1. Amaç:

Bilgi Yönetim Sistemi Politikası'nın oluşturulması etkin iş ve çalışma ortamının sağlanması, kurum kültürünün korunması, itibarın zarar görmemesi için önemlidir. Selçuk Üniversitesi Diş Hekimliği Fakültesi Bilgi Yönetim Sistemi Politikası'nın amacı kurumumuz bünyesinde yürütülen bilgi yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları tanımlamaktır.

2. Kapsam:

Fakültemizde Bilgi Yönetim Sistemi Politikası kapsamında kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının güvenliğinin (gizliliğinin ve bütünlüğünün) sağlanması hedeflenmektedir.

3.KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi

BİB: Bilgi İşlem Birimi

HBYS: Hastane Bilgi Yönetim Sistemi

PUKÖ: Planla, Uygula, Kontrol Et, Önlem Al

UPS: Uninterruptible Power Supply (Kesintisiz Güç Kaynağı)

4.TANIMLAR

Bilgi Güvenliği İhlal Olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

Bilgi Güvenliği Riski: Açıklıklardan fayda sağlamak suretiyle kuruluşa zarar verebilecek varlık ya da varlık gruplarının potansiyel tehdididir. Bir olayın ve sonucunun olasılığının kombinasyon koşulları olarak ölçülür.

Bilgi Güvenliği: Basılı ve elektronik ortamdaki tüm bilgilerin, yasal mevzuat ışığında hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde

kullanılarak "gizlilik, bütünlük ve erişilebilirlik" ilkeleri çerçevesinde istenmeyen kişiler tarafından elde edilmesini önlemektir.

Bilgi Yönetim Sistemi: Kurumların eğitimli kullanıcılar ve bilgisayar ağına bağlı cihazlar aracılığıyla, yapmış olduğu her türlü çalışmayı (poliklinik, laboratuvar, radyoloji, eczane hizmetleri vb.) gerçekleştirmesine, kaydetmesine ve muhafaza etmesine yarayan elektronik yazılımlar grubudur.

Etki: İş hedeflerinin başarısını etkileyen değişimi.

İş Sürekliliği Yönetimi: İş Sürekliliği Planının amacı, firmamızın bilişim sistemlerinde, olası felaket ve iş akışını engelleyecek veya aksatacak her türlü senaryonun gerçekleşmesi halinde, kurumun kritik fonksiyonlarının kesintisiz biçimde devam ettirilmesi ve kesintiye uğrayan fonksiyonların ihtiyaç duyulan süre içerisinde geri döndürülmesidir. İş sürekliliği yönetim sürecinde oluşturulan takımlar, belirli aralıklarla toplantı yapmalı ve sistemi gözden geçirmelidirler.

Risk Analizi: Tehdit ve iş etkisinin çarpımı olan risk puanının bulunması amacıyla her bir bilgi varlığı için zayıflıkların, tehditlerin, iş etkilerinin bulunması ve hesaplanması çalışmasını.

Risk Değerlendirme: Risk analizi sonucunda bulunan değerlerin yorumlanması ve derecelendirilmesini.

Risk Derecelendirmesi: Riskin önemini tayin etmek amacıyla tahmin edilen riskin, verilen risk kriterleri ile karşılaştırılması sürecini.

Risk İletimi: Karar verici veya diğer ortaklar arasında risk hakkındaki bilgiyi paylaşım ya da değişimdir.

Risk Yönetimi: Bilgi güvenliği risklerinin analizi, değerlendirilmesi, işlenmesi ve sürekli iyileştirilmesi amacıyla yürütülen yönetimsel faaliyetleri

Riski Belirleme: Riski oluşturan öğelerin ortaya çıkartılması, tasnif edilmesi ve özelliklerinin belirlenmesini içeren süreçtir.

Riski Transfer Etme: Bir riskin kayıplarını diğer paydaşlarla paylaşma. (Sigorta yaptırma gibi)

Riskin Kabulü/Kabul Edilebilir Risk: Bir riski kabul etme kararı. Bir riskin zararını (negatif sonuçlarını) kabullenmeyi.

Riskten Kaçınma: Riski oluşturan durumdan kaçınma kararıdır.

Varlık (Bilgi Yönetimi): Kuruma ait tüm hassas bilgiler ve bu bilgilerin işlendiği ortamlardır.

5. SORUMLULAR

- Fakülte Yönetimi
- Birim Sorumluları
- Bilgi İşlem Sorumlusu
- Firma Sorumluları
- Tüm Bilgi İşlem Firma Elemanları
- Fakülte Bilgi Yönetimi Sistemini Kullanan Tüm Çalışanlar

6.FAALİYET AKIŞI

Bu politika kurum bilgi işlem altyapısını kullanmakta olan tüm birimleri ve bağlı kuruluşları, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamakla birlikte;

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

b. Uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları,

c. Yönlendirici cihazları, güvenlik cihazları, sistem yönetim sunucuları, yasal yükümlülükler kapsamında kurulmuş sunucu sistemleri, bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıklar,

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

e. Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıklarını kapsamaktadır.

Bilgi Yönetim Sistemi Politikası uyumunda üst yönetim ve bilgi işlem birim personelleri yanı sıra kurumun tüm çalışanları sorumludur.

Bilgi yönetiminde ana hedeflerimiz:

a. Kurumu içeriden veya dışarıdan gelebilecek yazılım ve donanım ile ilgili tüm tehditlere karşı korumak,

b. Üretilen veya kullanılan bilgilerin gizliliğini güvence altına alarak Kişisel Verileri Koruma Kanunu çerçevesinde kurumun imajını korumak,

c. Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak,

d. Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamaktır.

Bilgi güvenliğinin 3 temel bileşeni vardır: Gizlilik, Bütünlük ve Erişilebilirlik. Gizlilik bilginin yetkisiz kişilerce erişime karşı korunmasıdır. Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi ve ortadan kaldırılmasına karşın korunmasıdır. Erişilebilirlik, bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir olmasıdır. Bu konuda tüm çalışanlara işe başlarken Personel Gizlilik Sözleşmesi imzalatılmaktadır. Fakültemizde bilgi güvenliğinin bir gereği olarak, bilgilere sadece yetkili kişilerin erişimi sağlanmaktadır.

Fakültemizde bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve bilgi varlıklarında gizlilik, bütünlük ve erişilebilirlik prensiplerine uyulacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir:

a. Bilgi güvenliğinin en önemli bileşeni kullanıcıların güvenlik bilincidir. Oluşan güvenlik açıklıklarının büyük kısmının kullanıcı hatasından kaynaklandığı bilinmektedir. Bilgi Yönetim Sistemi Politikası kapsamında tüm personelin bilgi güvenliği farkındalıklarını artırmak hedeflenmektedir. Bu amaçla işe alım esnasında

tüm personele ve gerek görüldüğünde ilgililere bu amaçla bilgilendirme yapılmaktadır.

b. Kurumsal şifrelerin seçiminde dikkat edilmesi gereken ayrıntılar belirtilmektedir.

c.Bilgi güvenliği yönetim sistemine karşı riskler düzenli olarak değerlendirilmektedir.

d. Risk seviyelerini kabul edilebilir risk seviyelerinin altında tutmak için önlemler alınmaktadır.

Fakültemiz bilgi işlem alt yapısını kullanan ve bilgi kaynaklarına erişen herkesin aşağıda tanımlanmış olan bilgi güvenliği ilkelerine uyması beklenmektedir:

a. Bilgi güvenliği ve bütünlüğünün korunması her zaman esas olmalıdır.

b. Sözlü, yazılı veya elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilgilerin gizliliği sağlanmalıdır.

c. Çalışanlar işlerinin önemine göre işledikleri bilgiyi yedeklemelidir.

d. Risk tür ve düzeylerine göre gerekli güvenlik önlemleri alınmalıdır.

e. Bilgi güvenliği ihlal olayları en kısa zamanda yetkililere bildirilmeli, raporlanmalı ve bu ihlallerin tekrarını engelleyecek önlemler hemen alınmalıdır.

f. Fakültedeki iş akışı için gerekli her türü bilgi, en az kesintiyle ilgili birim ve hizmet verenler için (yetki dâhilinde olmak koşuluyla) erişilebilir olmalıdır.

g. Hizmet alanlar ve hizmet verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınmalıdır.

h. Bilgi Yönetim Sistemi Politikasına uyum ile bilgi güvenliğine karşı riskler kabul edilebilir düzeyin altında tutulmalıdır.

ı. Bilgi Güvenliği, bilgiye elektronik erişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak her zaman sağlanmalıdır.

i. Bilgi kullanımı veya bilgiye erişimi konusunda gerekli durumlarda (araştırma, yayın, üçüncü kişiler ile paylaşım vb.) uygun izinler mutlaka alınmalıdır.

j. Kurum içi bilgi kaynakları (duyuru, doküman vb.) gerekli izinler ve üst yönetim onayı olmadan üçüncü kişilerle kesinlikle paylaşılmamalıdır.

k. Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kesinlikle kullanılmamalıdır.

Fakültemizde bilgi yönetimi kapsamında; "BY:TL:143.-Bilgi Güvenliği Talimatı", "BY.TL.119.-Bilgi Yönetimi Talimatı", "BY.PR.39.-Bilgi Güvenliği Prosedürü", "BY.PR.25.-Bilgi Güvenliği Gizlilik Sözleşmeleri Uygulama Prosedürü", "BY.FR.136.-Personel Gizlilik Sözleşmesi", "BY.FR.137.-Kurumsal Gizlilik Taahhütnamesi" dökümanları kullanılmaktadır.

6.1. BGYS EKİBİ VE YETKİLERİ

Selçuk Diş Hekimliği Fakültesi bünyesinde bu politika metninde, Bilgi Yönetim Standartlarını karşılamak üzere Bilgi Güvenliği Komitesi bulunmaktadır.

6.1.1. BG Üst Yönetim Görev, Yetki ve Sorumluluklar:

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

♦ Bilgi güvenliği birimi tarafından hazırlanmış bilgi güvenliği konularında geliştirilen politikaları uygulamak üzere gerekli altyapıyı oluşturmak için Bilgi Güvenliği Ekibi tarafından hazırlanmış projelere gerekli kaynağı sağlamak.

♦ Bilgi Güvenliği Ekibi tarafından hazırlanmış, tarafından kabul edilmiş Bilgi Güvenliği Politikasını onaylamak.

♦ Bilgi Güvenliği Ekibi tarafından hazırlanmış Üst Yönetim tarafından kabul edilmiş kontrollerin seçimlerine onay vermek.

♦ Çalışmaların yürütülebilmesi için yatırım kararlarına, Yönetim Kurulu ve üçüncü taraf hizmet alımlarında Bilgi Güvenliği Ekibi tarafından çalışılan uluslararası

standartlar çerçevesinde yapılması gereken çalışma süreçleri, usul ve esaslara dair değişiklikleri onaylamak.

♦ Belirli aralıklarla yapılacak olan Bilgi Güvenliği Ekibi YGG (Bilgi Güvenliği Yönetim Sistemi Yönetim Gözden Geçirme) toplantılarına başkanlık etmek.

♦ Kurum bünyesinde bilgi işleme olanaklarını kullanarak bilginin üretilmesini, taşınmasını, geliştirilmesini, yönetilmesini ve saklanmasını sağlayan tüm çalışanlar Bilgi Güvenliği farkındalığının artırılmasına yönelik planlanan çalışmaların etkinliğinin artırılması için teşvik edici faaliyetleri onaylamak.

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

♦ Bilgi Güvenliği Ekibi tarafından hazırlanmış, Yönetim tarafından kabul edilen Risk Kabul Kriterlerini ve kabul edilebilir riskleri onaylamak.

6.1.2 Bilgi Güvenliği Ekibi Görev, Yetki ve Sorumlulukları:

♦ Bilgi Güvenliği konularının altyapısını oluşturacak projeler hazırlanmasını sağlamak.

♦ Çalışmaların yürütülebilmesi için gerekli çalışma gruplarını oluşturmak ve görev tanımlarını yapmak.

♦ Fakülte bünyesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standartlar seviyesinde bir hizmet kalitesini yakalamak amacıyla TS ISO Bilgi Güvenliği Yönetim Sistemi Standardı, TS ISO Bilgi Teknolojileri Hizmet Standardı, Kurumsal Bilgi Güvenliği Mimarisi gibi konuların gerekliklerinin yerine getirilmesi için gerekli çalışmaları yapmak.

♦ Bilgi Güvenliği Ekibi ve varsa oluşturdukları çalışma gruplarından gelen istek ve talepleri değerlendirmek projelerin dayandırıldığı standartlar çerçevesinde onay vermek.

♦ Projelerde referans alınan standartların temel gereksinimlerinden olan Bilgi Güvenliği Yönetim Sistemi gerekliliklerini oluşturmak ve yönetmek.

♦ Yönetim Sistemi dokümantasyonlarının hazırlanmasına rehberlik etmek ve hazırlanan dokümanları onaylamak.

♦ Üst yönetim onayı gerektiren dokümanların üst yönetim tarafından onaylanmasını sağlamak.

♦ Çalışmaların yürütülebilmesi için gereken yerler ile ihtiyaç duyulan tüm resmi yazışmaların yapılmasını, izinlerin alınmasını sağlamak ve onaylamak.

♦ Projelerin yürütülebilmesi için gerekli olan yönetim hizmetleri çerçevesinde ihtiyaçların temin edilmesinin sağlanmak.

♦ Yapılan çalışmalarla ilgili üst yönetime ve Üst Yönetime rapor sunmak ve bilgilendirme toplantıları düzenlemek.

♦ Yönetim sistemi gerekliliklerinden olan Yönetim Gözden Geçirme, İç Denetim, Farkındalık Eğitimleri gibi faaliyetlerin gerçekleşmesini sağlamak.

♦ Yapılan çalışmalar doğrultusunda yapılacak olan belgelendirme dış denetimlerini (Belgelendirme ve ara denetimler) organize etmek.

♦ Projelerin daha verimli bir şekilde yürütülebilmesi için BGYS Birim personelinin kişisel gelişimleri için gerekli görülen eğitimleri düzenlemek ya da dış taraflarda düzenlenmiş eğitimlere gönderilmesini sağlamak konu ile ilgili tüm yasal izin ve finansal kaynağın sağlanmasını organize etmek.

6.1.3. BGYS Çalışma Grubu Görev, Yetki ve Sorumlulukları

♦ Bilgi Güvenliği altyapısını oluşturacak projeler hazırlanmasına katkı sunmak.

♦ Bilgi Güvenliği politikaların geliştirilmesi için gerekli araştırmaları yapmak, Koordinatöre katkı sunmak.

♦ Yapılacak olan çalışmalarda gerekli iletişim organizasyonu için gerekli düzenlemeleri yapmak.

♦ Fakülte bünyesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standartlar seviyesinde bir hizmet kalitesini yakalamak amacıyla TS ISO Bilgi Güvenliği Yönetim Sistemi Standardı, TS ISO Bilgi Teknolojileri Hizmet Standardı, Kurumsal Bilgi Güvenliği Mimarisi gibi konuların gerekliklerinin yerine getirilmesi için gerekli çalışmaları yapmak

♦ Projelerin yürütülebilmesi için gerekli olan tüm dokümantasyon (Politika, Prosedür, Plan, Süreç Analizi, Risk Yönetimi, Etki Analizi gibi) gerekliliklerine katılmak, dokümantasyon geliştirme faaliyetlerinde yer almak.

♦ Hazırlanan dokümantasyonun yönetim temsilcisi ve (gerekli olanların) üst yönetim tarafından onaylanmasını sağlamak.

♦ Projeler kapsamında yapılacak olan farkındalık eğitimi, temel eğitim, iç denetçi eğitimi gibi konular gereği gerekli düzenlemeleri ve organizasyonları yapmak, eğitim değerlendirmeleri yapmak, katılımcı imzalarının alınmasını sağlamak, rapor halinde Komite başkanına sunmak.

6.1.4. BGYS Ekibi Görev, Yetki ve Sorumluluklar

♦ Yönetim tarafından oluşturulur.

♦ Yönetim ekibe başkanlık eder.

♦ Bilgi Güvenliği konularının altyapısını oluşturacak projelerin yürütülebilmesi için gerekli onay vermek.

♦ Bilgi Güvenliği politikaların geliştirilmesi için hazırlanan projelere katkı sunmak.
♦ Yönetim gerekli görüldüğünde toplantılara katılmak.

♦ Kapsam kararları, risk değerlendirme metodolojisi, kontrollerin uygulanması konularında onay vermek ve bağlı oldukları birimlerde uygulanmasını sağlamak.

♦ BGYS Ekibi tarafından hazırlanan projelerin gerekliliği olan, birim çalışanlarının farkındalık düzeylerinin artırılmasına yönelik organize edilen çalışmaların tüm tabana yayılması için gerekli desteği vermek.

6.1.5. BGYS YGG (Bilgi Güvenliği Yönetim Sistemi Yönetim Gözden Geçirme) Toplantıları

♦ BGYS Komitenin ve üst yönetimin bilgi güvenliğinin uygunluğunu, verimliliğini, risk yönetiminin işlevselliğini, tetkik sonuçlarını, düzeltici ve iyileştirici faaliyetleri ele aldığı yılda en az bir defa düzenlenen bir toplantıdır. Bu toplantıda yönetim risk kabul kriterlerini ve kaynak ihtiyaçlarını değerlendirir. Çalışmaların, risk değerlendirme ve işleme faaliyetlerinin verimliliğini inceler.

♦ Bu toplantılarda standarda göre girdi ve çıktılar Toplantı Tutanağı Formu kullanılarak kayıt altına alınmaktadır.

6.1.6. Diğer BGYS İçerisindekileri Sorumlulukları

a) Bilgi Yönetimi Sistemini kullanan tüm çalışanlar

♦ HBYS sistemini kullanan tüm çalışanlar fakültedeki mevcut tüm bilgisayarlardan kendilerine verilmiş ve görevleri ile yetkilendirilmiş kullanıcı kodu ve şifresi ile yaptığı tüm işlemlerden sorumludur. (Veri girişi,değiştirmesi,silmesi vb.)

b) Tüm Bilgi İşlem Firma Elemanları

♦ Fakültede çalışan tüm personellere otomasyon ile ilgili destek vermek.

♦ Fakülte birimlerinde çalışan tüm personellerin yazılım üzerinde oluşabilecek yenileme, düzeltme gibi işlemleri tespit edip talep değerlendirme komisyonuna teslim etmek.

♦ 24 saat boyunca icap yöntemi ile hastane çalışanlarına uzaktan veya bizzat hastaneye gelerek soruna müdahale etmek.

♦ Sistem odasının fiziksel durumlarını her gün kontrol edip kayıt altına almak.(ısı,nem)

♦ Yazılım üzerinde her türlü gelişmeye destek vermek. c) Firma Sorumlusu

♦ Fakülte çalışanları tarafından bildirilen istekleri yazılım şirketine iletmek,takip etmek ve sonucunu bilgi işlem merkezi sorumlusuna rapor etmek.

♦ Gün içerisinde işlemlerin gün sonunda alınan yedeği sağlam ve çalışır durumda olduğunu kontrol edip imza karşılığı bilgi işlem sorumlusuna teslim etmek.

♦ Fakülte ile yazılım şirketi arasında koordineyi sağlamak.

d) Bilgi İşlem Sorumlusu

♦ Fakülteye ait bilgisayar sisteminin verimli ve amaca uygun çalışmasını sağlamak.
♦ Bilgisayar sistemleri ile ilgili her türlü donanım ve yazılım problemlerinin çözümü, yedeklerinin alınmasını ve bilgilerin arşivlenmesi işlemlerini yürütmek.

♦ Sistemlerin arızalanması durumunda ön inceleme ve bakımını yaparak, gerekli servis hizmetlerinin verilmesini sağlamak.

♦ Bilgisayar sistemlerinin periyodik bakımlarında ve onarımlarında sözleşmeli firma elemanlarını ve çalışmalarını denetlemek, gerekli gördüğü hallerde yazılı-sözlü bilgi vermek.

♦ Her gün mesai başlangıcında bilgisayar sistemleri ve donanımlarının açılmasını, iş bitiminde ise kapatılmasını sağlamak.

♦ Teknik malzemelerin alımında malzemelerin şartnamelere uygunluğunun kontrolünü yapmak.

♦ Faaliyetler çerçevesinde, ihtiyaç duyulan yazılım sistemleri konusunda personele destek vermek; meydana gelen küçük teknik arızaları geciktirmeden gidermek veya giderilmesini sağlamak.

♦ Bilgisayar donanımlarında meydana gelen aksaklıkların giderilmesi için amirine bilgi vermek.

♦ Konusuyla ilgili olarak amiri tarafından verilen diğer işleri yerine getirmek.

e) Bilgi Yönetim Sistemine ilişkin rol grupları ve yetkileri Otomasyon üzerinde yazılımı kullanan tüm personellerin yetkilendirilmesi yapılmıştır. Bu gruplardaki personeller yalnızca kendilerine verilen yetki kadar işlem yapabilir. Bu rol grupları;
♦ Öğretim Elemanları

♦ Klinik Hemşireleri

♦ Sağlık Teknikerleri/Teknisyenleri

♦ Klinik Sekreterleri

♦ Satın alma Birimi

♦ Kalite Yönetim Birimi

♦ Taşınır Kayıt Birimi

♦ Vezne

♦ 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.İşten ayrılırken ise ilişik kesmek için bilgi işleme başvurarak ilişik kesilir.

f) Disiplinler arası yetkilendirme aşağıdaki gibidir;

♦ Dekan : Fakültedeki tüm bilgilere ulaşır.

♦ Diş Hekimi: 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.

♦ Fakülte Sekreteri: İdari ve mali işlemlerle ilgili tüm bilgilere erişebilir.

♦ Hemşire/Sağlık Tek.: Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Silme ve değiştirme yetkileri yoktur. Kendi işlerine ait laboratuar ve preop –postop hasta bilgilerini, hastaya ait sarf ve işlem girişlerini yetkileri dahilinde yapabilirler.
♦ Klinik Sekretarya: Doktorun istemlerini ve sarfları hastanın hesabına ekler. Hatalı yaptığı işlemleri sorumlularına bildirirler. Sorumluların düzeltemediği işlemleri

BİMOB e bildirir. Hasta yatış -çıkış işlemleri için gerekli evrakları düzenler. Hasta taburcu işlemlerini yapar.

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

♦ Döner Sermaye Birimi: Ay içerisinde başvuran tüm hastaların faturalamasını ve anlaşmalı kurumlara teslimatı yapar. Döner sermayeden sorumlu başhekim yardımcısı kurumlara yapılan faturaların tutarlarını ve yapılan işlemleri görebilir inceleyebilir.

♦ 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.

♦ Protez Laboratuvarı: Hekimlerin hastaları için, yaptığı protoz işlerini alır, dezenfekte eder ve sisteme kaydeder. Hastalara ait tamamlanan protezleri system üzerinden hekimlere gönderir.

♦ Klinik 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 BİB tarafından verilir ve belli periyotlarda değiştirilmesi istenir. Yetkilendirilen çalışan, şifrelerin kullanılması ve korunması konusunda sorumlu tutulmaktadır.

6.2. BİLGİ GÜVENLİĞİ

6.2.1. BİLGİ GÜVENLİĞİ HEDEFLERİ VE PRENSİPLERİ

Bilgi güvenliği yönetimi kapsamına alınan tüm süreçlerde ve varlıklarda gizlilik, bütünlük ve erişilebilirlik prensiplerine uyacak önlemler almak amacıyla aşağıda detayları belirtilen risk yönetimi faaliyetleri yürütülmektedir. Her bir varlık için risk seviyesinin kabul edilebilir risk seviyesinin altında tutmak hedeflenmektedir. Risk yönetimi ve kontrollerin uygulanması sürekli bir faaliyettir ve kabul edilebilir risk seviyesinin altına inen riskler için de iyileştirme yapılması hedeflenmektedir.

7.1.1. Sunucuların Güvenliği Fakültemize ait Sunucular ana binamızda bulunmaktadır. Sunucular için aşağıdaki kriterler yerine getirilmektedir.

♦ Sunuculara tahsis edilmiş bir bağımsız oda bulunmaktadır.

♦ Oda kilit altındadır ve sadece bilgi işlem personelinin bilgisindedir. Görevlendirme olmayan personel bu odaya girememektedir.

♦ Oda fakültenin zemin katında bulunmaktadır. Oda içinde su tesisatı bulunmamaktadır.

♦ Sunucu Odalarında elektrik kesilmesi durumunda bağımsız UPS devreye girmektedir. Fakülte genelinde bulunan UPS sistemi desteklemektedir.

♦ Isı ve nem takibi yapılarak sıcaklık ve nem takip formu kayıt edilmektedir.(Sıcaklık 18-22 °C,Nem %30-%50 arasında bulunmaktadır)

♦ Genel iklimlendirmenin yanında 1 adet. Klima yedek olarak bulunmaktadır

♦ Bütün sunucuların yeri, sorumlu kişisi, donanımı ve işletim sistemi üzerinde çalışılan uygulama bilgileri liste halinde bilgi işlem biriminde ve kalite biriminde bulunmaktadır.

♦ Sunucuları içinde bulunduğu oda 24 saat kamera görüntüsü ile izlenmektedir.

6.2.2. Yedekleme

♦ Yedekleme harici bellek, ağ üzerinde çalışan bilgi işlem merkezinde 1 adet PC, sunucunun kendi üzerinde, sunucu odasında 1 adet PC'de yedeklenmektedir.

♦ Yedekleme sunucuda günlük olarak yapılmaktadır. Arşivlemesi harici bellekte 25 günlük, diğer PC'lerde aylık olarak yapılmaktadır.

♦ Veriler yedekleme yapıldıktan sonra offline ortamda saklanmaktadır.

6.2.3. Kişisel Sağlık Kayıtların Güvenliği Kullanıcılar tarafından, hasta ile ilgili bilgiler girilir, muayene ve reçete girildikten sonra hasta kaydı kapanır. Tekrar kullanıcılar bilgileri değiştiremez. Kişisel bilgiler kişinin kendisi veya mahkeme tarafından istenildiği takdirde verilir.

6.2.4. İnternet Erişim Ve Kullanım

♦ İnternet erişimi idari birimler, bilgi işlem ve poliklinikler olarak 3 ayrılmıştır. İdari birimler resmi site ve haber kaynaklı siteler dışı kapalıdır.(Tüm filtrelemeler alizer cihazında logları kayıt altında tutulmaktadır.)Tüm loglar izlenebilir durumdadır. Bilgi işlem Tüm sitelere açıktır. Poliklinikler resmi siteler ve haber siteler dışı tüm sitelere erişim kapalıdır.

6.2.5. Uzaktan Erişim

♦ Dış ortamdan iç ortama hangi durumlarda bağlanacağını belirten ilgili firma ile fakülte idaresi arasında gizlilik sözleşmesi bulunmaktadır. Dış ortamdan bağlanıldığı durumlar kayıt altına alınmaktadır.

♦ Fakülte bölümlerinde çalışan tüm personelin otomasyon sistemine girdiği, kullanıcı kodu ve parolası şifreli şekilde veri tabanında tutulmaktadır.

♦ Her kullanıcının yetkileri otomasyon üzerinden birim yöneticisi tarafından onaylanarak belirlenir.

♦ Fakülte içinde içeriği hasta mahremiyetini etkileyecek olan bilgiler otomasyon sisteminde yetkilendirilip, bilgi işlem personeli dahil kimseye gösterilmez. Yalnızca üst yönetimin onay verdiği kullanıcılara görme yetkisi verilir.

♦ Kullanıcıların sisteme kaydettiği nitelikli hizmetlerin hiçbiri yönetim onayı olmadan, bilgi işlem personeli haricinde hiçbir personel tarafından silinemez.

♦ Gün içerisinde otomasyon sistemine girilen tüm işlemlerin yedekleme işlemi otomatik olarak başlamaktadır.

♦ Personele ait özlük bilgileri ise yalnızca İnsan Kaynakları personeli tarafından görülüp, yetkileri yönetim tarafından belirlenir. Yetkili personel dışında kimse personel özlük bilgilerine erişemez.

♦ Gün içerisinde fakülte internet ağına bağlı olan tüm bilgisayarların hangi zamanda, hangi internet sitesine bağlandığını, ne kadar süreyle o sayfada kaldığı gibi tüm bilgiler fakülte fiziksel güvenlik duvarında yedeklenip log'ları kayıt altına alınmalıdır.

♦ Oluşabilecek virüs saldırıları için fakültenin/ üniversitenin anti virüs lisansı ile bilginin güvenliği sağlanır. Fiziksel güvenlik duvarı ve anti virüsün güncellemelerini ve üst versiyon yüklenmelerini bilgi işlem sorumlusu/Bilgi İşlem Daire Başkanlığı takip eder.

♦ Kurumumuz "Bilgi Güvenliği Planı" çerçevesinde, kurumsal bilgi sistemlerinin güvenliğinde herhangi bir aksamaya mahal verilmemesi için genel sistem seviyesinde alınmış olan güvenlik tedbirleri yanında aşağıda belirtilen hususlara bütün Kurum çalışanları uymak zorundadır.

♦ E-Posta Kullanım Planı

♦ Parola Kullanım Planı

♦ Anti virüs Planı

♦ İnternet ve Ağ Kullanım-Erişim Planı

♦ Genel Kullanım Planı

6.2.6. E-Posta Kullanım Planı

♦ Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.

♦ Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

♦ Kişisel kullanım için İnternet'teki sitelere üye olunması durumunda kurum e-posta adresleri kullanılmamalıdır.

♦ Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt verilmemelidir.
♦ Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

♦ Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

♦ Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

♦ Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.

♦ Kurum çalışanları kurumsal e-postaları kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

♦ Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu ekler virüs, e-mail bombaları ve truva atı gibi zararlı kodlar içerebilirler.

♦ Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.

♦ Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre (personel folder) çekilmelidir.

♦ Fakültemiz çalışanları gönderdikleri, aldıkları veya sakladıkları e-maillerde kişisellik aramamalıdır. Yasadışı ve hakaret edici e-posta haberleşmesi yapılması durumunda yetkili kişiler önceden haber vermeksizin e-mail mesajlarını denetleyebilir ve kullanıcı hakkında yasal ve idari işlemler başlatabilir.

♦ Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren yetkililerle temasa geçip durumu haber vermekle yükümlüdürler.

♦ Altı ay süre ile kullanılmayan e-posta kutuları Bilgi İşlem Birimi tarafından kaldırılabilir. Kurumdan ayrılan personel kurumsal e-posta sistemini kullanamaz. E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma, işten ayrılma sebepleriyle kurumdaki değişikliğini yetkililer tarafından Bilgi İşlem Birimine en kısa zamanda bildirilmesi gerekmektedir.

6.2.7. Parola (Şifre) Kullanım Planı

♦ 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.

♦ Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir.

♦ Tavsiye edilen değiştirme süresi her üç ayda birdir.

♦ 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

♦ Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

♦ Şifreler başkası ile paylaşılmamalı, kâğıtlara ya da elektronik ortamlara yazılmamalıdır.

♦ Şifreler, küçük ve büyük karakterine (örnek, a-z, A-Z), hem rakam hem de noktalama karakterlerine (örnek, 0-9, !''%&/()=?_;*) sahip olmalıdır.

♦ En az sekiz adet alfa nümerik karaktere sahip olmalıdır.

♦ Herhangi bir dilde argo, lehçe veya teknik bir kelime olmamalıdır.

♦ Aile isimleri kullanılmamalıdır. Örnek: Güçlü bir şifre: Br6s8G5!

♦ Herhangi bir kişiye telefonda şifre verilmemelidir.

♦ Şifreler aile bireyleriyle paylaşılmamalıdır.

♦ Şifreler, işten uzakta olunduğu zamanlarda iş arkadaşlarına verilmemelidir.

♦ Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.

♦ Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

6.2.8. Anti Virüs Planı

♦ Bütün bilgisayarlarda kurumun lisanslı anti virüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.

♦ Anti virüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalıdır

♦ Zararlı programları (virüsler, solucanlar, truva atı, e-mail bombalan vb) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.

♦ Hiçbir kullanıcı herhangi bir sebepten dolayı anti virüs programını sistemden kaldıramaz ve başka bir anti virüs yazılımını sisteme kuramaz.

6.2.9.İnternet ve Ağ Kullanım-Erişim Planı

♦ Hiçbir kullanıcı peertopeer bağlantı yoluyla internetteki servisleri kullanmayacaktır, (örneğin: KaZaA, iMesh, eDonkey, Gnutella, Napster, Aimster, Madstcr, FastTrak, Audiogalaxy, MFTP, eMule, Ovemet, NeoModus, Direct Connect, Asquisition, BearShare, Gnucleus, GTK-Gnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, XoLoX, OpenNap, WinMX. vb)

♦ Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

♦ Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ, MIRC, Messenger vb. mesajlaşma ve sohbet (chat) programları kullanılmamalıdır. Bu sohbet programları üzerinden dosya alışverişinde bulunulmamalıdır.

♦ Hiçbir kullanıcı internet üzerinden Multimedia Streaming (video, mp3 yayını ve iletişimi) yapmayacaktır.

♦ Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.

♦ İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) yasaktır.

♦ İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.

♦ Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır,

♦ Üçüncü şahısların kurum içerisinden interneti kullanımları Bilgi İşlem Birim Sorumlusunun izni ve bu konudaki kurallar dâhilinde gerçekleştirilebilecektir

♦ Bilgisayar işletim sistemlerine zarar verdiği için internet üzerinden ekran koruyucu, yamalar, masaüstü resimleri, yardımcı, tamir edici program olduğu belirtilen araçlar gibi her türlü dosya ve programların indirilmesi ve/veya kurulması yasaktır.

♦ Erişim Cihazları (Access Point) ve bilgisayarlara bağlanan bütün erişim cihazlarının ve alt arabirim kartlarının (örnek, PC Card) Bilgi İşlem birimi tarafından kayıt altına alınması gerekmektedir. Erişim cihazları periyodik olarak güvenlik testlerinden geçirilmelidir.

6.2.10. Genel Kullanım Planı

♦ Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.

♦ Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.

♦ Kurumda domain (çalışma alanı) yapısı varsa mutlaka login (oturum açılmalıdır) olunmalıdır. Bu durumda, domain' e bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.

♦ Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Fakülte Sekreterliğine haber verilmelidir.

♦ Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldınlardan (örneğin; elektronik bankacılık, hakaret- siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur,

♦ Kurumun bilgisayarları kullanılarak taciz veya yasadışı olaylara karışılmamalıdır.
♦ Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişilmemelidir.

♦ Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DOS saldırısı, port-network taraması vb. yapılmamalıdır.

♦ Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.

♦ Cihazlar, yazılımlar ve veriler izinsiz olarak kurum dışına çıkarılmamalıdır.

♦ Port veya ağ taraması yapılmamalıdır.

♦ Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.

♦ Kullanıcıların kişisel bilgisayarlan üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

♦ Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programlar (Dergi CD'leri veya internetten indirilen programlar vs.) kurulmamalı ve kullanılmamalıdır.

♦ Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler kurumumuzun bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kâğıt ortamında üçüncü kişi ve kurumlara verilemez.

♦ Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgi sayarlarındaki kurumsal bilgilerin güvenliği ile sorumludur.

♦ Bilgi İşlem Birimi tarafından yetkili kişiler kullanıcıya haber vermek kaydı ile yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım vc onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel bağlanılan bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.

♦ Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/kopyalanmamalıdır.

♦ Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

♦ Kurumda Bilgi İşlem Biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting,E-posta Servisi vb) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.

♦ Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarlarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

♦ Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisansız yazılımı bilgisayarında barından personel ilgili mevzuat çerçevesinde kendisi sorumludur.

♦ Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, Kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

♦ Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir.

7. HBYS'YE İLİŞKİN YAZIMSAL SÜREÇLER

7.1. Yazımsal Süreçler

♦ Fakülte çalışanları yaptıkları işle ilgili düzeltme, güncelleme, değişiklik gibi işlemleri için öncelikle talep değerlendirme komisyonuna görüşülmek üzere bilgi işlem personeline iletir.

♦ Talep kabul edilirse; 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 fakülte bilgi işlem sorumlusu tarafından kritik derecesi belirlenir. Genel olarak kritiklik derecesine göre 10 iş günü içinde istekler gerçekleştirilir.

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

7.2. Sorunların Çözümü

♦ Fakülte iç hat telefon numarası ve HBYS üzerinden arıza bildirimi yapılarak bilgi işlem servisi çalışanlarıyla irtibat kurulur.

♦ İlgili bölümlerden oluşan sorunlar hemen çözülmeye çalışılır çözülemediği takdirde bilgi işlem personelinden yardım alınır. İşlerin aksamamasına meydan verilmemeye çalışılır.

♦ İlgili sorun çözüldüğünde çözen bilgi işlem personeli tarafından HBYS kayıt edilir.

7.3. Bilgi Sistemleri Yöneticisine Açık Fakülte Bilgi Sistemi İşlemleri

7.3.1. Aşağıda belirtilen ve otomasyon sistemi üzerinde normal kullanıcı şifreleri ile yapılamayan işlemler Bilgi İşlem Biriminin yetkisinde olacaktır. Bu işlemlerin yapılabilmesi için gereken şifreler Bilgi işlem Sorumlusu tarafından verilecek ve gerektiğinde değiştirilecektir.

♦ Otomasyon sistemi üzerinde rutin kullanım yolları ile ancak yanlış olarak girilmiş ve aynı yollarla değiştirilmesi mümkün olmayan bilgilerin düzeltilmesi.

♦ Doğru olarak girilmekle beraber kullanıcıların kontrolü dışında yanlış sonuçlar doğuran ve aynı yollarla değiştirilmesi mümkün olmayan bilgilerin düzeltilmesi.

♦ Yetkilendirmeye uygun olmayan hastane bilgi sistemi işlemlerinin hangi operatörler tarafından ve ne zaman yapıldığının sistem kayıtlarından açığa çıkarılması.

7.4. Üst Yönetime Açık Fakülte Bilgi Sistemi İşlemleri

♦ Üst Yönetiminin kurum planlaması, tıbbi, işletme, mali değerlendirmeler ve benzeri amaçlar ile otomasyon sistemi üzerinden alacakları raporlar Bilgi İşlem Birimi Otomasyon çalışanları tarafından yapılır.

7.5. Otomasyon Bilgi İşlem Çalışanlarının Yetkilendirme İşlemleri

Aşağıda belirtilen işlemler doğrultusunda Bilgi İşlem Birimi Otomasyon çalışanları yetkilendirmektedir.

♦ Yazılım kurma ve silme işlemleri

♦ Bilgi Sistemleri Yöneticisine açık otomasyon sistemi işlemleri

♦ Üst yönetime açık otomasyon sistemi işlemleri

Yazılım Kurma ve Silme İşlemleri Otomasyon sistemi dahilindeki her türlü yazılımın kurma, silme ve düzenleme işlemleri ile işletim sistemi ayarlarının yapılması ve değiştirilmesi Bilgi İşlem Birimi Otomasyon yetkisindedir. Bilgi İşlem Birimi Otomasyon bilgisi dışında herhangi bir yazılım kurma ve silme işlemi ve işletim sistemi ayarları yetkilendirilmemiş bir işlem olarak değerlendirilecektir ve tamamen ilgili cihazın kullanıcısının sorumluluğundadır.

Otomasyon Sistemi Işlemleri Fakülte bilgi yönetim sistemi işlemleri, Otomasyon Yetkililerinin onayladığı şartlar kapsamında saptanan çalışanın veya Bilgi işlem dairesi başkanlığının yetkisinde olacaktır. Verilen standart yetkiler dışında istenilen bir yetki, bağlı bulunduğu yöneticinin onayından sonra, uygun görüldüğü seviyede BİMOB tarafından verilir.

8. SİSTEM ALT YAPISINA İLİŞKİN SÜREÇLER

8.1. 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 fakülte sistemindeki tüm bilgisayarlara yükler.

8.2. İnternet Bağlantılarının;

♦ Fakültemizin internet bağlantısı Recep Tayyip Erdoğan Üniversitesi Bilgi İşlem Dairesi Başkanlığı tarafından yönetilmektedir.

8.2.1.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.

8.2.2. Veri tabanlarının;

♦ 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 DVD medyada 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.

♦ Yedekleme cihazlarını izler.

♦ Yedekleri güvenli yerlerde saklar.

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

8.2.3. Yazılım Geliştirme

♦ Kurumsal kullanıcılardan gelen hastane hizmetlerine yönelik yazılım taleplerini değerlendirmek

♦ Talep değerlendirme komisyonu tarafından onaylanan yazılım talepleri ile analiz çalışmalarını yapmak.

♦ Programın çalışması için gerekli kaynakları belirlemek ve sistem yönetimine müdürün onayı sonrasında bildirmek

♦ Yazılım geliştirme platform ve temel yazılım geliştirme mimarisi belirlenir.(clien-server/web tabanlı,lokal,Windows vb.)

♦ Veri tabanı belirlenir. Yazılım geliştirme dili seçilir.

♦ Analiz çalışmalarına dayalı olarak temel fonksiyonların yazımı gerçekleştirilir, menülerin yazılımına başlanır.

♦ Programın yazılımı sonrasında çalışma testleri yapılır. Testler sonrasında çıkan bugler düzeltilir.

♦ Son kontroller sonrasında veri tabanındaki test verileri silinir, Programı yönetecek kişi için kullanıcı tanımlamaları yapılır.Program devreye alınır.

♦ Programın devreye alınması sonrasında program kullanıcılarından gelen programla ilgili sorunlar giderilir, kullanıcılara teknik destek verilir.

♦ Programın görsel tasarımı kurumsal kimlik standartlarına uygun olarak tasarlanır.

8.2.4. Web Uygulamaları ve Web Tasarım Çalışmaları

♦ Web uygulamaları geliştirme çalışmaları yapılır.

♦ Yazılım geliştirme sürecinde tanımlanan temel onay analiz ve ön çalışmalar yapılır.

♦ Uygulamaların intranet ya da internet uygulaması olması durumuna göre web sunumu, sistem yönetimi tarafından tahsis edilir, gerekli ağ ve güvenlik ayarları yapılır.

♦ Birimlerden gelen, duyuru, birim faaliyetleri, spor etkinlikleri, kültürel etkinlikler, yönetim kararları vb.fakülte web sitesinden yayınlanması amacıyla gerekli görüşme, kodlama ve tasarım çalışmaları yapmak.

♦ Fakülte sitesinde kullanılacak görsel materyalleri temin etmek, üretmek ve kurumsal kimliğe uyumlu olarak sitede kullanmak.

♦ Temin edilen materyalleri fish animasyon, ikon, buton üretmek

♦ Kurumsal uygulamalarının web sitesi içinde uyumlu biçimde çalışması için kodlama ve görsel tasarım çalışmaları yapmak(e-randevu, , yerleşim haritası, fakülte bilgi ehberi vb.)

♦ Web sitesi alt uygulamalarını geliştirmek ve yönetmek (istek, şikâyet, bilgi edinme, performans programı, stratejik plan, hizmetlerimiz)

8.2.5. Sistem Operatörleri

♦ Fakülteye özgü uygulamaların çalışırlığını izler, performanslarını varsa loglarını izler.

♦ Varsa yazılımı üreten firma aracılığı ile güncelleştirmeleri yapılır, uygulamada görülen aksaklıklar ilgili firmaya en hızlı yöntemlerle sözlü ve yazılı olarak iletilir.

♦ Fakülte uygulamaları aracılığı ile üretilen verilerin yedeklerini alır.

9. RİSK YÖNETİMİ

9.1. Risk Analizi ve Yönetim Stratejisi

♦ Risk analizi için Bilgi İşlem Ekibi tarafından riskler belirlenir, Kalite Yönetim Birimi ile koordineli olarak çalışılır.

10. BİLGİ HASSASİYETİ VE RİSKLER

10.1. BİLGİ VARLIKLARIMIZ

♦ Fakültemiz bünyesinde 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.

10.2. VARLIK SINIFLANDIRILMASI

Saklanma Yeri Dolap-Bilgisayar BİLGİ SINIFLANDIRMA KILAVUZU Gizli En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi İç Kullanım veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır. Sadece birimlere özel bilgilerdir. Birim çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır. Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel şifreli bilgisayarlar Birim dolapları, kişisel şifreli 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 çekmeceleri Kuruma Açık Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer. Birim ortak dolapları Halka Açık Bu bilgilertedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir. Dolaplar ve dolap dışlarında 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 için üçüncü taraflara verilen kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

10.3. KRİTİK VARLIKLAR

Varlık Kritik Değer Tablosundaki gizli ve iç kullanım varlıkları kritik varlık olarak kabul edilecektir. Bu varlıklar risk değerlendirme tablosundan faydalanılarak oluşturulacaktır.

11. SÜREKLİ İYİLEŞTİRME FAALİYETLERİ

İhlal olaylarıyla veya personelin kendi gözlemleriyle tespit ettikleri uygunsuzlukların tespitinde ve standarda, politikalarımıza, prosedür ve kurallarımıza uymayan durumların tespitinde ortaya çıkan uygunsuzluğun nasıl giderileceği ve potansiyel uygunsuzlukların henüz ortaya çıkmadan önce nasıl önleneceğine ilişkin prosedür ve talimatlarımız bulunmaktadır. Tüm personel belirlenen prosedürlere uymak ve katılmakla sorumludur.

12. İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ

Çalışan personele ait şahsi dosyalar Personel ve Özlük İşleri odasında muhafaza edilmekte ve odanın anahtarı sadece Personel ve Özlük İşleri Sorumlusunda bulunmaktadır. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmektedir. ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında (Hekim başlayış/ayrılış/kadro başvurusu v.b.) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmektedir. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemektedir. İmha

edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) geri dönüşüm olarak kullanılmamaktadır. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmaktadırlar. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim eder. İşe başlayan her personele (tam zamanlı/yarı zamanlı/iş-kur) bilgi güvenliği zafiyetleri konularında eğitim verilmektedir. Bu eğitimler uyum eğitimleri sonrasında yapılmaktadır. Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın) imzaladığı bir belgedir. İşe başlayan her personele kurum kimlik kartı vey aka kartı çıkartılmaktadır.

13. POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Bilgi Güvenliği Politikası kapsamında oluşturulmuş kural ve süreçleri ihlal eden personel, paydaş ve üçüncü taraflar hakkında adli ve idari yasal takibat başlatılarak; ilgili kanun hükümleri gereğince işlem yapılabilir ve /ve ya ilgili sözleşmelerde yer alan yaptırımları bir ya da birden fazla hükmü uygulanabilir. Bahsi geçen cezai işlemlerden bazıları aşağıdaki gibidir:

- ♦ Uyarma
- ♦ Kınama
- ♦ Aylıktan kesme
- ♦ Kademe ilerlemesinin durdurulması
- ♦ Para cezası
- ♦ Sözleşmenin feshi

14. PLANIN DUYURULMASI

İşbu "Bilgi Güveliği Politikasının " yürürlüğe girmesinin ardından tüm birimlere yazılı olarak iletilir. Politikanın tüm personelce okunup okunmadığı ayrı ayrı her bir birimin Amiri/Bölüm başkanı sorumluluğundadır.

15. PLAN GÖZDEN GEÇİRME KURALLARI

Bilgi Güvenliği Politikası, Bilgi Güvenliği Sorumluları tarafından periyodik olarak yılda bir kez, gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler planının gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen plan Kurum Yönetimi tarafından onaylanır. Onaylanan plan Kurum internet sitesi ve çeşitli duyuru kanallarında yayımlanır.

HAZIRLAYAN	**KONTROL EDEN** Kal. Yön. Sorumlusu	**ONAYLAYAN** Dekan