



T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	1 / 10

**1.AMAÇ:** Kurumumuzda bilgi yönetim sisteminin detaylarının belirlenmesi ve bilgi güvenliğinin sağlanması amacıyla uygulanan işlemlerin politikasını ve şeklini belirlemek. Hasta ve çalışanlara ait tıbbi ve kişisel bilgilerin, doğru ve güvenli şekilde kayıt altına alınması ve depolanması ile ihtiyaç duyulan doğru bilgilerin, bilgi mahremiyeti ve güvenliği gözetilerek, doğru zamanda, doğru kişiye ulaştırılmasını sağlamaktır.

**2. KAPSAM:** Bu doküman kurumumuz bilgi yönetimi işlemleri, genel HBYS kullanım ve erişim kuralları ve bilgi güvenliği konularını kapsar.

**3. KISALTMALAR:** HBYS: Hastane bilgi yönetim sistemi UPS: Kesintisiz Güç Kaynağı ÇKYS: Çekirdek Kaynak Yönetimi Sistemi

**4. TANIMLAR:** Bilgi Güvenliği: Bilginin hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, 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 v.b.) gerçekleştirmesine, kaydetmesine ve muhafaza etmesine yarayan elektronik yazılımlar grubu. Otomasyon Sistemi: Hastane Bilgi Yönetim Sistemi Otomasyon: Girdilerin bilgisayara girilmesi ile işlemlerin bilgisayar tarafından otomatik olarak yürütülmesi.

### 5. SORUMLULAR:

- Başhekim,
- İdari İşler Müdürü,
- Bilgi İşlem Sorumlusu,
- Muhasebe Müdürü ,
- Personel,
- Bilgi İşlem Personeli,
- Hasta Kayıt -Kabul Sekreterleri (klinik sekreterleri, poliklinik sekreterleri, hasta kayıt ve danışma sekreterleri, yönetici sekreterleri),
- Tüm hastane işletim sistemindeki (H.B.Y.S) yetkilendirilmiş kullanıcıları

### 6. FAALİYET AKIŞ

#### 16.1 BİLGİ İŞLEM BİRİMİ

Kurumumuzda bilgi yönetiminden sorumlu Bilgi Güvenliği, Yazılım ve Donanım Teknik Destek ekibi mevcuttur. Ekip, Bilgi İşlemden Sorumlu Başhekime bağlı çalışmaktadır. Yazılım ve Donanım Destek Ekibi ve HBYS yazılımının desteğini sağlayan firma yetkilileri de Bilgi Güvenliği ve Teknik Destek Ekibi'nde görev almaktadırlar ve 7/24 kesintisiz hizmet sunmaktadır. Gerek duyulması durumunda ekipteki firma yetkilileri aranarak yaşanan soruna müdahale etmeleri sağlanmaktadır. T.C. Sağlık Bakanlığı Yozgat İl Sağlık Müdürlüğü'nde bulunan tüm bilgisayarlar üzerinde Yazılım-

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	2 / 10

donanım Destek Birimi çalışanlarının irtibat bilgileri yer almaktadır. Birim çalışanları 24 saat destek vermektedir.

Kurumumuzda kullanılan Hastane Bilgi Yönetim Sistemi'nde (HBYS) tüm birimlerimiz için tek bir veri tabanı üzerinde bulunmaktadır. Hasta Kayıt, Hasta Yatış, Poliklinik, Klinik, Eczane, Depo, Ayniyat, Laboratuvar, Vezne, Faturalandırma, Arşiv, Cihaz Takip, Sağlık Çalışan Takip, Radyoloji, Satın Alma, Personel modülü başta olmak üzere HBYS' de mevcut tüm modüllerin aktif olarak kullanılması sağlanmaktadır. Gerektiğinde personele HBYS kullanımı ile ilgili eğitimler düzenlenmelidir. Ayrıca bölümlerin malzeme ve demirbaş istemlerinin; yapılması, onaylanması, satın alınması, depoya teslim edilmesi, bölümler tarafından teslim alınması da HBYS üzerinden gerçekleşmelidir.

### 6.2 BİLGİ YÖNETİMİNE İLİŞKİN FAALİYETLERİN YÜRÜTÜLMESİ VE KOORDİNASYONUNA YÖNELİK SORUMLULAR VE SORUMLULUKLAR

**6.2.1 Hastane Bilgi Yönetimi Sistemini kullanan tüm çalışanlar:** HBYS sistemini kullanan tüm çalışanlar hastanedeki mevcut tüm bilgisayarlardan kendilerine verilmiş ve görevleri ile yetkilendirilmiş kullanıcı kodu ve şifresi ile yaptığı tüm işlemlerden sorumludur.(Veri girişi,değiştirmesi,silmesi vb.)

**6.2.2 Tüm Bilgi İşlem Personeli:**Bilgi işlem merkezinde görevli personelle hastanede çalışan tüm personellere otomasyon ile ilgili destek vermek. Hastane birimlerinde çalışan tüm personellerin yazılım üzerinde oluşabilecek yenileme,düzeltilme gibi işlemleri tespit edip firmadan talep etmek. Gün içerisinde hastalara ait sevklerin, bilgi eksikliği(tanı,işlem)gibi tespit edip mesai bitiminde kontrol oluşturup aksaklıkları düzeltmek.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 vermekten sorumludur.

#### 6.2.3 Bilgi İşlem Sorumlusu:

Hastaneye 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.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	3 / 10

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

Hastaneye ait elektronik postasına gelen bilgi ve talepleri ilgili birimlere iletmek.

Bilgisayar donanımlarında meydana gelen aksaklıkların giderilmesi için amirine bilgi vermek. Konusuyla ilgili olarak amiri tarafından verilen diğer işleri yerine getirmek sorumlulukları arasında yer almaktadır.

### 6.3 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. **Bilgi Yönetim sistemleri Personel Ekleme ve Yetkilendirme Formu** üzerinde Hastanemizde bulunan kullanıcı grupları tanımlanmıştır.

#### Bu rol grupları;

Doktor  
Poliklinik danışmanı  
Servis Hemşiresi  
Servis danışmanı  
Laboratuvar personeli  
Radyoloji personeli  
Satın alma  
Personel  
Kalite  
İstatistik  
Faturalama vb.

Çalışanların yetkileri düzenlenmiştir ve kayıt altına alınmaktadır. Aynı görevde çalışan personellerin yetkileri de aynıdır.İşe yeni başlayan personel İnsan Kaynakları Birimi tarafından **Bilgi Yönetim Sistemleri Personel Ekleme ve Yetkilendirme Formu ile Bilgi İşlem Birimine yönlendirilerek** birim yöneticisinin onayı ile kullanıcı adı ve şifresi verilir. İşten ayrılırken ise İlişik Kesme Formu ile bilgi işleme başvurarak ilişik kesilir.

### 6.4 DİSİPLİNLER ARASI YETKİLENDİRME AŞAĞIDAKİ GİBİDİR:

**Hastane Yöneticisi:** Hastanedeki tüm bilgilere ulaşır.

**Başhekim:** Hastanedeki tüm bilgilere ulaşır.

**İdari İşler Müdürü:** İdari, mali ve teknik işlemlerle ilgili tüm bilgilere erişebilir.

**Doktor:** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Elektronik ortamda kayıtlı olması gereken hastaya ait tüm bilgileri girebilir. Onay işlemlerini kendi şifreleri ile yapmakla

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	4 / 10

yükümlüdürler. Onaylanmadan önce kendilerine ait raporlar üzerinde silme ve değişiklik yapabilir. Raporlar onaylandıktan sonra değiştirilemez. Otomasyon üzerinden e-reçete yazar.

**Hemşire:** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Silme ve değiştirme yetkileri yoktur. Kendi işlerine ait laboratuvar ve pre op. –post op. hasta bilgilerini, hastaya ait ilaç, sarf ve tetkik girişlerini yetkileri dahilinde yapabilirler.

**Personel Birimi:** Personel özlük bilgilerine ulaşabilir, mesai, izin, rapor gibi işlemlerini otomasyon üzerinden gerçekleştirir.

**Faturalama Birimi:** Ay içerisinde başvuran tüm hastaların faturalamasını ve sosyal güvenlik kurumlarına elektronik ortamda ya da posta yoluyla teslimatını yapar. Faturalamadan sorumlu Başhekim ve Muhasebe Müdürü kurumlara yapılan faturaların tutarlarını ve yapılan işlemleri görebilir, inceleyebilir.

**Eczane:** Servislerden gelen eczaneye ilgili taleplerin girişlerini yapar, otomasyon üzerinden girişlerin ve ilaçların karşılamasını yapar. Hastaların reçeteleri doğrultusunda ilaçların takibini sağlar, stokları kontrol eder, Fatura girişi, Malzeme girişi yapabilir.

**Radyoloji:** Hastaların radyolojik işlemlerini yapar. Tetkik işlemlerinin sonuç raporlarını otomasyon üzerinden yazar, Kullanılan ilaçların düşümünü yapabilir.

**Laboratuvar:** Doktorların hastaları için yaptığı istemleri karşılar, 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 sonuçları görülebilir. Hastalar muayene oldukları poliklinikten veya hastane web sayfası üzerinden sonuçları alabilirler.

**Poliklinik Sekreterleri:** Muayene başlatma ve muayene bitirme işlemlerini yapar. Doktorun istediği istemleri otomasyon üzerinden yapar. Yatış öncesi işlemleri gerçekleştirir.

**Hasta Kayıt-Kabul Sekreterleri:** Hastaların gelişte otomasyon programına kayıtlarını yapar. Hastalardan gerekli evrakları alır, takip alınacak hastalara otomasyon üzerinden provizyon alır.

**Klinik Sekreterleri:** Doktorun istemlerini ve sarfları hastanın dosyasına ekler. Hatalı yaptığı işlemleri sorumlularına bildirirler. Sorumluların düzeltemediği işlemleri Bilgi İşlem birimine bildirilir. Hasta yatış -çıkış işlemleri için gerekli evrakları düzenler. Hasta taburcu işlemlerini yapar. Her kademedeki çalışan sadece yetkilendirilmiş olduğu işlemleri yürütebilmektedir.

•Yetkilendirilmemiş kişiler 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.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	5 / 10

•HBYS şifreleri kullanıcılara ilk kez Bilgi İşlem Birimi 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 kullanıcıya 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 İşlem çalışanları yetkilendirmektedir.
- Yazılım kurma, güncelleme ve silme işlemleri
- Otomasyon sistemi işlemleri
- Bilgi İşlem Birimi Sorumlusuna açık hastane bilgi sistemi işlemleri
- Donanım desteği verme işlemleri
- Sorunların çözümü

### **6.5. BİLGİ YÖNETİM SİSTEMİ İLİŞKİN RİSKLER:**

Bilgi Yönetim İlişkin risk analiz "Risk Analizi Bölümü" başlığı altında yapılmaktadır. Risk Analizi doğrultusunda tespit edilen risklere yönelik iyileştirme çalışmaları yapılmaktadır. Kurumun bilgi sistemlerine bağlı tüm cihaz, yazılım, veritabanı gibi konularda sistem sorunlarını tespit etmek ve gerekli tedbirlerin alınmasını sağlamak amacıyla bilgi yönetimi ekibi tarafından risk analizi yapılır. Risk analizi kurum içerisinde bilgi güvenliği, bilgi mahremiyeti, kullanıcı hataları yazılım, donanım gibi konuları kapsar.

Bilgi yönetimi sistemi en uygun hale getirmeyi amaçlayan kararları sistemin gelişmesi için uygulama kararı alır. Alınan kararlar ilgili firmalara bildirilir. İlgili uygulamanın çalıştırılması, geliştirilmesi ve uygulanması Kurum ve ilgili firmanın sorumluluğunda değerlendirilir. Risk analizi süresince çalışanlar gerekli noktalarda yardımcı olacaklardır. Çalışanlar daha sonra Risk Değerlendirme takımı ile birlikte geliştirme ve iyileştirme sürecine katkıda bulunacaklardır.

Risk değerlendirme raporları Kuruma elden teslim edilecek ve rapor, söz konusu risk ve hassasiyetler giderilene kadar Bilgi İşlem Biriminde çevresel ve fiziksel güvenlik önlemleri alınmış bir ortamda saklanacaktır. Risk değerlendirme çalışmaları sırasında sistemler üzerinde servis reddi veya herhangi bir sebeple iş sürekliliği en aza indirilecek şekilde aksatılmadan devam etmesini sağlamak.

### **6.6. BİLGİ YÖNETİM SİSTEMİ İLİŞKİN HATA BİLDİRİMLERİ**

Bilgi Yönetimi kapsamında karşılaşılan sorunlarda hastane iç hat telefon numarası, Kısa kod ile cep telefonu ve HBYS üzerinden arıza bildirimini ile Bilgi İşlem birimi çalışanlarıyla irtibat kurulur. Bilgi İşlem

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	6 / 10

personeli arasında modül ve birim bazında iş bölümü oluşturulmuştur. İlgili bölümlerde oluşan sorunlar hemen çözülmeye çalışılır, işlerin aksamamasına çalışılır. İlgili sorun çözüldüğünde çözen bilgi işlem personeli tarafından otomasyona tamiri bitti işaretlenerek açılan arıza bildirimini kapatılır. Süreçlerle ilgili yapılan hata kayıtları; HBYS üzerinde sorunun tarih ve saati, bildirim yapıldığı tarih ve saati kayıt altına alınmaktadır.

### 6.7 BİLGİ GÜVENLİĞİ MAHREMİYETİ

Bilgi güvenliği mahremiyeti Bilgi Güvenliği Politikası doğrultusunda gerekli tedbirler alınmaktadır. Bilgi güvenliği konusunda çalışanlara yıllık eğitim planı dâhilinde farkındalık eğitimleri verilmektedir. Verilen eğitimler kayıt altına alınmaktadır.

### 6.7 Şifre Kullanımı

#### 6.7.1 Genel

Bütün sistem seviyeli şifreler (örnek, root, administrator, vs.) en az on beş günde bir değiştirilmelidir. Bütün kullanıcı seviyeli şifreler (örnek, masaüstü bilgisayar vs.) on beş günde bir değiştirilmelidir. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir. Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir. Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılmayacak güçlü bir şifreye sahip olmalıdır. Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır. Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır.\*\*Bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki ana noktalara uymalıdır.

#### 6.7.2 Ana Noktalar

**Genel Şifre Oluşturma Kuralları** Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs. Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen gösterilmelidir.

**Zayıf şifreler aşağıda belirtilen karakteristiklere sahiptir.**Şifreler altıdan daha az karaktere sahiptirler. Aaabbb, qwerty, zyxwuts, 123321, vs. gibi sıralı harf veya rakamlar. Yukarıdaki herhangi bir kelimenin geri yazılış şekli. Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek, gizli1, gizli2).

**Güçlü şifreler aşağıdaki karakteristiklere sahiptir.**

Küçük ve büyük karakterlere sahiptir.(örnek, a-z, A-Z)Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir.(0-9, !@#\$%A&\*()\_+|=VÖ[]:”;<?>,/)En az altı adet alfa nümerik karaktere sahiptir. Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır. Aile isimleri gibi kişisel bilgilere ait olmamalıdır. Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü





T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	7 / 10

tutulmamalıdır. Kolayca hatırlanabilen şifreler oluşturulmalıdır. Örnek olarak;” olmaya devlet cihazında bir nefes sıhhat gibi” cümlesi “OdC1nSg!” veya türevleri şeklinde olabilir.

Son üç ay içerisinde kullanılmış şifrelerin tekrar kullanımının engellenmesi sağlanır.

**Not:** Yukarıdaki herhangi bir örneği şifre olarak kullanmayınız.

### 6.7.3 Şifre Koruma Standartları

Kurum bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanmayınız. (örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde). Değişik sistemler için farklı şifreleme kullanın,(örnek, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanınız). Kurum bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler kuruma ait gizli bilgiler olarak düşünülmelidir. Aşağıdakiler yapılmayacakların listesidir;

Herhangi bir kişiye telefonda kalıcı/gerçek şifre verilmez.

E-posta mesajlarında şifre belirtmek

Üst yöneticinize şifreleri söylemek.

Başkaları önünde şifreler hakkında konuşmak.

Aile isimlerini şifre olarak kullanmak.

Herhangi form üzerinde şifre belirtmek.

Şifreleri aile bireyleri ile paylaşmak.

Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmemek.

Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem Birimi yetkilisini aramasını söyleyiniz.

Uygulamalardaki “şifre hatırlatma” özelliklerini seçmeyiniz, (örnek, Outlook, Internet Explorer vs.)

Şifreler en az 3 ayda bir değiştirilmelidir.

**6.8. HBYS kullanıcı dostu olarak;** HBYS veri girişi doğrulama kontrolleri, tarih ve kısa yol kontrolleri yazılımsal olarak yapılmaktadır.

**6.9.**Bilgi yönetim sistemi etkin kullanabilmesi için tüm çalışanlar yıllık eğitim planı doğrultusunda eğitimler verilmektedir. Verilen eğitimler kayıt altına alınmaktadır. Bilgi sistemlerine yönelik yapılan güncellenmeler hakkında sistem üzerinde mesajlama yolu ile bilgilendirme yapılmaktadır. Bilgi yönetim sistemi kullanıcılara işe başlamasında tüm personele “Personel Gizlilik Sözleşmesi” imzalanmaktadır.

### 6.10 HASTANE BİLGİ YÖNETİM SİSTEMİNDE YER ALAN MODÜLLER

HBYS üzerinde aşağıdaki modüller aktif olarak kullanılmaktadır.

- ✓ Hasta Kayıt
- ✓ Hasta Yatışı
- ✓ Poliklinik

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	8 / 10

- ✓ Klinik
- ✓ Eczane
- ✓ Depo
- ✓ Satın alma
- ✓ Ayniyat
- ✓ Laboratuvar
- ✓ Vezne
- ✓ Faturalandırma
- ✓ Radyoloji
- ✓ Personel modülü

Malzeme ve cihaz istemlerinin yapılması, bölümlerde kullanılması ve tüm süreçlere ilişkin işlemler HBYS üzerinden gerçekleştirilmektedir. HBYS üzerinde, modüllerin kullanımına ilişkin yardım bilgileri bulunmaktadır.

### Personel modülünde;

- ✓ Çalışana ait fotoğraf
- ✓ Çalıştığı bölüm
- ✓ Kan grubu
- ✓ İletişim bilgileri
- ✓ İzin ve rapor bilgileri
- ✓ Eğitim durumu
- ✓ Sertifikaları
- ✓ Hizmet içi eğitimleri
- ✓ Yabancı dil bilgisi bilgileri yer almaktadır.

### 6.11 HBYS ÜZERİNDE YAPILAN İŞLEMLERİN İZLENMESİ

Düzeltilme ve iptal kayıtları, toplanan tüm tıbbi bilgilerin geçmişe yönelik takibi sistem üzerinde yapılmaktadır. Sistem üzerinde yapılan takiplerde; Salt okunur özellikte ayrı bir veritabanı, sisteme giriş yapan kullanıcılar, gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalar log izlemi yazılım tarafından kayıt altına alınmaktadır. Veri tabanına sadece bilgi sisteminde yönetici olarak yetkilendirilmiş Bilgi İşlem personeli ulaşmaktadır.

### 6.12 HBYS ÜZERİNDE VERİLERİN YEDEKLENMESİ

Yedekleme ilk olarak HYBS nin kendi içerisine alınıp daha sonra farklı bir sunucuya aktarılmakta ayrıca offline ortama USB HDD' e sıkıştırılmaktadır. Yedekleme günlük olarak üç defa yapılmaktadır. Arşivlemesi günlük olarak yapılmaktadır. Veriler yedekleme yapıldıktan sonra offline ortamda (harici disk) saklanmaktadır. Ayrıca farklı iki yerde daha saklanmaktadır.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü





T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	9 / 10

Her yıl sonunda alınan yedekler offline ortama USB HDD' e sıkıştırılıp hastane dışında iki farklı ortamda yönetim tarafından saklanmaktadır. Yedeklemeler aracılığı ile yılda bir kez veri kurtarma testi yapılmaktadır. Yapılan veri kurtarma işlemi veri kurtarma test formu ile ve görsel kayıt şeklinde altına alınmaktadır.

**6.13 BİLGİ YÖNETİM SİSTEMİNDE KULLANILAN TÜM BİLGİSAYARLARA YÖNELİK DÜZENLEME**  
Kurumumuzda kullanılan tüm donanım ve yazılımlarının güncel envanteri Bilgisayar Donanım ve Envanter Listesi ile kayıt altına alınmaktadır. Hazırlanan Listede; bulunduğu bölüm, marka, model, seri no, demirbaş numarası, donanım ve yazılım adı, işletim sistemi, ek aksesuarlar, alınma tarihi, varsa garanti süreleri bulunmaktadır. Bu dokümanın düzenlenmesi ve güncelliğinin sağlanmasından Bilgi İşlem Sorumlusu sorumludur. Tüm bilgisayarlarımızda merkezi sunucu tarafından kontrol edilebilen güncel antivirüs programı yüklenmiştir. Kablosuz erişim bulunmaktadır. Güvenlik nedeniyle Firewall'dan ayrı bir çıkış verilmiş ve farklı bir ip blogundan çıkış atanmıştır ayrıca bağlanılan wifi cihazlarında belirli sayıda ip blogu tanıtılmış ve yatak sayısı kadar giriş izni verilmiştir. Wifi internet erişim hizmetinden sadece yatan hasta ve yakınları faydalanabilmektedir, kullanıcı adı ve şifre bulunduğu kattaki kat danışmanları tarafından TC kimlik numarasına göre şifre verilmekte ve sadece 24 saat izin verilmektedir.

### 6.14. BİLGİ YÖNETİM SİSTEMİ TEKNİK DESTEK VE ALT YAPISI

Hastanemizde bilgi yönetimi yazılım ve donanım teknik destek Bilgi İşlem Birimi tarafından sağlanmaktadır. Bilgi İşlem Birimi İletişim Bilgileri tüm kullanıcılarla paylaşılmıştır. Bilgi İşlem Birimi 24 saat kesintisiz hizmet vermektedir. HBYS devre dışı kaldığı durumlarda Gösterge Kartı ile kayıt altına alınmaktadır.

### 6.15 SUNUCULARIN GÜVENLİĞİ

☑Sunuculara tahsis edilmiş bir bağımsız oda bulunmaktadır.

☑Oda Şifreli kilit sistemi ile kilit altında ve şifreler sadece bilgi işlem personelinin bilgisindedir. Görevli harici personelin server odasına (sistem odası) girişi yasaktır.(asıl anahtar kartı hastanemiz kasasında saklanmaktadır, yedek anahtar kartı İdari İşler Müdüründe muhafaza edilmektedir.)

☑Oda hastanenin 3 katında bulunmaktadır. Oda içinde su tesisatı bulunmamaktadır.

☑Sunucu Odalarında elektrik kesilmesi durumunda tesisat katımızda bulunan Hastaneden bağımsız 2 adet yedekli UPS bulunmaktadır arıza durumunda devreye girmektedir. İki UPS arıza durumunda ise gelen hattın bir ucu Hastane genelinde bulunan UPS e bağlıdır.

☑İsı ve nem takibi otomasyondan yapılmaktadır.(Sıcaklık 18-22 °C, Nem %30-%50 arasında Bulunmaktadır).Arıza ve ısı değişimleri otomatik olarak tarafımıza arıza sms olarak bildirilmektedir(Teknik Servis, Bilgi İşlem ).

☑İkinci klima yedek olarak bulunmaktadır.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

## BİLGİ YÖNETİM SİSTEMİ VE GÜVENLİĞİ PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	10 / 10

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

☑Sunucuların yazılım ve donanım bakımları bilgi işlem tarafından yapılmaktadır gerek görüldüğünde ilgili firma ile görüşüp gerekli bakım desteği alınmaktadır.

☑Sunucularımız ve sisteme bağlı olan tüm cihazlar güvenlik duvarının arkasında bulunmaktadır.

### 6.16 VERİ TABANI GÜVENLİĞİ

Veritabanı sistem logları tutulmakta ve gerektiğinde hastane yönetimi tarafından izlenmektedir. Veritabanı ya da tablolarla sisteme giriş yapan kullanıcılar, gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalar log izleme yazılımı tarafından kayıt altına alınmaktadır. Ayrıca Bilgi İşlem Server Odası Arıza Bildirim Formu'nda kayıt edilmektedir. Veritabanı ile ilgili sorumlu kişilerin iletişim bilgileri güncel olarak Yazılım-Donanım Destek Birimi İletişim Bilgileri formunda bulunmaktadır. Kullanıcıların arayüze bağlanmak için kullandıkları şifreler şifreli bir şekilde veri tabanında saklanmaktadır. Kullanıcılar veritabanına yapılacak müdahale öncesinde mesaj olarak HYBS üzerinden bilgilendirilmektedir

### 6.17. DIŞ ORTAMDA İÇ ORTAMA ERİŞİM

Hastaneye destek veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında hastane tarafından onaylanmış gizlilik sözleşmesi bulunmaktadır. Dış ortamdan iç orta yapılan kayıtlar kayıt altına alınmaktadır. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

### 7. İLGİLİ DOKÜMANLAR

Bilgi Güvenliği Politikası

Bilgi Yönetim sistemleri Personel Ekleme ve Yetkilendirme Formu

Personel Gizlilik Sözleşmesi

Uzaktan Erişim Taahhütnamesi

Uzakta Erişim Formu

Isı ve Nem takip formu

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü