SSL VPN bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) 10 dakika olarak belirlenmiş olup herhangi bir işlem yapılmadığı takdirde ilgili oturum kapanır.

 **Uzak bağlantı, masaüstü erişim amaçlı olarak yapılıyorsa;**

* Bağlantı SSL VPN üzerinden yapılır.
* Bağlantı yapan kişinin, hedef bilgisayarda oturum açma iznine sahip bir kullanıcı olması gerekir. V
* Hedef bilgisayara kullanıcı adı ve parola girilerek oturum açılır. Anonim girişlere izin verilmez.
* Hedef bilgisayarda uzak bağlantı için kullanılan servis/arayüz vasıtasıyla, bilgisayara erişecek kullanıcılar “kullanıcı adı ve/veya IP adresi” bazında sınırlandırılır. Bu

yöntemle sadece yetki verilen kullanıcıların/bilgisayarların uzaktan erişim yapması sağlanır.

* Bağlantı yapan kullanıcının hedef bilgisayardaki oturum açma, oturum kapatma gibi kullanıcı hareketleri kayıt altına alınır ve söz konusu iz kayıtları en az 1 (bir) yıl süre ile saklanır.
* Hedef bilgisayar üzerinden bir başka sunucuya bağlantı yapılacak ise (örneğin SBYS yazılımı kullanılacak ise) ilgili kullanıcının söz konusu sunucuda yaptığı işlemlere ait iz kayıtları da kayıt altına alınır.
* Uzak bağlantı yazılımı olarak mümkün ise “Microsoft Uzak Bağlantı Programı” kullanılır.
* Microsoft işletim sistemi dışında bir başka bilgisayara erişim yapılıyorsa aynı güvenlik özelliklerini sağlayan, lisanslı ve/veya açık kaynak kodlu, güvenilir bir erişim programının kullanılması tercih edilir.
	+ Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların bilgileri hastanemiz Bilgi İşlem birimine HBYS kullanıcı talep formu ile mümkün olan en kısa zamanda bildirilir ve Yetkili personelce ilgili kullanıcının yetki ve hesap özellikleri buna göre güncellenir.
	+ Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantıyı herkese açık güvenli olmayan alanlarda (kafeler, lokantalar, oteller vb.) yapmaz.
* Uzaktan erişim yaparken sahibi bilinmeyen/herkes tarafından erişilebilen cihazlar (internet kafe, otel bilgisayarları, kiosklar vb.) kullanılamaz
* Uzak çalışma için kullanılacak cihaz ve ortamlarda asgari olarak aşağıda belirtilen güvenlik tedbirlerinin alınmış olması gerekir:
* Cihazlara kişisel güvenlik duvarı kurulur ve aktif halde olmalıdır.
* İşletim sistemi ve diğer uygulamalar için yayımlanan güvenlik yamalarının otomatik güncelleme seçilerek güncel halde tutulması sağlanmalıdır.
* Virüs, fidye yazılımları, truva atları ve benzeri zararlı yazılımlardan korunmak için uygun bir koruma yazılımı olmalıdır. Yazılımın kendisi ve imza dosyaları güncel halde tutulur.Cihaz üzerinde uzaktan çalışma için kullanılmak üzere asgari yetkilere sahip ayrı bir kullanıcı hesabı açılır. Yönetici yetkisi ile uzaktan çalışma yapılmaz.
* Cihaza ekran koruma süresi konularak belli bir süre kullanılmadığında ekranın otomatik olarak kilitlenmesi sağlanır.
* Cihazlar fiziki güvenliği olmayan ortamlarda kullanılacak ise dizüstü bilgisayar kilidi kullanılmak suretiyle çalınmaya karşı cihaz emniyete alınır.
* Cihazın üzerinde yer alan ve kullanılmayan ağ özellikleri (WİFİ, bluetooth, RS232 vb.) pasif hale getirilir.
* Disk şifreleme vb. araçlarla bilgisayarlarda tutulan verilerin şifreli olarak saklanması sağlanır. Disk şifreleme işlemleri için https://bilgiguvenligi.saglik.gov.tr/ adresinde yayımlanan sürücü şifreleme el kitaplarından yararlanılır
* Uzaktan çalışma için kullanılan bilgisayarların yerel disklerinde yer alan kurumsal

verilerin yedeklenmesi için gerekli tedbirler alınır. Alınacak bu yedekler sadece şifreli ortamlarda ve/veya şifreli yedeklenmiş olarak tutulabilir.

* Uzaktan çalışma ve uzaktan erişim için kullanılacak cihazlara çok faktörlü kimlik doğrulama yapılarak giriş yapılması tercih edilir.
* Hassas işlemlerde kullanılan üçüncü taraf bilgisayarlarındaki kurumsal verilerin kalıcı olarak silinmesi için gerekli teknik ve idari tedbirler alınır.
* Mobil cihazlara yüklenecek uygulamalar, ilgili işletim sistemi üreticisi tarafından sağlanan uygulama mağazalarından (AppStore, PlayStore vb.) indirilir.
* Kullanılan uygulamaların varsa güvenlik ayarları yapılarak daha güvenli kullanım ortamı sağlanır.
* Mobil cihaz işletim sistemi tarafından dayatılan kısıtlamalardan kurtulmak için

“jailbreak” veya “rootlama” işlemi yapılmaz. Bu işlemlerin yapıldığı cihazlar, uzaktan çalışma için kullanılmaz.

* Tüm mobil cihazlara (telefon/tablet) mutlaka lisanslı anti-virüs yazılımı kurulması gerekir.
* Kullanılan her türlü mobil cihaz için üreticinin sağladığı işletim sistemi

güncelleştirmeleri ve yazılım güncelleştirmeleri mutlaka periyodik olarak kontrol edilir ve uygulanır.

* 1. **Kurum Parola Politikası**: Kurumumuzda kullanılan sistem ve uygulamaların, kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmak zorundadır.
* Parolalar en az 8 (sekiz) karakterden oluşur. Sistem yönetim işlemlerinde kullanılan parolaların (root, administrator, sysadmin vb.) en az 12 karakterden oluşması tavsiye edilir.
* İçerisinde en az 1 (bir) tane büyük ve en az 1(bir) tane küçük harf bulunur.
* İçerisinde en az 1 (bir) tane rakam bulunur.
* İçerisinde en az 1 (bir) tane özel karakter bulunur. (©, !,?,A,*,$,#,&,/,1,*,-,1.2,...)
* Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab...)
* Sıralı karakterlerin kullanılması engellenir. (abcd, gwert, asdf,1234,zxcvb...)
* Kişisel bilgiler veya klavye kombinasyonları ile basitçe üretilebilecek karakter dizilerinin kullanılması engellenir. (Örneğin 12345678, gwerty, doğum tarihi, çocuğun adı, soyadı gibi)
* Sözlükte bulunabilen kelimelerin kullanılması engellenir.
* Kullanıcının son 3 (üç) parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir. Sistem ve uygulamalarda oturum kontrolü yapılarak bir kullanıcı adı ve parolasının aynı anda birden çok bilgisayarda kullanılması engellenir.
* VTYS, aktif dizin sunucusu, uygulama sunucusu, ağ cihazları gibi sistem hesaplarına ait parolalar (root, administrator, sysadmin vb.) en geç 3 (üç) ayda bir değiştirilir.
* Kullanıcı hesaplarına ait parolalar (örnek: SBYS, e-Posta, web, masaüstü bilgisayar vb.) en geç 6 (altı) ayda bir değiştirilmesi sağlanır.
* Sistem yöneticileri ayrıcalıklı işlemleri normal kullanıcı adı ve parola ile yapmaz. Bu maksatla farklı kullanıcı adı ve parola kullanılır.
* Parolalar, e-Posta iletilerine veya herhangi bir elektronik forma eklenmez.
* Parolalar gizli bilgi olarak muhafaza edilir. Kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.
* Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu bölümde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.
* İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola

hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.

# İŞLETİM GÜVENLİĞİ

* + 1. **Kurum Yedekleme Politikası**: Bilgi sistemlerinde oluşabilecek hatalar karşısında

sistemlerin kesinti sürelerine ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler

üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesinin sağlanmasıdır

Bilgi sistemlerinde oluşabilecek hatalar karşısında, sistemlerin kesinti sürelerine ve olası bilgi kayıplarını en az düzeye indirmek için sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekmektedir.

# Verilerin yedeklenmesi:

* + - * Verinin yedekleri, operasyonel ortamda online olarak aynı disk sisteminde farklı disk bölümlerinde ve offline olarak Backup Server, Harici Disk, Nas Cihazları, DVD veya CD ortamına bilgi işlem sorumlusu tarafından alınır.
			* Yedekleme ortamları, hastane yönetimi tarafından, (Backup Server, Harici Disk, Nas Cihazları, DVD veya CD vb. ) fiziksel olarak bilgi işlem odalarından farklı odalarda

veya binalarda güvenli bir şekilde saklanır, veriler offline ortamlarda sınırsız süreyle saklanır. Saklama ortamlarında verilerin bozulmasını, çalınmasını engelleyecek tedbirler hastane yönetimi tarafından alınır

* + - * Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintilerin kritik olduğu sistemlerin bir varlık envanteri çıkartılır ve yedekleme ihtiyacı bakımından

sınıflandırılarak kayıt altına alınır.

* + - * Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya, bilgi sistemlerinde değişiklik yapma yetkili personel ve yetki seviyeleri kayıt altına alınmalıdır.
			* Hastanemiz gereklilikleri doğrultusunda bir Yedekleme Planı hazırlanmıştır.

Hastanemiz SBYS yedekleri bu plana göre düzenli aralıklarla alınmakta ve sürekli olarak gözden geçirilmektedir. Yapılan yedeklemeler Yedekleme Kontrol Listesi ile kayıt altına alınır.

* + - * Yedekleme ve yapılan yedeklemenin kontrolü, bilgi yönetim ekibi denetiminde hastane bilgi işlem sorumlusu ve bilgi işlem birimi tarafından yapılır.
			* Yedeklerin alınacağı sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak konu ile ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
			* Yedek ünite, gereksiz yer tutmamak üzere kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyalar yedekleme listesine dâhil edilmez.
			* Yeni sistem ve uygulamalar devreye alındığında ve Yedeklenecek bilgiler değişik gösterebileceğinden yedekleme listesi bilgi yönetim ekibi tarafından periyodik olarak gözden geçirilir ve güncellenir. Yedekleme ortamlarının düzenli periyotlarda

test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması için geri yükleme prosedürü (veri kurtarma testi) uygulanır.

# Geri Dönüş Testleri:

* + - * Yedeklenen verilerin orijinal verileri yansıtması ve başarılı bir şekilde yedeklenip yedeklenmediğinden emin olunması için belirli aralıklarla geri dönüş testlerinin yapılması gerekir.
			* Bilgi işlem sorumlusu tarafından, Yılda en az 2 (iki) kez geri dönüş testi yapılarak tutanakla kayıt altına alınır. Tutanakta; sunucu adı, test tarihi, önceki test tarihi, yedek türü ve yedek durumu, geri yükleme testlerinin kimler tarafından ne zaman yapıldığı, başarılı olup olmadığı gibi asgari bilgiler yer almalıdır.
			* Yedekten geri yükleme testlerinin, başarısız olması, bu nedenle veri kaybı olması olasılığı göz önüne alınarak, canlı ortamda değil gerçek ortamın aynısı olan test ortamında yapılması gerekmektedir.

# Antivirüs Yönetimi:

* + 1. Hastanemiz net work ağına bağlı olarak çalışan tüm bilgisayarlara lisanslı antivirüs yazılımı yüklenmiştir. Eğer kullanıcının bilgisayarında antivirüs yazılımı yok ise bunu bilgi işlem birimine bildirmekle yükümlüdür.
		2. Antivirüs yazılımının virüs veritabanı güncel tutulur. Kullanıcı, antivirüs yazılımının güncelleme yapmadığını fark ederse derhal bilgi işlem birimine bildirir.
		3. Anti virüs programının güncellemesi bilgi işlem birimi tarafından sunucu üzerinden yapılır. Güncelleme sırasında kapalı olan bilgisayarlar sunucu üzerinde listelenir ve açıldığı anda güncelleme gönderilip doğrulanır.
		4. Yapılan periyodik güncellemeler ile, virüs taraması, zayıf noktalar (farklı programların açıkları) antivirüs yazılımının sürümü, durum bilgisi ve birçok yararlı bilgi sunucu üzerinden raporlanır. Antivirüs sunucusunu yöneten personel ağda

yönetilen tüm bilgisayarların antivirüs yazılımının ne durumda olduğunu görür ve ona göre müdahalelerde bulunur

* + 1. Kullanıcı, bilgisayarındaki antivirüs yazılımını kapatmamalı yada devre dışı bırakmamalıdır.
		2. Kullanıcı, bilgisayarına taktığı CD/DVD, USB, Taşınabilir Disk vb. ortamları mutlaka güncel antivirüs yazılımıyla taratmalı ve tarama tamamladıktan sonra kullanmalıdır.
		3. Kullanıcıların, bilgi sistemler ine zarar verebilecek herhangi bir bilgisayar kodunun kasıtlı olarak yazmaları, çoğaltmaları, kopyalamaları, üretmeleri ve çalıştırmaları yada tanıtmaları yasaktır.
		4. Antivirüs yazılımları bazı otomasyonların (HBYS, PACS, tıbbi cihaz yazılımları vs) yoğun ağ trafiğini saldırı olarak görüp engelleyebilir. Bu durumda antivirüs

yazılımına sunucu üzerinden ilgili yazılımın güvenli olduğunu gösteren “güvenilir uygulama” tanımlaması yapılır.

* + 1. Antivirüs yazılımları her zaman güncel tutulmalı ve sunucuyla haberleşebilir durumda olmalıdır.
		2. Yüklü olan antivirüs programının kullanıcı tarafından devre dışı bırakılması veya sistemden kaldırılmasını engellemek amacıyla parola koruması uygulanır.

# BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

* + 1. Kurumumuz çalışanları ve vatandaşlar tarafından tespit edilen Sağlık Bakanlığı uygulamaları ile ilgili her türlü bilgi güvenliği ihlal olayı https://bilgiguvenligi.saglik.gov.tr/adresinde yer alan merkezi ihlal bildirim sistemine girilir.
		2. Olay bildirim sistemini kullanamayacak durumda olanlar kendi kurumlarındaki bilgi güvenliği yetkililerine bildirim yapabilir. Bilgi güvenliği yetkilisine yapılan

bildirimler, bilgi güvenliği yetkilisince merkezi ihlal bildirim sistemine girilir.

* + 1. Merkezi ihlal bildirim sistemine girilen olaylar; SBSGM Bilgi Güvenliği Politikaları Kılavuzunda belirtildiği şekilde Sağlık Bilgi Sistemleri Genel Müdürlüğünce işlem tesis edilir.
		2. Küçük çaplı, yalnızca kurumu ilgilendiren ve kurum Bilgi Güvenliği Yetkilisi kendi imkânları ile yerel olarak çözülebilecek olaylarda bilgi güvenliği olay bildirim ve

müdahale formu doldurulur. Bu tür olaylarda kurum Bilgi Güvenliği Yetkilisince veya bilgi işlem personeli tarafından gerekli müdahaleyapılır. Müdahale sonrası formun ”nci Bölümünü (Olay Müdahale) doldurulur ve İl Bilgi Güvenliği Yetkilisine bilgi verilir.

* + 1. Hizmet verdiği kurumla birlikte diğer kurum ya da kişileri etkileyecek şekilde iş sürekliliğine zarar veren veya durduran, acil müdahale gereken, kurum imajına

zarar verebilecek ihlal olaylarında “bilgi güvenliği olay müdahale ekibi” kurulur. İlgili ekip, gerekli müdahaleyi yapar. Destek istediği durumlarda sırasıyla İl Sağlık Müdürlüğümüz SOME ekibinden, Sektörel SOME'den görüş/destek alır. Olayın

çözümünde Ek -4 OLAY BİLDİRİM VE MÜDAHALE FORMU'nun2?'nci Bölümünü (Olay Müdahale) doldurarak bilgiguvenligi ©saglik.gov.tr adresine gönderir.

# TEDARİKÇİ İLİŞKİLERİ

* + 1. **Mal ve Hizmet Alımları Güvenliği:**
			- Satın alma faaliyetleri; 4734 sayılı Kamu İhale Kanunu, 4735 sayılı Sözleşmeler Kanunu, 5018 sayılı KamuMali Yönetimi ve Kontrol Kanunu, Kamu İhale Kurumu Tebliğleri ve yönetmeliklerinin tanımlamış olduğuusul ve esaslara göre yapılır.
			- Satın alma faaliyetine konu olan iş kapsamında; yüklenicinin yükümlülüklerini

gerçekleştirmesi içinyükleniciye özel koruma ihtiyacı olan veri/bilgi teslim edilmesi, ilgili kurumun fiziki alanlarında personelçalıştırılması veya kurum bilgi sistemlerine (uzaktan erişimler dâhil) erişim yapılması ihtiyacı olması halinde; satın alma için

hazırlanan teknik ya da idari şartnamelere “Bilgi Güvenliği Gereksinimleri” başlığı altında asgari olarak aşağıdaki hususlar eklenir:

* + - * + Yüklenici sözleşmeye konu yükümlülüklerini ifa ederken, Bakanlık Bilgi Güvenliği politikalarına uymak zorundadır. Bakanlığın Bilgi Güvenliği

Politikaları, “Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi” ve “Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu”nda açıklanmıştır. Bahse konu dokümanlara, Bakanlığın resmi web sitesinden erişilebilir.

* + - * Bakanlık/Kurum BGYS Politikaları uyarınca, idareye ait bilgilerin korunması maksadıyla, yükleniciler ile“Kurumsal Gizlilik Sözleşmesi” ve söz konusu iş kapsamında çalışacak olan yüklenici personeli ile “PersonelGizlilik Sözleşmesi” imzalanır. Bahse konu dokümanların boş halleri, hazırlanan teknik veya idari

şartnameye eklenir.

* + - * İhaleyi kazanan firma ile sözleşmenin imzalanmasını takiben kurumdaki yetkili makam (Satın Alma Birimivb.) huzurunda “Kurumsal Gizlilik Sözleşmesi” imzalanır.
			* “Kurumsal Gizlilik Sözleşmesi” ve ihaleye konu iş kapsamında çalıştırılacak personelin “PersonelGizlilik Sözleşmeleri” imzalanmadan ve idareye teslim edilmeden, yüklenici tarafından işe başlanamaz.
			* Yüklenici çalışanlarının bilgi ve bilgi işleme tesislerine erişim yetkileri, “Personel Gizlilik Sözleşmeleri”idareye teslim edildikten sonra tanımlanır.
			* Yapılacak iş kapsamında alt yüklenici kullanılacaksa, alt yükleniciler de yukarıda belirtilen hükümlere aynen uymak zorundadır. Yüklenici, alt yüklenicileri ve

çalışanlarının gizlilik sözleşmeleri ile ilgili yükümlüklere uymasından birinci derecede sorumludur.

* + - * Yukarıda belirtilen gereksinimlere ek olarak, aşağıdaki konular teknik/idari

şartnamelere veya tedarikçiler ile imzalanacak gizlilik sözleşmelerine eklenerek, garanti altına alınır:

* + - * + Alınan hizmetle ilgili olarak güvenlik kontrol gereksinimleri, hizmet seviyeleri ve yönetim gereksinimleri,
				+ Yükleniciye verilecek veya erişilecek bilgilerin tanımları ile bu bilgilerin sağlanma veya erişim metodları,
				+ Yüklenici ile paylaşılacak olan bilgilerin kabul edilebilir kullanım kuralları ve gerekiyorsa kabul edilemez kullanım durumları,
				+ Yüklenici personeli için erişim yetkilendirme ve yetki kaldırma prosedürleri,
				+ Bilgi güvenliği olay müdahale prosedürleri (özellikle olay bildirimi ve olay müdahalesinde işbirliği kuralları).
			* “Kurumsal Gizlilik Sözleşmesi” ve “Personel Gizlilik Sözleşmesi” olarak Ek'te yer alan sözleşmeler kullanılabilir. Bahse konu sözleşmelerin içeriği, satın almaya konu mal veya hizmetin türüne ve kurumun kendine özgü ihtiyaçlarına bağlı olarak revize

edilip kullanılabilir.

* + - * Yüklenicinin fikri mülkiyet hakları ve telif hakları dâhil, yasal ve düzenleyici gereksinimlere uyması ile ilgili hususlar satın alma dokümanlarına konulur.
			* Alınacak mal veya hizmetin tahmini bedelleri bağlamında idare tarafından yapılan yaklaşık maliyet çalışması, ihale aşamasına kadar gizli tutulur.
			* Söz konusu alım için gerekli iş tanımı ölçütleri, personel istihdam edilecekse ilgili personel özellikleri açıkçabelirtilir.
			* Tedarikçinin çalıştırılacağı personelin adli sicil kayıtlarını sorgulatıp, bunları idareye bildirmesi istenir.Projelerde çalışacak personelin; TCK'nın 53'ncü maddesinde belirtilen süreler geçmiş olsa bile devletin güvenliğine karşı suçlar, anayasal düzene ve bu düzenin işleyişine karşı suçlar, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin

ifasına fesat karıştırma, suçtan kaynaklanan mal varlığı değerlerini aklama ve kaçakçılık suçlarından mahküm olmamış olması gerekir.

* + - * Satın alma faaliyetine konu iş uygulamay/yazılım geliştirme ise; uygulama ile ilgili gerekli dokümantasyonun hazırlanması, ilgili projeye ait kaynak kodların teslim edilmesi gibi hususlar, idare tarafından açıkça tanımlanır. Ayrıca geliştirilen

yazılım/uygulamada Özel nitelikli kişisel veriler işlenecek ise KVKK'nın 2018/10

sayılı kararında belirtilen ilave güvenlik tedbirleri ile ilgili hususlar da teknik şartnamelere eklenir.

* + - * Anlaşmalar gereği, tedarikçilerce üretilen hizmet raporları düzenli olarak gözden geçirilir ve proje ilerleme toplantıları yapılır.
			* Tedarikçilere verilen fiziksel ve mantıksal erişimler, Kurum Bilgi Güvenliği Alt komisyonlarında gözden geçirilir. Hassasiyet arz eden erişimler için yönetim onayı alınır. Olası güvenlik zafiyetlerinin engellenmesi için yüklenici personeline verilen yetkiler periyodik olarak kontrol edilir. İhtiyacın bitmesi durumunda,verilen yetkiler kaldırılır. Personelin kurumla ilişiği kesilir kesilmez, erişim yetkileri de kapatılır.
			* Yazılım tedarikçilerinin destek faaliyetleri (ör: tedarikçi personelinin sistem

üzerinde çalıştırdığı komutların iz kayıtlarının tutulması ve incelenmesi gibi) izlenir.

* + - * Ürünlerin satın alınmadan önce kurumsal olarak belirlenen güvenlik gereksinimleri için risk oluşturmadığından emin olunması için test edilmesi gerekir.
			* SBYS Firmaları ile İlişkilerde Dikkat Edilecek Hususlar
				+ Sağlık tesisleri tarafından klinik, idari ya da yönetimsel amaçlarla kullanılan, gerektiğinde diğer bilgi yönetim sistemleri ile veri alış verişi yapabilen yazılım, sistem ya da alt sistemler Sağlık Bilgi Yönetim Sistemi (SBYS) olarak adlandırılır.
				+ Hastane Bilgi Yönetim Sistemi (HBYS), Aile Hekimliği Bilgi Sistemi

(AHBS), Laboratuvar Bilgi Yönetim Sistemi (LBYS), Görüntü Saklama ve Arşivleme Sistemleri/Radyoloji Bilgi Sistemi (PACS/RIS) vb. yazılımların tamamı SBYS yazılımıdır.

* + - * Kurumumuzda kullanılacak tüm SBYS yazılımlarının Bakanlık tarafından yayımlanan sağlık ( bilişimi standartlarına ve veri gönderim servislerine uyumlu olmaları

gerekmektedir. SBYS üreticisi firmalar,Bakanlık ve İl Sağlık Müdürlüğümüz ve kurumumuz tarafından talep edilen geliştirmeleri ve güncellemeleri belirtilen süreler içerisinde sistemlerine yansıtmakla mükelleftir.

* + - * SBYS yazılımları, kurum içerisindeki entegre edilebilir cihazlar, sistemler ve Bakanlığın tanımladığı ve yürüttüğü uygulamalarla uyum sağlamak zorundadır.
			* SBYS yazılım üreticileri, Bakanlık Kayıt Tescil Sistemine (KTS) kayıt olarak aktif listede yer alması gerekmektedir.
			* Kullanılmasına karar verilen sağlık bilişimi standartları ve veri gönderiminde dikkat edilecek hususlar SBSGM web sayfasında yayımlanır ve güncellenir. SBYS yazılımı

üreticilerinden bu güncellemeleri takip etmesi ve sisteminde gerekli güncellemeleri yapması beklenir.

* + - * Sağlık hizmeti sunucularınca SBYS yazılım üreticilerinden, ürettiği SBYS yazılımının minimum şartlara uyum sağladığını gösteren “KTS Kayıt Belgesi” istenir. KTS kayıt belgesinin geçerliliği KTS web sayfası üzerinden sorgulanır.
			* KTS yetki belgesi olmayan, geçersiz yetki belgesi ibraz eden ya da KTS web

sayfasında pasif listede yer alan SBYS yazılım üreticileri ile sözleşme imzalanmaz.

* + - * Kurum ile SBYS yazılım üreticisi arasında yaşanabilecek uyuşmazlıklarda uygulanacak cezai şartların SBYS yazılım üreticisi ile yapılacak sözleşmelerde yer alması sağlanır.
			* Kurum, SBYS yazılım üreticisi ve bayileriyle ayrıca gizlilik sözleşmesi imzalamalıdır. Kurum bu maksatla EKteki Kurumsal ( Gizlilik Sözleşmesini kullanabilecekleri gibi kendileri de sözleşme metinlerini oluşturabilirler.
			* SBYS'lerin ilk kurulumu esnasında uzaktan destek ile kurulum talepleri kabul edilmez.
			* SBYS yazılım üreticisi, ilk kurulum esnasında çalıştıracağı personel ile ilgili planlamayı kurulum ve proje planında detaylı olarak açıklamak zorundadır.
			* Kurulum ve proje planının işletmeye alınacağı tarihe, kurum tarafından karar verilir.
			* Kurum, HBYS tedarikçilerinden en az altı ayda bir kez olacak şekilde son alınan yedek üzerinden veri kurtarma testi yapmasını istemeli ve gerekli kontrolleri yapmalıdır.
			* Herhangi bir sebeple mevcut SBYS yazılımının kullanımına son verilirse, verilerin tamamı orijinal veri tabanı formatında, kolay ve sorunsuz okunabilir bir medya ortamında, 3 (üç) kopya halinde sağlık kuruluşuna teslim edilmek zorundadır.
			* Kritik alanlardaki değiştirme ve silme işlemlerinin, ancak yetki ölçüsünde yapılması gerekir. Değişikliklere sonradan erişim ve geri düzeltme için mutlaka iz kaydı

dosyaları detayları olarak tutulmalı veya VTYS katmanındaki denetleme (audit) uygulama yazılımından da desteklenir olmalıdır.

* + - * Kişisel sağlık verileri özel nitelikli kişisel veriler kapsamında olması sebebiyle;

sözleşme süresince veya sonrasında kayıtlı tüm veriler hiçbir surette, hiçbir zaman SBYS üreticisinde kalmak üzere kopyalanamaz, çıktı alınamaz, firma sunucularına aktarılamaz, ifşa edilemez.

* + - * SBYS yazılımları tüm sistem genelindeki kullanıcı, işlem ve bilgi düzeylerinde bilgi gizliliğini ve güvenliğini sağlamak zorundadır. Her kullanıcının gerektiğinde

değiştirilebilir kişisel bir parolası olmalıdır. Bu parola ile farklı bir lokasyonda oturum açıldığında ilk oturum otomatik olarak kapatılmalıdır. Bir kişiye ait parolanın birden çok kişi tarafından kullanılmasına izin verilmemelidir.

* + - * Çeşitli yetki düzeyleri ve grupları tanımlanabilmeli, yetki değişimi SBYS Yöneticisi tarafından yapılabilmelidir. Verilere erişim bu tanımlamalar çerçevesinde

yapılmalıdır.

* + - * SBYS'de kullanıcılar için saat bazında sisteme giriş sınırlandırması yapılabilmelidir.
			* SBYS“de kullanıcıların otomasyona giriş - çıkış zamanları ve geçersiz giriş denemeleri istenildiğinde raporlanabilmelidir.
			* Poliklinik, Klinik, Laboratuvar bazında yetkilendirmeler yapılabilmelidir. Kullanıcının yetki verilmeyen bir poliklinikteki hasta listesine erişimi engellenmelidir.
			* SBYS yazılımlarında Kurum Parola Politikası maddesinde belirtilen parola özellikleri tanımlanabilmeli ve bu kurala uymayan parolalar kabul edilmemelidir.
			* Sağlık kuruluşu ile ilişiği kalıcı olarak kesilen tüm personelin SBYS erişim yetkisi tamamen ve otomatik olarak iptal edilmelidir.
			* Geçici olarak sağlık kuruluşunda bulunmayan (izin, rapor, geçici görev kurs, eğitim vb.) personelin SBYS'ye girişi otomatik olarak engellenmelidir.
			* Sunucu işletim sistemi, sunucu yazılımları, veri tabanında yapılacak yapısal

değişiklikler gibi tüm sistemi etkileyen güncellemeler mesai saatleri dışında veya hasta yoğunluğunun en az olduğu saatlerde yapılmalıdır. Acil müdahale edilmesi gereken bir arıza durumunda ise mesai saatleri içinde güncelleme yapılabilir.

Doküman adı Doküman kodu

# İlgili dökümanlar:

Bilgi Güvenliği Sözleşmesi

Bilgi Güvenliği Farkındalık Bildirgesi Kurumsal gizlilik sözleşmesi

Bilgi güvenliği olay bildirim ve müdahale formu Kurum yedekleme planı

Kurum yedekleme kontrol listesi HBYS kullanıcı talep formu

Genel ve mesleki oryantasyon eğitim formu Görev devir teslim formu

İlişik kesme formu

HBYS kullanıcı iptal formu Arşiv işleyiş prosedürü