Rev. No.	Revizyon Sebebi	Revizyon Tarihi
01	Prosedür SKS 6 kapsamında gözden geçirildi. Bilgi Güvenliği, Bilgi Güvenliği İhlal Olayı ve Bilgi Güvenliği Yönetim Sistemi (BGYS) tanımları eklendi. Bilgi Güvenliği Ekibi SKS 6 da geçmediği için prosedürden çıkarıldı. Bilgi yönetim sisteminin yönetilmesindeki görev ve sorumluluklara değinildi.	03.03.2021

1. **AMAÇ:** Tüm süreçlerde bilgilerin yönetilmesi, korunması, dağıtımı ve bilgilerin güvenliğini sağlamak üzere;

- Bilgi yönetimini etkin bir şekilde sağlamak,
- Bilgi Güvenliği Yönetim Sistemi gereksinimleri olan bilginin gizliliği, bütünlüğü ve erişilebilirliği prensiplerine uymak amacıyla risklerin belirlenerek, risklere ilişkin kontrol önlemlerinin alınmasını içeren risk yönetim metodolojisini sürekli uygulanabilir kılmak,
- Bilgilerin bütünlüğünü ve gizliliğini korumak,
- Bilgi Güvenliği kapsamında iş gücünü, kaliteyi ve memnuniyeti arttırmak, standart ve yasal mevzuata uyumu sağlamak,
- BGYS'nin verimliliğini, iç ve dış denetimlerle kontrol etmek, izlemek, gözden geçirmek ve sistemi sürekli uyumlu kılmak, sürekli iyileştirmek.

2. **KAPSAM:** Bu prosedür sunulan tüm hizmetlerde bilgilerin yönetimi, güvenliği ve korunmasını kapsar.

3. **KISALTMALAR:**

3.1. **NOC:** Network Operations Center

3.2. **ICT:** Information and Communication Technology

3.3. **BGYS:** Bilgi Güvenliği Yönetim Sistemi

3.4. **SBYS:** Sağlık Bilgi Yönetim Sistemi

3.5. **VPN:** Virtual Private Network

3.6. **LBYS:** Laboratuvar Bilgi Yönetim Sistemi

3.7. **PACS:** Picture Archiving Communication Systems

3.8. **VLAN:** Sanal Yerel Alan Ağı

4. **TANIMLAR:**

4.1. **Gizlilik:** Bilginin sadece yetkili kişiler tarafından erişilebilir olması, bilginin yetkisiz kişilerce yapılan değiştirmelerden korunması ve değiştirildiğinde farkına varılması durumudur.

4.2. **Kullanılabilirlik/Erişilebilirlik:** Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an erişilebilir ve kullanılabilir olması durumudur.

4.3. **Bilgi Güvenliği:** Bilgi ve bilgi işleme tesislerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümüdür.

4.4. **Bilgi Güvenliği İhlal Olayı:** Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarıdır.

4.5. **Bilgi Güvenliği Yönetim Sistemi (BGYS):** Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, yazılı hale getirilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünüdür.

4.6. **İdare:** Kamu Hastane Yönetimi

4.7. **İşletme:** Akfen Hastane Yönetimi

4.8. **Log Kaydı:** Log kaydı; tüm hareketlerin birer birer kayıt altına alınmış olduğu dosyalardır. Örneğin bir web sunucusunun içerisinde yer alan log dosyaları incelenerek ziyaretçilerin nereden geldiği ve web sunucusuna hangi istekleri gönderdiği kolaylıkla anlaşılabilir.

4.9. **NOC Ekibi:** Bir kurumun iş ağının gece gündüz izlendiği ve sorunlarının giderildiği Ağ Yönetimi Sistemine bağlı olarak çalışan fiziksel altyapıya sahip bir merkezde hizmet sunan tekniker ve mühendislerden oluşan ekiptir.

4.10. **ICT Ekibi:** Hastanenin hasta kabul etmeye devam etmesi ve hastane çalışanlarının görevlerini ve faaliyetlerini sürekli şekilde yerine getirebilmesi için hastane içerisinde kapsam gereği kurulumu yapılan bilgi teknolojileri altyapı sistemi, ekipmanları ve yazılımlarının izlenmesini, izleme sistemlerinin üreteceği alarmlar doğrultusunda erken müdahale yapılmasını ve kullanıcılardan gelecek talep ve arıza konularına performans parametrelerinde belirtilen süreler içerisinde yanıt verilmesini ve düzeltilmesini sağlayan ekiptir.

4.11. **E-Nabız:** Sağlık Bakanlığı tarafından oluşturulan, kişisel sağlık bilgilerinizi yönetebileceğiniz, Türkiye'nin güvenilir kişisel sağlık kaydı sistemidir.

5. **SORUMLULAR:** Bu prosedürün uygulanmasından tüm çalışanlar sorumludur.

6. **FAALİYET AKIŞI:**

6.1. **BİLGİ YÖNETİM SİSTEMİ AMAÇ VE KAPSAMI**

Prosedürde belirtilen politika, 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 kullanılabilirliğini sağlamayı amaçlamaktadır.

İdare, İşletme ve HBYS Uygulama ve İşletim Hizmetleri tarafından BGYS'nin tüm süreçleri için gerekli yönetimsel destek ve kaynaklar sağlanır.

Kurum bilgi güvenliği faaliyetlerinin etkin olarak yürütülmesi maksadıyla yaygın olarak kabul gören bilgi güvenliği standartları, ilgili yasa, mevzuat ve yönetmeliklerin gerektirdiği şartlara yönetim tarafından uyulacak, ilgili taraflarca uyulması sağlanacaktır. İç bağlamda belirtilen unsurlar, ilgili standart, mevzuat ve yönetmeliklerin getirdiği sorumluluklara uymakla yükümlüdür.

6.2. **BİLGİ GÜVENLİĞİ**

6.2.1. BYS ile ilgili politikaların oluşturulması, BYS'ye ilişkin faaliyetlerin yürütülmesi ve koordinasyonunun sağlanması, bilgi güvenliği ile ilgili hususlarda gerekli çalışmaların yapılması amacıyla sorumlular ve sorumluluklar ilgili görev tanımlarında belirtilmiştir.

6.2.2. **Bilgi Yönetimi ve Güvenliği Hedefleri**

Bilgi güvenliği hedefleri aşağıdaki gibi sıralanmıştır:

- Kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak
- Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak

Amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi yönetimi ve güvenliğini sağlamayı hedefler.

Hizmet sunumu sürecinde yer alan tüm bilgi sistemlerini, bilişim kaynaklarını, fiziksel bilgi varlıklarını, bilişim ağları ve altyapısını, uygulama yazılımlarını, veri tabanı sistemlerini, tüm bilgi işlenen platform ve süreçleri ve bu süreçlerde görev yapan personel ve tedarikçiler de dâhil tüm paydaşları kapsar.

Bilgi güvenliği ve kişisel verilerin korunması konusunda çalışanlara yılda en az bir kez farkındalık eğitimi, ayrıca bilgi yönetim sisteminin etkin kullanılabilmesine ilişkin bilgi yönetim sistemi uygulamaları hakkında eğitim verilmektedir.

6.2.3. **Bilgi Yönetimi ve Güvenliği İlkeleri**

Hizmet politikası gereği ilkemiz Tekirdağ Şehir Hastanesi'nde kurulan sistemde Hastane Bilgi Yönetim Sistemi'ni etkin ve verimli yöneterek, çalışanlarımızın, tedarikçilerimizin, hizmet verdiğimiz tüm kurum ve kişilerin memnuniyetini sürekli arttırmaktır. Prosedürde belirtildiği üzere HBYS Uygulama ve İşletim Hizmetinin sunumu Turkcell tarafından gerçekleştirmektedir.

Bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kesinlikle kullanılmaz.

Bilgi güvenliği konusunda gizlilik, bütünlük ve erişebilirlik olmak üzere 3 temel prensip göz önünde bulundurulur.

Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:

- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
- Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
- Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı, risk analizi; yazılım ve donanımla ilgili sorunlar, bilgi güvenliği, bilgi mahremiyeti, kullanıcı hatalarını içerir. Tespit edilen riskler doğrultusunda iyileştirme çalışmaları yapılır.

Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3. kişilere iletilemez.

Bilgi güvenliği konusunda tüm çalışanlara **"Yıllık Eğitim Planı"**nda belirlenen zamanlarda ve uyum eğitimi kapsamında işe başlarken bilgi güvenliği ve kişisel verilerin korunması konusunda farkındalık eğitimi verilir.

Şifre kullanımı ile ilgili detaylar **"Şifrelendirme Prosedürü"**nde belirtilmiştir. Bilgi yönetim sisteminde kullanılan parolalar, Bakanlık parola politikaları ile uyumludur.

Bilgi yönetim sistemi sorumluları ve kullanıcılarına **"Personel Gizlilik Sözleşmesi"** imzalatılır.

6.2.4. Erişim ve Yetki Kontrolü

Erişim ve yetki kontrolü aktif dizin üzerinde bulunan güvenlik grupları ile sağlanır. Bilgilerin güvenliği için tüm kullanıcılara kendi yetkilerine göre her kademede yetkilendirme yapılmıştır. Tüm personel kendi alanı ile ilgili, ancak yetkilendirilmiş olduğu işlemleri gerçekleştirilebilir. Erişimler HBYS Uygulama ve İşletim Hizmetleri tarafından **"Bilgi Sistemleri Yetkilendirme Prosedürü"** doğrultusunda gerçekleştirilir.

Bilgilerin bütünlüğü ve güvenliği kurulmuş olan bilgisayar yazılım programlarında yetkilendirilmiş girişler ile korumaya alınmıştır.

6.2.5. Fiziksel ve Çevresel Güvenlik Yönetimi

Güvenlik önlemleri kapsamında tüm bilgisayarlar ve yazıcıların güç kabloları kullanıcıların temas mesafesinden uzak ve dağınık olmayacak bir şekildedir. Ayrıca tüm yazıcılar bulundukları masalara sabitlenmiş durumdadır.

6.2.6. Uzaktan ve Kablolu Erişimlerde (Dış Ortamdan İç Ortama Erişim) Güvenlik Tedbirleri

Sisteme erişim ve yetkilendirme İdare, İşletme ve HBYS Uygulama ve İşletim Hizmetleri tarafından belirlenmiş olan esaslara göre düzenlenir.

Sisteme erişim kontrolü Proje Yöneticisi ve ICT Ekip Lideri tarafından ilgili kişilerin yetki ve sorumlulukları dikkate alınarak düzenlenir.

Sistemde herhangi bir arıza durumunda, NOC Ekibi uzaktan erişimle arızaya müdahalede bulunur.

Proje Yöneticisi ve ICT Ekip Lideri bilgisi dışında bilgisayarlar üzerindeki ağ ayarlarında, kullanıcı tanımlarında, kaynak profillerinde vb. uygulamalar üzerinde mevcut yapılan düzenlemeler hiçbir suretle değiştirilemez.

Bakanlığın bilgi güvenlik politikası gereği domain yapısı oluşturulmuş, tüm bilgisayarlar domain yapısına login durumda çalışmaktadır. Domaine bağlı olmayan bilgisayarlar yerel ağdan çıkarılmış, yerel ağdaki cihazlar arasında bilgi alışverişi yapılmamaktadır.

Dış ortamdan iç ortama erişebilme koşulları ve erişim sağlayabilecek kişiler belirlenmiştir. Dış ortamdan iç ortama yapılan erişimler **"Dış Ortamdan İç Ortama Erişim Prosedürü"** doğrultusunda yapılır ve dış ortamdan iç ortama yapılan erişimler kayıt altına alınır.

Hizmet alımı kapsamında hastane verilerine fiziksel veya bilgi sistemleri vasıtası ile erişim sağlayabilen tüm kişilere personel gizlilik sözleşmesi imzalatılır.

Hastane verilerine fiziksel veya bilgi sistemleri vasıtası ile erişim sağlayabilen tüm firmalar ile kurumsal gizlilik sözleşmesi yapılır.

6.2.7. Kişisel Verilerin Korunması

"6698 Sayılı Kişisel Verilerin Korunması Kanunu"na göre hizmet verilir. Kişisel verilerin depoladığı sistemler yetkisiz erişime karşı korunur.

Çalışanların ve hastaların kişisel bilgilerine erişim, sadece bilgilere ulaşma yetkisi bulunan çalışanlar ile sınırlı tutulur ve bu kişiler gizliliği koruma yükümlülüklerini bilerek çalışır. Çalışanların ve hastaların bilgilerine yetkili olmayan kişilerin ulaşımına / kullanımına izin verilmez.

Kullanıcılar SBYS veya Windows ortamına aktif dizin hesapları ve parola politikasına uygun güçlü şifreleri ile giriş sağlar. Ek olarak tüm cihazlarda aktif ve güncel çalışan (merkezi yönetilen) antivirüs yazılımı bulunur. Bu sayede kişisel verilere tehdit oluşturan dış etkenlere karşı koruma sağlanır.

6.2.8. Virüs ve Saldırganlardan Korunma

Bilgisayarları virüslerden ve saldırılardan korumak için gerekli alt yapıyı sağlamak ICT Ekibinin, bilgisayarları virüslerden koruma sorumluluğu ise kullanıcılara aittir.

Sorumlular tarafından virüs ve saldırılardan korunma için gerekli donanım ve yazılım İdare ve İşletme'ye bildirilerek firewall, kullanıcı yetkileri gerekli tedbirler alınmaktadır.

Bu tedbirler, güncel anti virüs yazılımları ve firewall gibi donanımsal ve yazılımsal uygulamaları içeren asgari şartlardan oluşur.

Bu yazılımların güncellenmesini zamanında gerçekleştirmek de ICT Ekip Lideri Sorumlusunun sorumluluğundadır. Güncellenme zamanlarında İdare ve İşletme konu ile ilgili bilgilendirilir.

6.2.9. Dosya Sunucusu

Çalışanlar ağ üzerinde bulunan dosya sunucusu üzerinde yetkilendirildikleri alanlara erişebilirler.

6.2.10. İletişim Güvenliği

6.2.10.1. İnternet Erişimi ve Kullanımı

İnternet erişimi FW (Güvenlik Duvarı) üzerinden Sağlık Bakanlığına (SB-Net) yönlendirilerek yapılır.

İnternet erişimi, kullanımı ve kısıtlamalar Sağlık Bakanlığı Kamu Hastaneler Birliği (KHB) tarafından belirlenen yetki çerçevesinde sağlanır. Bunun haricinde tüm bilgisayarlardan resmi sitelere erişim sağlanmaz.

Proje Yöneticisi ve ICT Ekip Lideri sadece İdare ve İşletme tarafından gelen, internet erişim ve kullanım taleplerini karşılar.

İnternet erişimi ve e-posta kullanım bağlantıları firewall cihazı tarafından kontrol edilir. İnternet kullanımında giriş yapılabilecek sayfalar ve internet uygulamaları firewall üzerinden yetkiye dayalı olarak belirlenmiştir.

Kişisel ve elektronik iletişimde üçüncü taraflarla yapılan bilgi alışverişinde kuruma ait bilgilerin gizliliği sağlanır.

6.2.10.2. E-Posta Kullanımı

İşe alınan tüm çalışanlara e-posta adresi ve şifresi bağlı çalıştıkları firmalar ve kamu çalışanlarına İdare tarafından verilir. Kişilere mail adresleri verildikten sonra ICT Ekip Lideri tarafından gerekli e-posta programları ve yapılandırmalar gerçekleştirilir.

6.3. BİLGİ YÖNETİM SİSTEMİNİ OLUŞTURAN ALT SİSTEMLER

Tekirdağ Şehir Hastanesi'nde SBYS ile entegre olarak LBYS (Laboratuvar Bilgi Yönetim Sistemi) ve PACS (Picture Archiving Communication Systems) sistemleri bulunmaktadır.

6.4. SAĞLIK BİLGİ YÖNETİM SİSTEMİ İŞLETİM VE DEĞİŞİKLİK YÖNETİMİ

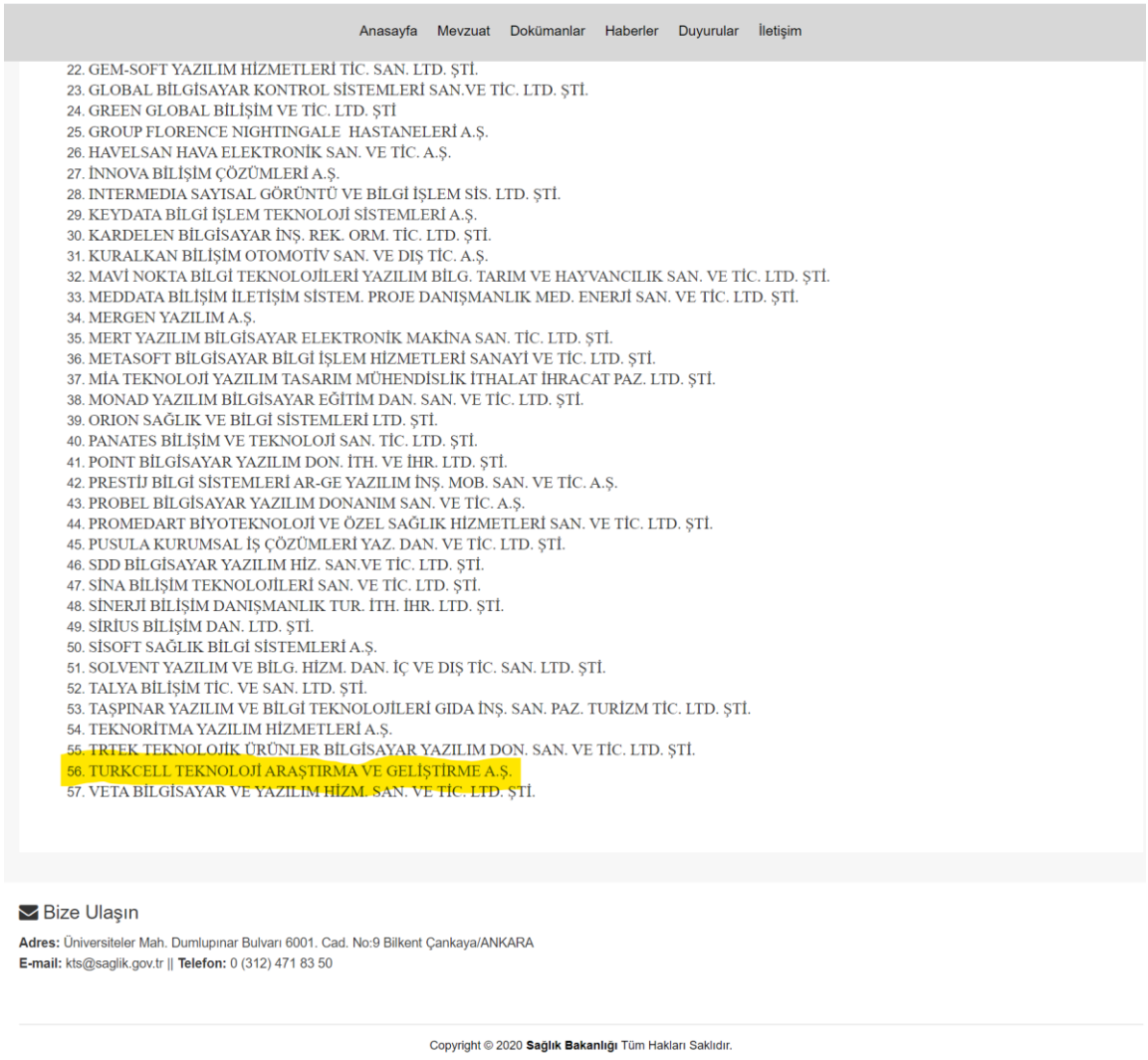
Hastanemizde kullanılan SBYS kullanıcı dostudur. Sistem ara yüzü tüm kullanıcıların kolaylıkla kullanılabileceği bir şekilde dizayn edilmiştir. SBYS tarafından tarih kontrolleri yapılır. SBYS üzerinde kullanıcılar için kısayollar oluşturulmuştur. Tüm kısayollar sistematiktir. Kısayollar **"HBYS Kısayol Listesi"**nde belirtilmiştir.

Bilgi Yönetim Sisteminin etkin kullanılabilmesi amacıyla ilgili tüm çalışanlara işe girişten itibaren ve ihtiyaç durumunda eğitimler verilir. Eğitimler **"Eğitime Katılım Formu"** ile kayıt altına alınır.

SBYS'nin muayene ekranlarından ulusal sağlık veri tabanına (e-nabız) entegrasyon sağlanmıştır. Hastaların aynı hastanedeki geçmiş tıbbi kayıtlarına SBYS üzerinden erişim sağlanabilir.

SBYS, T.C. Sağlık Bakanlığı Kayıt Tescil Birimi tarafından tescil edilmiştir. SBYS tescil durumu T.C. Sağlık Bakanlığı https://kayittescil.saglik.gov.tr/TR,54929/aktif-hbys-listesi.html adresinden teyit edilebilmektedir.

Kayıt tescil durumu aşağıda belirtilmiştir:



Anasayfa Mevzuat Dokümanlar Haberler Duyurular İletişim

22. GEM-SOFT YAZILIM HİZMETLERİ TİC. SAN. LTD. ŞTİ.
23. GLOBAL BİLGİSAYAR KONTROL SİSTEMLERİ SAN.VE TİC. LTD. ŞTİ.
24. GREEN GLOBAL BİLİŞİM VE TİC. LTD. ŞTİ
25. GROUP FLORENCE NIGHTINGALE HASTANELERİ A.Ş.
26. HAVELSAN HAVA ELEKTRONİK SAN. VE TİC. A.Ş.
27. İNNOVA BİLİŞİM ÇÖZÜMLERİ A.Ş.
28. INTERMEDIA SAYISAL GÖRÜNTÜ VE BİLGİ İŞLEM SİS. LTD. ŞTİ.
29. KEYDATA BİLGİ İŞLEM TEKNOLOJİ SİSTEMLERİ A.Ş.
30. KARDELEN BİLGİSAYAR İNŞ. REK. ORM. TİC. LTD. ŞTİ.
31. KURALKAN BİLİŞİM OTOMOTİV SAN. VE DIŞ TİC. A.Ş.
32. MAVİ NOKTA BİLGİ TEKNOLOJİLERİ YAZILIM BİLG. TARIM VE HAYVANCILIK SAN. VE TİC. LTD. ŞTİ.
33. MEDDATA BİLİŞİM İLETİŞİM SİSTEM. PROJE DANIŞMANLIK MED. ENERJİ SAN. VE TİC. LTD. ŞTİ.
34. MERGEN YAZILIM A.Ş.
35. MERT YAZILIM BİLGİSAYAR ELEKTRONİK MAKİNA SAN. TİC. LTD. ŞTİ.
36. METASOFT BİLGİSAYAR BİLGİ İŞLEM HİZMETLERİ SANAYİ VE TİC. LTD. ŞTİ.
37. MİA TEKNOLOJİ YAZILIM TASARIM MÜHENDİSLİK İTHALAT İHRACAT PAZ. LTD. ŞTİ.
38. MONAD YAZILIM BİLGİSAYAR EĞİTİM DAN. SAN. VE TİC. LTD. ŞTİ.
39. ORION SAĞLIK VE BİLGİ SİSTEMLERİ LTD. ŞTİ.
40. PANATES BİLİŞİM VE TEKNOLOJİ SAN. TİC. LTD. ŞTİ.
41. POINT BİLGİSAYAR YAZILIM DON. İTH. VE İHR. LTD. ŞTİ.
42. PRESTİJ BİLGİ SİSTEMLERİ AR-GE YAZILIM İNŞ. MOB. SAN. VE TİC. A.Ş.
43. PROBEL BİLGİSAYAR YAZILIM DONANIM SAN. VE TİC. A.Ş.
44. PROMEDART BİYOTEKNOLOJİ VE ÖZEL SAĞLIK HİZMETLERİ SAN. VE TİC. LTD. ŞTİ.
45. PUSULA KURUMSAL İŞ ÇÖZÜMLERİ YAZ. DAN. VE TİC. LTD. ŞTİ.
46. SDD BİLGİSAYAR YAZILIM HİZ. SAN.VE TİC. LTD. ŞTİ.
47. SİNA BİLİŞİM TEKNOLOJİLERİ SAN. VE TİC. LTD. ŞTİ.
48. SİNERJİ BİLİŞİM DANIŞMANLIK TUR. İTH. İHR. LTD. ŞTİ.
49. SİRİUS BİLİŞİM DAN. LTD. ŞTİ.
50. SİSOFT SAĞLIK BİLGİ SİSTEMLERİ A.Ş.
51. SOLVENT YAZILIM VE BİLG. HİZM. DAN. İÇ VE DIŞ TİC. SAN. LTD. ŞTİ.
52. TALYA BİLİŞİM TİC. VE SAN. LTD. ŞTİ.
53. TAŞPINAR YAZILIM VE BİLGİ TEKNOLOJİLERİ GIDA İNŞ. SAN. PAZ. TURİZM TİC. LTD. ŞTİ.
54. TEKNORİTMA YAZILIM HİZMETLERİ A.Ş.
55. TRTEK TEKNOLOJİK ÜRÜNLER BİLGİSAYAR YAZILIM DON. SAN. VE TİC. LTD. ŞTİ.
56. TURKCELL TEKNOLOJİ ARAŞTIRMA VE GELİŞTİRME A.Ş.
57. VETA BİLGİSAYAR VE YAZILIM HİZM. SAN. VE TİC. LTD. ŞTİ.

Bize Ulaşın

Adres: Üniversiteler Mah. Dumlupınar Bulvarı 6001. Cad. No:9 Bilkent Çankaya/ANKARA
E-mail: kts@saglik.gov.tr || **Telefon:** 0 (312) 471 83 50

Copyright © 2020 **Sağlık Bakanlığı** Tüm Hakları Saklıdır.

6.4.1. SBYS Modülleri

SBYS'de, farklı hizmet süreçlerine yönelik birçok farklı modül bulunur. SBYS'de yer alan modüller birbirine entegre bir şekilde çalışmaktadır. SBYS'de, farklı hizmet süreçlerine yönelik gerekli modüller oluşturulmuş ve sistem ihtiyaçları karşılayacak şekilde belirli aralıklarla güncellenmektedir.

Malzeme ve cihaz istemlerinin yapılmasından, bölümlerde kullanılmasına kadar geçen tüm süreçlere ilişkin işlemler SBYS üzerinden gerçekleştirilir.

SBYS üzerinde, ilgili modüllerin kullanımına ilişkin yardım bilgileri bulunur.

6.4.2. SBYS Üzerinde Yapılan İşlemlerin İzlenmesi

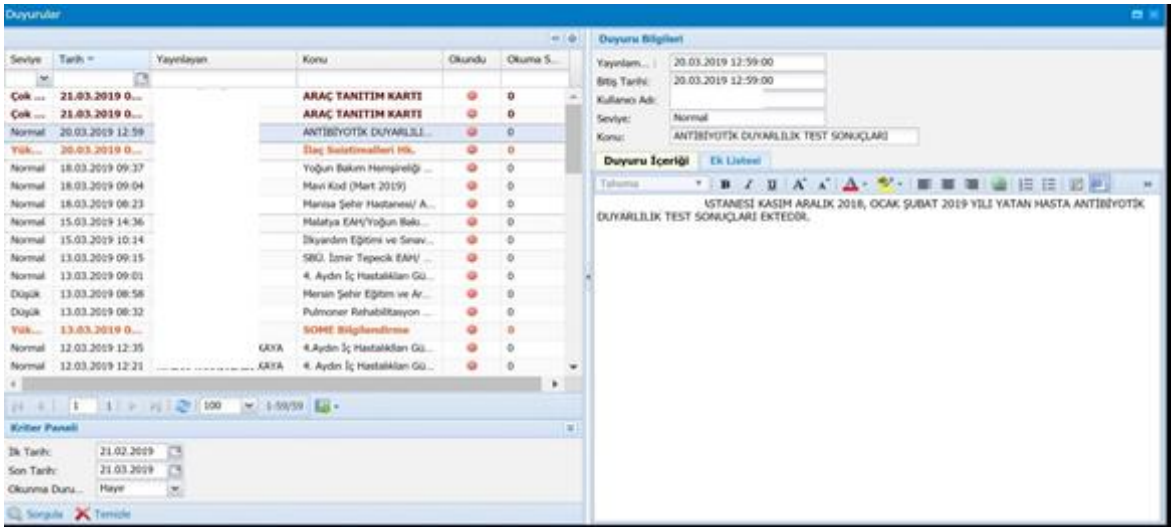
SBYS üzerinde yapılan işlemler **"Sağlıkta Minimum Loglama Standartları (SAMİLOG)"** doğrultusunda loglanır. Toplanan tüm tıbbi bilgilerin geçmişe yönelik takibi yapılabilir:

- Tüm düzeltme ve iptal kayıtları tutulur.
- Salt okunur özellikte ayrı bir veritabanı ya da tablo bulunur.
- Veritabanı ya da tablolarda sisteme giriş yapan kullanıcılar, gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalar log izleme yazılımı tarafından kayıt altına alınır.
- Bu veritabanı ya da tablolara sadece bilgi sisteminde yönetici olarak yetkilendirilmiş kişiler ulaşabilir.

6.4.3. SBYS Uygulamalarına İlişkin Güncellemeler

SBYS yazılım geliştirme süreçleri **"Yazılım Geliştirme ve Test Versiyonu Uygulama Prosedürü"** doğrultusunda yürütülür. SBYS versiyonları öncelikle kurumun test sunucusuna aktarılır ve testler tamamlandıktan sonra gerçek ortamda devreye alınır.

SBYS de yapılan değişiklikler sonucunda sürüm notlarıyla yeni versiyon yayınlanır ve bilgi yönetim sistemi uygulamalarına ilişkin güncellemeler hakkında kullanıcıların bilgilendirilmesi sağlanır. SBYS de duyuruya eklenerek kullanıcının bilgilendirilmesi sağlanır. Sağlık Bilgi Yönetim Sistemi uygulamalarına ilişkin güncelleme geçmişleri kullanıcılar tarafından izlenebilir.



6.4.4. Bilgi Yönetim Sistemine İlişkin Rol Grupları ve Yetkileri

Bilgi yönetim sistemine ilişkin rol grupları (hekimler, hemşireler, sekreterler vb.) ve yetkileri belirlenmiştir. İşe yeni başlayan ve işten ayrılan personele erişim yetkilerinin verilmesi ve iptal edilmesine yönelik yetki verme ve iptal etme süreçleri **"Bilgi Sistemleri Yetkilendirme Prosedürü"**nde tanımlanmıştır. Çalışanlar yetkileri konusunda bilgilendirilir ve yetki düzeyleri kayıt altına alınır. Her kullanıcının Sağlık Bilgi Yönetim Sistemi uygulamalarında hangi bilgilere erişebileceği tanımlanmıştır. Aynı görevi icra eden çalışanlar aynı yetki gruplarına sahiptir.

Rol grupları ve kullanıcılar için tanımlanan yetkiler İdare tarafından, periyodik olarak ve gerektiğinde (görev değişikliği, işten ayrılma vb.) gözden geçirilmekte, gerekli güncellemeler yapılmaktadır.

6.5. BİLGİ YÖNETİM SİSTEMİ DONANIM, ALTYAPI, YÖNETİM VE TALEP SÜREÇLERİ

6.5.1. Sistem Sürekliliği İçin Gerekli Teknik ve Destek Alt Yapıları

Bilgi Yönetim sisteminin etkinliği ve sürekliliği için gerekli teknik ve destek alt yapıları oluşturulmuştur.

Yazılım-donanım destek birimi bulunmaktadır. Donanım ve yazılım destek birimi 24 saat ulaşılabilir durumdadır. İletişim bilgileri hastanenin ilgili birimlerinde bulunur.

Bilgi yönetim sisteminin kesintisiz ve güvenli çalışabilmesi ICT ve HBYS Ekip Liderleri sorumluluğundadır. Bilgi güvenliğine yönelik gerekli tüm önlemler ICT ve HBYS Ekip Liderleri tarafından alınır.

Bilgisayar uygulamalarında ve veri tabanı sunucularında donanım ve yazılıma ait problemler ortaya çıktığında, bilgi güvenliği ile ilgili acil bir durum oluştuğunda ve yerel / uzaktan sisteme bağlanarak çalışmaların devam ettirilmesi gerektiğinde öncelikle Proje Yöneticisi durumdan haberdar edilir. Proje Yöneticisinin yönlendirmesi doğrultusunda ilgili kişilerle iletişime geçilir.

Bilgi yönetim sistemdeki arızalar ve devre dışı kaldığı durumlar nedenleri ile birlikte kayıt altına alınır. Sistemde tespit edilen kesinti ve arızalara yönelik gerekli iyileştirme çalışmaları yapılır.

Bilgi yönetim sistemi ile ilgili olarak oluşan durumlara yönelik tüm kararlar Proje Yöneticisi tarafından alınır ve gerekli ise Hastane İdaresi Bilgi İşlem Sorumlusu durumdan haberdar edilir.

7/24 sistem izleyen ve gerektiğinde destek hizmeti veren NOC Ekibi'nin dış ortamdan iç ortama hangi durumlarda erişim yapacağı, HBYS Uygulama ve İşletim Hizmetleri ile firma arasında imzalanan ve her iki tarafın da onayladığı teknik şartname ve hizmet alım sözleşmesine göre kayıt altına alınmıştır.

6.5.2. Veri Merkezlerinin (Sunucu Odalarının) Güvenliği

Sunucu odalarının güvenliği **"Veri Merkezi (Sunucu ve Sistem Odası) Güvenliği Prosedürü"** doğrultusunda sağlanır. Sadece sunuculara tahsis edilmiş, 2 ayrı lokasyonda bulunan, bağımsız, 2 ayrı veri merkezi bulunmaktadır.

Sistem odasına girişler kontrol altına alınmıştır. Yetkisiz kişilerin veri merkezlerine girmesine izin verilmez. Veri merkezi kapıları geçiş kontrollüdür, giriş çıkış yapan personellerin kaydı tutulur. Veri merkezleri kamera sistemleri ile izlenir.

Veri merkezlerinde su kaynaklı tehlikelere karşı gerekli önlemler alınmıştır. Veri merkezleri suya karşı iyi bir yalıtıma sahiptir. Veri merkezlerinde su basmasına neden olabilecek musluk, kalorifer peteği, atık su gibi tesisat bulunmaz.

Veri merkezlerinde yangın tehlikesine karşı gerekli önlemler alınmıştır. Gaz temelli yangın söndürme sistemi FM 200 sistemi bulunmaktadır. Elektrik sisteminin güvenliği sağlanmaktadır. Yangın dağılımını kolaylaştıracak tefrişat ve malzeme bulunmamaktadır. Gaz temelli yangın söndürme sistemi için gerekli kişisel koruyucu ekipmanlar hazır bulundurulur.

Veri merkezlerine özel hastanedeki diğer kesintisiz güç kaynaklarından bağımsız kesintisiz güç kaynağı bulunmaktadır.

Veri merkezlerinde yedekli olarak çalışan ve nem tutma özelliği olan klimalar bulunur. Sıcaklık ve nem takibi yapılarak kayıt altına alınır. Veri merkezi sıcaklığının 18-22 ^{o}C, nem oranının ise %45-%70 aralığında olması sağlanır.

Veri merkezlerinde alev, duman, ortam sıcaklığı ve su basması ile ilgili olağan dışı durumlarda sistem yöneticilerini uyarmak üzere ortam izleme ve uyarı sistemleri bulunur.

6.5.3. Sunucu Özellikleri

Kurumda bulunan bütün sunucuların kayıtları tutulur. Bu kayıtlarda asgari sunucunun adı, yeri, IP adresi, türü, ana işlevi, üzerinde çalışan uygulama ve servisler, işletim sistemi ve sürümü, sorumlu kişi ve iletişim bilgileri, donanım bilgileri, garanti durumu bilgileri yer alır. Tüm bu bilgiler **"Sunucu Özellikleri Bilgi Formu"**nda belirtilmiştir.

Veri merkezinde bulunan sunucuların sorumlusu ICT Ekip Lideri'dir. Sunucu üzerinde çalışan işletim sistemleri hizmet sunucu yazılımları ve antivirüs programları günceldir. Sistem üstündeki tüm bileşenler, yedekli olarak çalışır.

Sunucuların yazılım ve donanım bakımları garanti kapsamında ise üretici firmanın uygun gördüğü sıklıkla gerçekleştirilir. Garanti süresi bittiğinde firma ile bakım anlaşmalı yapılmış ise bakım anlaşmasında göre bakım yaptırılır. Anlaşma yok ise ICT Ekip Lideri tarafından bakım gerçekleştirilir.

Sunucular güvenlik duvarının arkasında yapılandırılmıştır.

Bütün sunucuların yönetiminden ICT Ekibi sorumludur. Sunucu konfigürasyonları, sunucular üzerindeki her türlü yazılım, işletim sistemi, veri tabanı, bilgi işlem birimi ve dış hizmet alınmış ise yazılım elemanları tarafından gerçekleştirilir.

6.5.4. Veri Tabanı Güvenliğini Sağlamaya Yönelik Tedbirler

Veri tabanı güvenliği **"Veri Tabanı Güvenliği Prosedürü"** doğrultusunda sağlanır. Bilgi yönetim sisteminde kritik verilere ve tıbbi bilgilere ait değiştirme, düzeltme, silme, erişim işlemleri (veri tabanı ya da tablolarda sisteme giriş yapan kullanıcılar, gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalara ilişkin iz kayıtları) bir noktada loglanır.

Bu loglar veri tabanı içinde güvenli olarak kayıt altına alınmakta ve salt okunur bir şekilde saklanır.

Log kayıtlarına HBYS ve ICT Ekip Liderleri'nin izni olmadan kesinlikle hiçbir şekilde erişilemez, ihtiyaç durumunda HBYS ve ICT Veri Tabanı Uzmanları tarafından ancak hastane yönetimi onayı ile loglanan bilgilere ulaşılır.

Bilgi sisteminde veri tabanı sistem logları, gerektiğinde veya acil durumlarda izlenebilmek amacıyla 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"a uygun şekilde saklanır. Loglanan tüm bilgilerin geçmişe dönük olarak takibi yapılabilir.

Kullanıcıların arayüze bağlanmak için kullandıkları parolalar şifreli bir şekilde saklanmaktadır.

Veri tabanının güvenlik açıkları ve ihlalleri ICT Ekibi tarafından tespit edilir ve tespit edilen açıklar, yazılım firmasına iletilerek çözümü sağlanır. Problemlerin çözümünden sonra güvenlik açıklarının ve ihlallerin giderilip giderilmediği ICT Ekip Lideri tarafından yapılan kontrol testleri ile teyit edilir.

HBYS Uygulama ve İşletim Hizmetleri'nde veri tabanı ile ilgili sorumlu kişilerin iletişim bilgileri bulunur. Veri tabanı ile ilgili sorumlu kişilerin iletişim bilgileri **"Veri Tabanı Sorumluları İletişim Bilgi Formu"**nda belirtilmiştir.

Veri tabanı üzerinde iz kaydı alınması gereken işlemler belirlenerek veri tabanında iz kaydı alınan işlemler listesi ile kayıt altına alınmıştır.

Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulur ve sonrasında ilgili uygulama kontrolleri gerçekleştirilir. Kullanıcılar veri tabanına yapılacak müdahale öncesinde, gerekli görülmesi durumunda hastane yönetiminin belirlediği zaman diliminde ile tüm client PC lere bilgi iletilir.

6.6. VARLIK YÖNETİMİ

6.6.1. Bilgisayarlara Yönelik Düzenleme

Bilgi Yönetim Sisteminde kullanılan tüm bilgisayaralar hastane etki alanına dahil edilir. Bilgisayarlarda lisanssız program kullanımına izin verilmez. Tüm bilgisayarlarda merkezi sunucu tarafından kontrol edilebilen antivirüs yazılımları bulunur. Ayrıca tüm bilgisayarlara yönelik güncel envanter oluşturulur. Bilgisayar donanım ve yazılım envanterinde aşağıdaki bilgiler bulunur:

- Bulunduğu bölüm
- Marka
- Model
- Seri no

- Demirbaş numarası
- Donanım ve yazılım adı
- İşletim sistemi
- Ek aksamlar
- Alınma tarihi
- Varsa garanti süresi

Kullanıcı bilgisayarlarındaki virüs yazılımları ve virüs tarama dosyaları ile işletim sistemi ve güvenlik yamalarının güncellenmeleri merkezi bir sunucu vasıtası ile otomatik olarak yapılır.

Bilgi güvenliği amacıyla kablosuz ağ bağlantıları için farklı VLAN bağlantıları oluşturulur. Misafir kullanıcıların bağlandığı kablosuz ağ bağlantıları için farklı vlan oluşturulur.

6.7. İŞ SÜREKLİLİĞİ YÖNETİMİ

6.7.1. Bilgi Yönetim Sistemi Risk Yönetimi

Bilgi Yönetim Sistemine yönelik olarak fiziksel tehlikeler, yazılım ve donanımla ilgili sorunlar, bilgi güvenliği, bilgi mahremiyeti, kullanıcı hataları, kişisel verilerin korunması gibi konularda **"Risk Belirleme, Değerlendirme ve Analiz Formu"** ile 6 ayda bir risk analizi yapılarak riskler tespit edilir. Tespit edilen risklerin ortadan kaldırılması amacıyla iyileştirme çalışmaları yapılır.

Risk değerlendirmesinde asgari aşağıdaki konular yer alır:

- Fiziksel tehlikeler
- Kişisel verilerin korunması
- WEB sitesinin hacklenme durumu
- Yedekleme sırasında sorunlar çıkarsa nasıl geri dönüleceği
- Yazılım ve donanımla ilgili sorunlar
- Bilgi güvenliği ve mahremiyeti
- Kullanıcı hataları
- Veri kaybı
- Alım süresi ve dolum yüzdesi göz önüne alınarak serverların kapasite planlaması
- Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler gibi yedekleme kapasitesi artış gereksinimi
- SBYS'ye giriş yapma imkânı olmadığında kimin, hangi kayıtları, nereye, kaydedeceği ve sonrasına yönelik eylem planının nasıl olacağı ve çalışanların konu hakkındaki bilgilendirilmesi

6.7.2. Bilgi Yönetim Sistemine İlişkin Hata ve İhlal Olayı Bildirimleri

Bilgi yönetim sistemine ilişkin olası yazılımsal ve donanımsal sorunların, ihlal ve hataların nasıl bildirileceği ve hatalara nasıl müdahale edileceği **"Bilgi Sistemleri Hata ve İhlal Raporlama Prosedürü"**nde belirtilmiştir.

Bildirilen hata ve ihlal olayları ile ilgili aşağıdaki bilgiler kayıt altına alınır:

- Hatanın oluştuğu tarih ve saat
- Bildirimin yapıldığı tarih ve saat
- Hatanın içeriği
- Hatanın giderildiği tarih ve saat

Karşılaşılan hatalar, çözüm süreçleri, ne kadar sürede hatanın çözüldüğü gibi bilgiler kayıt altına alınır, benzer hataların gerçekleşmesi durumunda bu kayıtlar izlenebilir. Hatalar giderilinceye kadar işlerin aksamamasına yönelik yapılması gerekenler bölüm bazında belirlenmiştir.

Meydana gelen ihlal olayları ve kesintiye sebep olan tüm arızalar İdare personelleri tarafından MYM üzerinden bildirilir. Alt yüklenici firma personelleri tarafından ise **"Bilgi Sistemleri Hata ve İhlal Raporlama Formu"** ile kayıt altına alınır, HBYS Uygulama ve İşletim Hizmetlerine iletilir ve gerekli düzeltici-önleyici faaliyetler planlanarak iyileştirmeler sağlanır.

Bilgi yönetim sistemdeki arızalar ve devre dışı kaldığı durumlar nedenleriyle birlikte **"HBYS Kesinti Süreleri Kayıt ve Analiz Formu"** ile kayıt altına alınır. Sistemde tespit edilen kesinti ve arızalara yönelik gerekli iyileştirme çalışmaları yapılır.

6.8. YEDEKLEME

Bilgi sisteminde oluşabilecek hatalar karşısında; sistemin kesinti süresini ve olası bilgi kayıplarını en aza indirmek için sistem üzerindeki konfigürasyon, sistem bilgileri ve kurumsal veriler **"Bilgi Sistemleri Yedekleme Prosedürü"**nde belirlenen ilkeler doğrultusunda düzenli olarak yedeklenmektedir.

Yedekleme ile ilgili süreçler, verinin depolanması ve korunmasına yönelik dikkat edilmesi gereken hususlar ve veri kurtarma testi planlarını kapsayacak şekilde tanımlanmıştır.

Veri yedekleme standardı, yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı ne koşullarda ve hangi aşamalarda yedeklerin yükleneceği **"Bilgi Sistemleri Yedekleme Prosedürü"**nde belirtilmiştir. Yedekten geri dönüş testi ve teste ilişkin diğer süreçler **"Bilgi Sistemleri Yedekten Geri Dönüş Prosedürü"** doğrultusunda gerçekleştirilir.

Uygulamalarda herhangi bir değişiklik olması durumunda **"Bilgi Sistemleri Yedekleme Prosedürü"**nün işlerliği ve güncelliği gözden geçirilir.

6.9. BİLGİ TEKNOLOJİLERİ İMHA YÖNETİMİ

HBYS Uygulama ve İşletim Hizmetleri yönetiminde olan cihaz ve ekipmanların arıza vb. durumlar sebebiyle kullanım dışı kalması durumunda ilgili cihaz ve ekipmanlar imha edilmez, garanti kapsamında anlaşmalı firmalara iade edilir ve firmalar tarafından değişimleri yapılır.

Tekirdağ Şehir Hastanesi'nde HBYS Uygulama ve İşletim Hizmetleri bünyesindeki bilgi saklama ortamlarının nasıl yok edileceğini **"Bilgi Saklama Ortamları Yok Etme Prosedürü"**nde belirtilmiştir.

7. İLGİLİ DOKÜMANLAR

7.1. Yıllık Eğitim Planı

7.2. Şifrelendirme Prosedürü

7.3. Personel Gizlilik Sözleşmesi

7.4. Dış Ortamdan İç Ortama Erişim Prosedürü

7.5. Bilgi Sistemleri Yetkilendirme Prosedürü

7.6. HBYS Kısayol Listesi

7.7. Eğitime Katılım Formu

7.8. Sağlıkta Minimum Loglama Standartları (SAMİLOG)

7.9. Yazılım Geliştirme ve Test Versiyonu Uygulama Prosedürü

7.10. Veri Merkezi (Sunucu ve Sistem Odaları) Güvenliği Prosedürü

7.11. Sunucu Özellikleri Bilgi Formu

7.12. Veri Tabanı Güvenliği Prosedürü

7.13. Veri Tabanı Sorumluları İletişim Bilgi Formu

7.14. Risk Belirleme, Değerlendirme ve Analiz Formu

7.15. Bilgi Sistemleri Hata ve İhlal Raporlama Prosedürü

7.16. Bilgi Sistemleri Hata ve İhlal Raporlama Formu

7.17. HBYS Kesinti Süreleri Kayıt ve Analiz Formu

7.18. Bilgi Sistemleri Yedekleme Prosedürü

7.19. Bilgi Sistemleri Yedekten Geri Dönüş Prosedürü

7.20. Bilgi Saklama Ortamları Yok Etme Prosedürü