1. AMAÇ:

Bu prosedürün amacı, Özel Ekol Hastanesinde hastalara ait bilgilerin güvenliğinin sağlanması amaçlı öncelikle verilerin doğru olarak toplanması, depolanması ve kullanılmasına ilişkin uygulamalarımızı ve güvenlik önlemlerimizi dâhili olarak gözden geçirmek ve kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemlerini almak ve bunun devamlılığını sağlamaktır.

2. KAPSAM:

Bu prosedür hastanede tüm çalışanları kapsar.

3. KISALTMALAR:

HBYS: Hastane Bilgi Yönetim Sistemi

UPS: Kesintisiz Güç Kaynağı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. SORUMLULAR:

Bu prosedürün uygulanmasından Başhekim, Tedavi ve Bakım Hizmetleri Müdürü, İdari ve Mali İşler Müdürü, Bilgi İşlem Sorumlusu, tüm hastane işletim sistemindeki (H.B.Y.S) yetkilendirilmiş kullanıcıları sorumludur.

5.FAALİYET:

5.1 HBYS'YE İLİŞKİN YAZIMSAL SÜREÇLER

* Hastane çalışanları yaptıkları işle ilgili düzeltme, güncelleme, değişiklik gibi işlemleri bilgi işlem personeline iletir.

* Bilgi işlem personeli kullanıcı ile birlikte sorunu tespit eder ve yazılımsal değişikliğe gerek olan durum varsa firma sorumlusu ile birlikte yazılım şirketine ait olan internet ortamındaki istek bilgilerini sisteme yazılımsal isteği kaydeder ve raporunu bilgi işlem sorumlusuna teslim eder.

*Yazılım şirketi isteği değerlendirip 48 saat içerisinde planlamaya alır. Planlamaya alınan istekler hastane bilgi işlem sorumlusu tarafından kritik derecesi belirlenir. İsteklerin kritik derecesi;

ÇOK KRİTİK: 3 iş günü içerisinde (Yeni çıkan tebliğ, yönetmelik güncellemeleri)

KRİTİK: 5 iş gün içerisinde (Bir bölümün işletmesini aksatacak istekler)

NORMAL: 30 iş günü içerisinde herhangi bir işleve etki etmeyecek, yazılımda düzeltme yapılacak istekler.

*İstekler yukarıda belirtilen süreler dışına çıkmış ise sözleşmesinde belirtilen cezai işlemler devreye girer.

*Normal sürelerde yapılan istekler ise bilgi işlem sorumlusu ve isteği yapan kullanıcı tarafından onaylanarak, sistem üzerinden kapatılır.

BİLGİ YÖNETİM SİSTEMİNE İLİŞKİN ROL GRUPLARI VE YETKİLERİ

Otomasyon üzerinde yazılımı kullanan tüm personellerin yetkilendirilmesi yapılmıştır. Bu gruplardaki personeller yalnızca kendilerine verilen yetki kadar işlem yapabilir.

Bu rol grupları;

• Yönetim • Başhekim • Doktor • Başhemşire • Hemşireler • Poliklinik sekreteri
• Satın alma • Kalite • Faturalama vb.

Çalışanların yetkileri düzenlenmiştir ve kayıt altına alınmaktadır. Aynı görevde çalışan personellerin yetkileri de aynıdır. İşe yeni başlayan personel bilgi işlemden kullanıcı yetkilendirme formu doldurarak birim yöneticisinin onayı ile kullanıcı adı ve şifresi verilir.

Birimler arası yetkilendirme aşağıdaki gibidir:

Yönetim: İdari ve mali işlemlerle ilgili tüm bilgilere erişebilir.

Başhekim: Hastanedeki tüm bilgilere ulaşır.

Doktor: Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Elektronik ortamda kayıtlı olması gereken tüm hastaya ait tüm bilgileri girebilir. Onay işlemlerini kendi şifreleri ile yapmakla yükümlüdürler. Onaylanmadan önce kendilerine ait raporlar üzerinde silme ve değişiklik yapabilir.

Hasta ‘Adli Olgu’ ise hasta raporu ancak uzman tarafından girilebilir ve aynı uzman tarafından onaylandıktan sonra değiştirilemez.

Başhemşire/Hemşire: Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Silme ve değiştirme yetkileri yoktur. Kendi işlerine ait laboratuvar ve preop. –postop. hasta bilgilerini, hastaya ait sarf ve işlem girişlerini yetkileri dahilinde yapabilirler.

Poliklinik Sekretarya: Doktorun istemlerini ve sarfları hastanın hesabına ekler. Hatalı yaptığı işlemleri sorumlularına bildirirler. Sorumluların düzeltemediği işlemleri hastane otomasyonu üzerinde sorumlusuna bildirir. Hasta yatış –çıkış işlemleri için gerekli evrakları düzenler. Hasta taburcu işlemlerini yapar.

İnsan Kaynakları Birimi: Personel özlük bilgilerine ulaşabilir, mesai, izin, sevk, rotasyon gibi personelin tüm işleyişini otomasyon üzerinden gerçekleştirir.

Eczane: Katlardan gelen eczaneyle ilgili taleplerin girişlerini yapar, otomasyon üzerinden girişlerin ve ilaçların karşılamasını yapar. Hastaların reçeteleri doğrultusunda ilaçların takibini sağlar.

Radyoloji: Hastaların radyolojik işlemlerini yapar. Tetkik işlemlerinin sonuçlarını otomasyon üzerinden raporunu yazar.

Kalite Birimi: Kalite Dokümantasyon Sisteminden dokümanların kontrolü yetkisine sahiptir. İstatistiki verilere ulaşmak için HBYS'de ilgili alanlara ulaşır.

Laboratuvar: Doktorların hastaları için, yaptığı istemleri alır, çalışmasını yapar ve otomasyon üzerinde hastanın sonuçlarını girer. Otomatik cihazlar için bu işlemler barkotlu sistem ile çalışır. Hasta test sonuçları Laboratuvar Uzman Doktoru tarafından onaylandıktan sonra istem yapan kişiler tarafından hasta dosyasında sonuçlar görülebilir. Hastalar muayene oldukları poliklinikten ve web üzerinden(hastane web sayfası) sonuçları alabilirler.

Sekretarya: Hastaların gelişte otomasyon programına kayıtlarını yapar. Yatış öncesi işlemleri gerçekleştirir.

* Her kademedeki çalışan sadece yetkilendirilmiş olduğu işlemleri yürütebilmektedir. Yetkilendirilmemiş kimseler tarafından yapılan herhangi bir işlemi saptayan bölüm yetkilileri bu durumu en kısa zamanda yeterli delilleri ile birlikte bağlı bulunduğu birime iletilmek üzere bir üst yetkiliye bildirmektedir.

* Tüm çalışanlar otomasyon üzerinde yetkili oldukları bilgileri herhangi bir şekilde farklı ortamlarda paylaşamaz bilgi taşıyamaz.

* Kullanılan yazılımlarla ilgili şifreler kullanıcılara bilgi işlem tarafından verilir ve belli periyotlarda değiştirilmesi istenir. Yetkilendirilen çalışan, şifrelerin kullanılması ve korunması konusunda sorumlu tutulmaktadır.

Kullanıcılara verilen şifrelerle ilgili işlemler aşağıdaki şekilde yürütülmektedir:

* Belirli bir şifre ile yapılan tüm işlemlerin idari ve yasal sorumluluğu söz konusu şifrenin tanımlanmış kullanıcısına ait olduğundan, verilen şifre kullanıcı tarafından değiştirilerek kullanılır.

*Çalışanların yer değiştirmesi veya işten ayrılması durumunda şifrenin kapatılma işlemleri: Bilgi güvenliği açısından ilişiği kesilen personelin şifresinin bir an önce iptali esastır. İlişiği kesilen personelin tüm şifreleri ve kullanıcı yetkileri kullanıma kapatılır.

Otomasyon Bilgi İşlem Çalışanlarının Yetkilendirme İşlemleri:

Aşağıda belirtilen işlemler doğrultusunda bilgi işlem çalışanları yetkilendirmektedir.

• Yazılım kurma ve silme işlemleri

• Bilgi Sistemleri Yöneticisine açık otomasyon sistemi işlemleri

• Üst yönetime açık otomasyon sistemi işlemleri

5.2. SİSTEM ALT YAPISINA İLİŞKİN SÜREÇLER:

5.2.1 Network Donanım Cihazlarının;

*Ana omurgayı (Merkez Switch) taşıyan cihazın, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.

*Ağ cihaz ve yazılımlarını kurar, internet ve intranet bağlantılarını yönetir

*Kenar switch cihazlarının, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.

*Routerların, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.

*Güvenlik cihazlarının, değişen şartlar ve ihtiyaçlar doğrultusunda yapılandırmasını yapar.

*Kablolu (ADSL, GSHDSL, Metro Ethernet) ve kablosuz iletişim cihazlarının (wireless cihazlar, Optik Laser Hat, Wimax..) iletişim cihazlarının yapılandırılmalarını, yönetimini gerçekleştirir.

*Bilgisayar sistemlerinin fiziksel güvenliğinin ötesinde yazılımsal güvenlini de sağlamak.

*Elektronik ortamda sisteme olabilecek saldırıları (virus, worm, rootkit, backdoor, trojan, hacker keyloger, spyware v.b.) engellemek,

*Sistem odasındaki cihazların bakım ve onarımlarını yapar/yaptırır.

*Tüm bilgisayar sisteminin sağlıklı çalışmasını sağlayan antivirus sunucularını, kurar, günceller, bakımını yapar, sistemin virüs saldırıları nedeni ile kesintiye uğramaması için tedbirler alır. Yeni çıkan virüslere yönelik güncelleştirmeleri sisteme yükler.

*Tüm bilgisayarların donanımsal ve yazılımsal arızalarını giderir. Son çıkan güncellemeleri takip eder ve hastane sistemindeki tüm bilgisayarlara yükler.

5.2.2 İnternet Bağlantılarının;

*Hastanenin internet Bağlantısını yönetir, izler yetkili kullanıcıların internete erişimine izin verir.

*Firewall cihazının yönetimini yapar, IP, port, yetkilendirmesi yapısını yönetir.

*Filtreleme cihazı aracılığı ile uygun olmayan içeriğe ulaşımı engeller, zararlı sitelerin kullanıcı bilgisayarlarını bozmasına engel olur. Yeni çıkan zararlı siteleri cihaz güncellemeleriyle engeller.

*Internet kullanıcılarının hastane web sitesine ulaşmasını, Web Sunucusunun güvenli biçimde internet üzerinden internet yayını yapmasını sağlar.

*Elektronik posta sunucusunu kurar, işletir, kurum kullanıcılarının e-posta alıp göndermesini sağlar.

*Kurumsal kullanıcıların kendilerine verilen yetkilendirmeler dâhilinde sistem kaynaklarını kullanmasına izin verir.

5.2.3 İşletim Sistemlerinin;

*Yazılım güncelleştirmelerini, yamalarını, loglarını, performanslarını izlerler.

*İşletim sistemlerinin yapılandırma/konfigürasyonlarını yaparlar.

*İşletim sistemlerinin güvenlik ayarlarını yaparlar.

*İşletim sistemlerinin üzerinde çalıştığı fiziksel sunucuların çalışma düzenini kontrol ederler.

*Donanım kaynaklarının (Diski, Ram, Kontrol Kartları, Güç Kaynakları, İşlemciler) çalışırlığını izler ve kontrol ederler.

5.2.4 Sunucu ve Veritabanlarının;

Sunuculara tahsis edilmiş bir bağımsız oda bulunmaktadır

*Sunucuların olduğu odaya görevlendirme olmayan personel bu odaya girememektedir.

*Oda hastanenin B Blok 5. katında bulunmaktadır. Oda içinde su tesisatı bulunmamaktadır.

*Sunucu Odalarında elektrik kesilmesi durumunda UPS devreye girmektedir. Bunun yanında yedekli güç kaynakları (UPS) mevcut olup, periyodik bakımları yapılmaktadır.

*Isı ve nem takibi otomatik olarak yapılarak sıcaklık ve nem 2 saat arayla sisteme kayıt edilmektedir 30 derece üzerine çıkan oda sıcaklıklarında bilgi işlem sorumlusuna SMS ile bilgilendirme atılmaktadır.(Sıcaklık 18-22 °C,Nem %30-%50 arasında bulunmaktadır)

*2. Klima yedek olarak bulunmaktadır.

*Veri tabanın performansını izlerler.

*Veri tabanının bakımını gerçekleştirir.

*Yedeklerinin alınmasını sağlar ve/veya gerçekleştirirler.

*Yedek alma ve arşivleme işlemi depolama cihazlarını ve kotaları yönetir,

*İlgili sistemlerde bulunan verilerin yedeğini uygun periyotlar da alır.

*Programlar her veri güncellemesinde yedeklenir ve harici harddisk de arşivlenir.

* Kullanıcı bilgisayarlarındaki verilerin merkezi olarak yedeklenmesi ve arşivlenmesi teknoloji olarak mümkün olmakla birlikte hali hazırdaki birim imkânları ile gerçekleştirilemediğinden kullanıcılara ait veri yedekleme işlemi kullanıcıların kendileri tarafından müdürlük yedekleme talimatına uygun olarak yapılmaktadır.

*Belirli aralıklarla veri arşivleme çalışması yapar. Güvenli yerlerde muhafaza eder.

*Yedekleme cihazlarını izler.

*Yedekleri güvenli yerlerde saklar.

5.2.5 Antivirüs Politikası:

Bütün bilgisayarda kurumun lisanslı antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır. Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen bilgi işlem 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.

5.2.6 E-Posta Kullanım:

İdari birimler e posta gelen ve giden olarak kullanabilir, diğer birimlere kapalıdır.

5.2.7 Uzaktan Erişim:

- Dış ortamdan iç ortama hangi durumlarda bağlanacağını belirten ilgili firma ile hastane idaresi arasında gizlilik sözleşmesi bulunmaktadır. Dış ortamdan bağlanıldığı durumlar kayıt altına alınmaktadır.
- Hastane çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere kimseye vermemelidir.
- Hastanenin ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdır.
- Uzaktan erişim yöntemi ile kuruma erişen bütün bilgisayarlar en son güncellenmiş anti virüs yazılımına sahip olmalıdır.
- Hastanenin ağına standart dışı erişim isteğinde bulunan organizasyon veya kişilere Bilgi İşlem biriminin özel izni geçici olarak izin verilebilir.
- Periyodik olarak yapılan kontrollerde kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

5.2.8 Şifre Koruma

- Bütün kullanıcılar seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Şifreler başkası ile paylaşılmamalı, kağıtlara ya da elektronik ortamlara yazılmamalıdır.
- Şifrelemede küçük ve büyük karakterlere (örnek, a-z, A-Z), hem de noktalama karakterleri ve ayrıca harflere (örnek, 0-9, !'^+%&/()=?_;*) sahip olmalıdır.
- En az sekiz adet alfa nümerik karaktere sahiptir.
- Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
- Aile isimleri kullanılmamalıdır.
- Herhangi bir kişiye telefonda şifre verilmemelidir.
- E-posta mesajlarında şifre yazılmamalıdır.
- Şifreler aile bireyleriyle paylaşılmamalıdır.
- Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
- Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.

5.2.9 HBYS De Oluşan Sorunların Çözümünde Uyulması Gereken Kurallar

Konu ile ilgili sorunlar HBYS alanında Bilgi İşlem İstekleri bölümünden online istekte bulunarak arıza durumları ve istekler iletilmektedir.

HBYS ile ilgili sorunlar ve çözümler sorunun oluştuğu tarih ve saat bildirimin yapıldığı tarih ve saat kayıt altına alınmaktadır. Bu kayıtlar HBYS modülü üzerinden izlenebilmektedir.

Aylık göstergeler kalite yönetim birimi işbirliği ile yapılmakta olup, sorunlarla ilgili gerekli durumlarda düzeltici önleyici faaliyet başlatılmaktadır.

5.2.10 Bilgi Paylaşımı

İleri tetkik ve tedavi yöntemleri için başka hastane veya özel merkezler sevk sırasında hastaya ait bilgiler ilgili mevzuatın gereklerine uygun belgeler ile hastanın kendisi tarafından iletilmektedir.

Hasta sağlık bilgileri hastanemiz tarafından veya Sağlık Bakanlığının bilgi yönetim sistemleri tarafından araştırma, istatistik ve karar destek sistemleri için kullanılır.

5.2.11 Güvenlik Raporlama Sistemi

Hasta güvenliği ile ilgili istenmeyen olaylar; ilaç güvenliği, cerrahi güvenlik, transfüzyon güvenliği, tesis güvenliği, düşmeler, radyasyon güvenliği, bilgi güvenliği gibi konularda gelişebilir. Hasta güvenliği kapsamında bilgi güvenliği yer almaktadır. Bilgi güvenliğini ilgilendiren istenmeyen durumlarda HBYS ortamında yer alan Güvenlik Raporlama Sistemi alanından bildirimler yapılır. Bildirimlerde gizlilik esastır.

5.2.12 Bilgi Sistemlerinin Genel Kullanım Politikası Uygunsuz Kullanım

Genel olarak aşağıdaki eylemler yasaklanmıştır. Sistem yöneticileri bu kapsamın dışında olabilir. Herhangi bir kullanıcı kurumun kaynaklarını kullanarak hiçbir şart altında herhangi bir yasadışı aktivitede bulunamaz.

5.3 BİLGİ GÜVENLİĞİ

Kurum olarak gizliliğin önem teşkil etmektedir. Bu politika hastanemizde sunulan tüm sağlık hizmetleri için geçerlidir. Hastanemiz hasta hakları, güvenlik, veri bütünlüğü, erişim ve uygulama ile ilgili gizlilik ilkelerine bağlıdır. Verileri yetkisiz erişime, yetkisiz şekilde değiştirilmelerine, açıklanmalarına veya imha edilmelerine karşı korumak için uygun önlemler alınır. Bilgi yönetimine ilişkin faaliyetlerin yürütülmesi ve koordinasyonuna yönelik sorumlular belirlenmiş ve sorumluluklar tanımlanmıştır. Her kullanıcının bilgi yönetim sistemi uygulamalarında hangi bilgilere erişebileceği tanımlanmıştır. Hastanın özlük bilgileri ve kurum bilgileri sadece poliklinik ve servis bilgisayar sekreterleri tarafından değiştirilebilir. Bilgisayar sekreterlerinin bilgileri silme yetkileri yoktur. Hastalarla ilgili her türlü kaydın kim tarafından, hangi tarihte girildiği, ulaşma, değiştirme bilgisi hastane bilgi işlem programı log kayıtları altında tutulmaktadır. Hastaların klinik kayıtlarına yalnızca konu ile ilgili yetkilendirilmiş kişinin giriş yaptığı hastane bilgi işlem programında

"Güvenlik Sistemi" adı altında izlenebilmektedir. Veri tabanı üzerinde Hasta kayıt logları, Hasta Hizmet logları, Hasta Fatura Logları, Hasta Poliklinik logları, Tanımlama Logları, Hasta Dosya logları, Veri tabanı oturum logları, Sağlık kurulu kayıt logları kayıt altına alınmaktadır. Kullanıcıların ara yüze bağlanmak için kullandıkları şifreler, şifreli biçimde veri tabanında saklanmaktadır. Veri tabanı sistem logları gerektiğinde idare tarafından izlenmektedir. Kullanıcılar veritabanına yapılacak müdahale (güncelleme v.b) öncesinde otomasyon sistemi üzerinden bilgilendirilmektedir. Hastaneye destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında hastane tarafından onaylanmış gizlilik sözleşmesi mevcut olup dış ortamdan iç ortama erişimler kayıt altına alınmaktadır.

Topladığımız bilgiler ve onları nasıl kullandığımız: Sağladığınız bilgiler; hastanemize teşhis ve tedavi için başvurduğunda hastalarımızdan kişisel bilgiler (ad, soyad, hastalık bilgileriniz, T.C. Kimlik numarası, adres, telefon bilgileri, vb..) istenmektedir. Hastanemiz yalnızca, hasta bilgi güvenliği politikası ve/veya belirli hizmetlere ilişkin gizlilik uyarısında açıklanan amaçlarla kişisel bilgileri kullanır. Otomasyon kullanan tüm veri giriş personeline işe alınmadan önce eğitim verilmekte, bilgi güvenliği politikasına uymayanlar hakkında gerekli yasal işlemler yapılmaktadır.

5.4. KİŞİSEL SAĞLIK KAYITLARIN GÜVENLİĞİ

Kullanıcılar, hasta ile ilgili bilgileri girilir, muayene ve reçete girildikten sonra hasta kaydı kapanır. Tekrar kullanıcılar bilgileri değiştiremez.

5.5. RİSK YÖNETİMİ

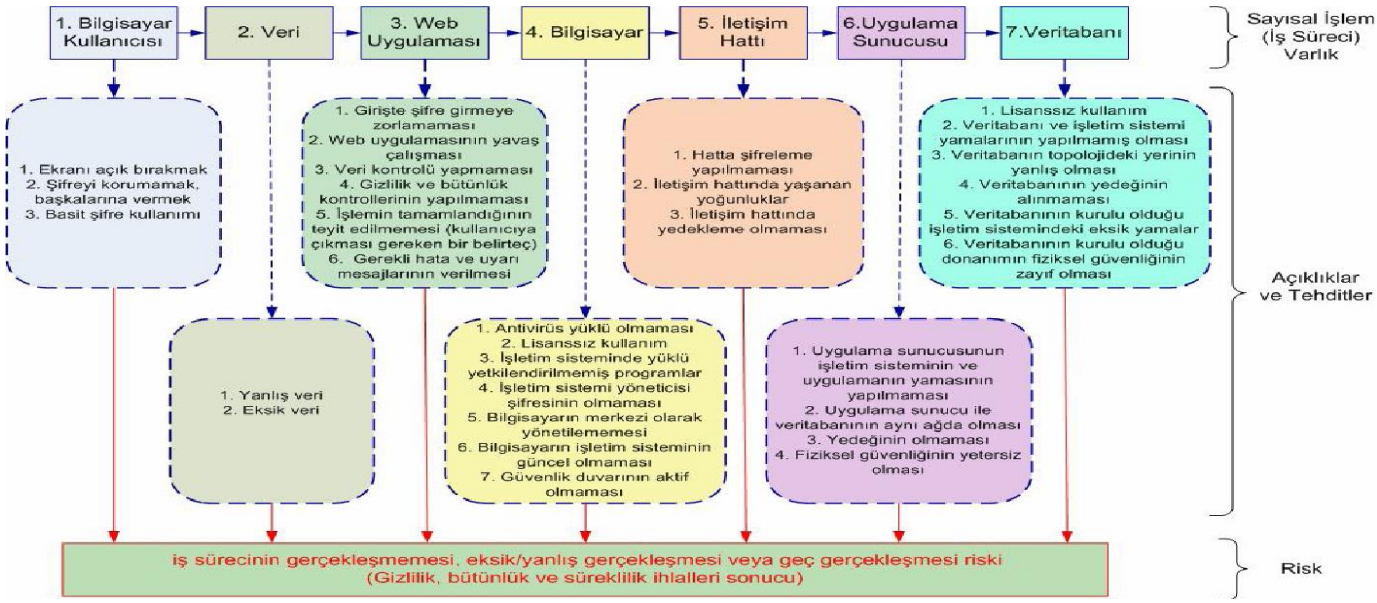
5.5.1 Risk Analizi ve Yönetim Stratejisi

Risk analizi için aşağıdaki metot uygulanmaktadır. Bu faaliyetle ilgili kayıtlar risk değerlendirme raporunda tutulmaktadır. Kapsam dahilinde ki ve bilgi ile ilişkisi olan her varlığın tespiti için varlık keşif çalışması yapılır. Varlık envanteri ile her kullanıcının sahip olduğu (kullandığı ve yönettiği) varlıklar tespit edilir ve varlıkların sorumluları atanır. Risk analizi çalışması tehdit olasılığı ve işe etkisi boyutlarında değerlendirilecektir.

Risk analizi Bilgi Güvenliği Yönetim Sisteminin kapsamına giren hizmetlerin uygulanması sırasında kullanılan ve kazanılan bilgilerin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine yönelik risklerin değerlendirilmesidir.

Risk analizi çalışması tehdit olasılığı ve işe etkisi boyutlarında değerlendirilmektedir. Risk hesaplama formülü kullanılarak her bir varlık için var olan risk değeri hesaplanır. Risk takip tablosunda tanımlanan her bir risk için 6 aylık risk durum değerlendirmeleri yapılarak son durum hesaplanır. Risk değerleri için Risk Değerlerine

Göre İşleme Seçeneklerinden uygun olanı seçilir. Kontrolün nasıl uygulanacağı, kim tarafından uygulanacağı Risk İşleme Takip Tablosunda izlenir.



5.5.2 Bilgi Varlıklarımız

Özel Ekol Hastanesi kapsamı dahilinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları işlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır.

Masaüstü bilgisayarlar, laptoplar, CD ve DVD ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, e-mail, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

Tablo1.VarlıkSınıflandırılması

BİLGİ SINIFLANDIRMA KILAVUZU		Saklanma 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.	Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel bilgisayarlar
İç Kullanım	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi 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

Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan ve işlem içinüçüncü taraflara verilen kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

5.5.3. Kritik varlıklar

Bir organizasyonda varlıkların belirlenmesi ve varlıklara değer atanması, risk analizi süreci için temel bir adımdır. Özellikle ele geçirilmemesi, değiştirilmemesi gerekli bilgiler içeren süreçler veya sürekliliği organizasyonun iş hedefleri ve itibarı için önemli olan süreçler BGYS kapsamında değerlendirilebilir (örneğin web servisi, personel özlük bilgileri).Varlıklara değer atanmasının yapılabilmesi için bir envantere ihtiyaç vardır. Varlık envanteri, olası bir felaket esnasında veya sonrasında, kurtarma veya geriye dönme işlerinde kullanılmak üzere gerekli detayları içermelidir. Varlık tipi, formatı, bulunduğu yer, yedek bilgileri, lisans bilgileri ve ticari bilgileri bulunmalıdır

Varlık envanterinin aşağıda tanımlanan bilgileri içermesi tavsiye edilir:

Varlık: Tabloda bu bölüme varlığın adı yazılır varlıkların birbirinden ayrılması için gereklidir.

Varlık Grubu: Varlık envanterinin okunabilirliğini arttırmak ve düzenli bir yapıda olmasını sağlamak maksadı ile varlıklar gruplandırılabilir. Mantıksal olarak benzer iş için kullanılan varlıklar bir grupta bulunabileceği gibi (ör: dokümanlar, kılavuzlar, altyapı sistemi, e-posta servisi vb.) iş süreçleri çerçevesinde bir gruplandırma (ör: iş sürekliliği süreci) yapılabilir. Ayrıca varlıklar, mantıksal olarak varlık grupları altında listelenebilirler. Varlık grubu veya varlığın adı yazılır. Ör: Kablosuz ağ sistemi, uygulama ve veri tabanı sistemi.

Kategori: Varlık envanterinde anlaşılabilirliğin arttırılması maksadıyla varlıklar ortak kategoriler altında derlenebilirler. Sunucu, yazılım, donanım, medya, doküman, kılavuz, tablo, bilgi, kurum çalışanı vb ortak özelliklere sahip varlıklar bu kategori altında listelenebilir.

Varlık Sahibi: Varlık sahibi, tanımlanan rol ve sorumluluklara paralel olarak belirlenir. (Ör:Muhasebe Bölümü Sorumlusu)

Emanetçi: Varlığın –varsa– emanetçisini belirtir. (Ör: Ağ Yöneticisi)

Bulunduğu Yer: Varlığın bulunduğu fiziksel yeri belirtir.(Ör: Sistem odası)

Gizlilik Değeri: Varlığın yetkisiz kişilerce erişilmesi sonucu doğacak zararı belirtir.

Bütünlük Değeri: Varlığın bütünlüğünün bozulması sonucunda doğacak zararı belirtir.

Erişilebilirlik Değeri: Varlığın erişilebilirlik açısından önemini belirtir.

Değer: Gizlilik, bütünlük ve erişilebilirlik değerleri kullanılarak belirlenebilecek bir değerdir.

Varlığın Eklenme Tarihi: Varlığın, varlık listesine eklenme tarihidir. Envanter takibi ve uygun risk analizinin yapılıp yapılmadığını takip etmek için kullanılabilir bir veridir.

Tablo 2. Güvenlik Hedefi Varlık Değeri Tablosu

GÜVENLİK HEDEFİ	DÜŞÜK	ORTA	YÜKSEK	ÇOK YÜKSEK
GİZLİLİK	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkilemez /çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
BÜTÜNLÜK	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
ERİŞİLEBİLİRLİK/ KULLANILABİLİRLİK	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Açıklama: Nitel değerlendirmelerle ilgili yardımcı açıklamalar, varlığın kısa tanımını ve gerekli olabileceği düşünülen diğer bilgileri içerir.

Bunların yanında, envanter hazırlanırken her bir varlık için alınmış *güvenlik önlemleri*nin envantere işlenmesi risk analizi için gerekli zaman ve iş gücünü ciddi anlamda azaltacaktır.

Karşı kontroller belirlenirken varlık için alınmış güvenlik önlemleri değerlendirilecektir.

Donanım varlıkları için *marka, model, seri numarası* bilgileri, yazılımlar için *yazılım tipi,üretici bilgisi, sürüm numarası, lisans bilgileri, yama bilgileri* envantere işlenmesi tavsiye edilen bilgiler arasındadır.

Hazırlayan	Kontrol Eden	Onaylayan
Kalite & Akreditasyon Sorumlusu Kardelen ASMA	Kalite Koordinatörü Yeşim İNCİ	Kalite Yönetim Direktörü Prof. Dr. Tuncay ÇAĞLAR