T.C.

SAĞLIK BAKANLIĞI

TURHAL DEVLET HASTANESİ

BİLGİ GÜVENLİĞİ POLİTİKASI
01/03/2018

İçindekiler

1. AMAÇ

Turhal Devlet Hastanesi'nin bilgi güvenliğini yönetmekteki amacı; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden ve/veya dışarıdan gelebilecek, kasıtlı veya kasıtsız oluşabilecek tüm tehditlerden korunması ve yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesini temin etmektir. Bilgi Güvenliği Politikasının hazırlanmasındaki amaç ise, Turhal Devlet Hastanesi'nin sahip olduğu tüm bilgi varlıklarının korunması ve uygun biçimde yönetilmesinin sağlanmasıdır. Aynı zamanda tüm ilgili taraflara Turhal Devlet Hastanesi bilgi güvenliği gereksinimlerinin bildirilmesi ve yazılı kuralların temel dayanağının oluşturulmasıdır.

2. HEDEF

Bilgi Güvenliği Politika şartlarını yerine getirerek, çalışanların bilgi güvenliği farkındalığını arttırmak, teknik güvenlik kontrollerini uygulamak ve kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak (iş sürekliliği), kurumsal riskleri en alt seviyeye indirerek kurumun güvenliği ile güvenilirliğini ve temsil ettiği kurumun imajını korumaktır.

3. KAPSAM

Bu politika Turhal Devlet Hastanesini kapsar. Turhal Devlet Hastanesi Bilgi Güvenliği Politikası aşağıdaki varlık ve teknoloji kategorilerini kapsamaktadır:

1.1.Veri dosyaları, sözleşmeler ve benzeri tüm bilgi varlıkları,
1.2.Uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları,
1.3. Yönlendirici cihazları, güvenlik cihazları, sistem yönetim sunucuları, yasal yükümlülükler kapsamında kurulmuş sunucu sistemleri, uydu sistemleri, bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıklar,
1.4.Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,
1.5.Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları

varlıkları,
1.6.Kurum tarafından üretilen, kullanılan ve/ve ya geliştirilen tüm verileri kapsar.

4. TANIMLAR

Bu politika ve esaslarında geçen,

Bilgi Güvenliği : Turhal Devlet Hastanesi bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunması.

Varlık : Turhal Devlet Hastanesi iş süreçleri için değeri olan, kaybı halinde işlerin aksayacağı, insan, yazılım, donanım,itibar, bilgi gibi unsurların tümüdür.

Gizlilik : Bilginin sadece yetkili kişiler tarafından erişilebilir olması.

Bütünlük : Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması.

Erişilebilirlik : Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an erişilebilir olması.

Turhal Devlet Hastanesi bünyesinde, bu politika metninde madde 4 de tarif edilen kapsam dahilinde Bilgi Güvenliği Faaliyetlerini yürütmek amacıyla Bilgi Güvenliği Komisyonu kurulmuştur.

BİLGİ GÜVENLİĞİ YÖNETİMİ EKİBİ	
Tıbbi Yönetici Temsilcisi Dr. Cahit Şemsi SAY	Başhekim Yrd.
İdari Yönetici Temsilcisi Ömer TOK	İdari Ve Mali Hizmetler Müdürü
Bilgi Güvenliği Yetkilisi Abdulvahap DOĞAN	Müdür Yardımcısı
Kalite Yönetim Direktörü Kevser KESKİNEROĞLU	Kalite Yönetim Direktörü
Hastane Bilgi Yön. Sist. Sor. Gökay KOÇAK	Bilgi İşlem Birim Sorumlusu

Bilgi Güvenliği Ekibi Görev, Yetki ve Sorumlulukları

1. Ekip hastanenin büyüklüğü ve hizmetlerin çeşitliliği dikkate alınarak hastanede yapılan çalışmaların etkililiğini, sürekliliğini ve sistematikliğini sağlayacak şekilde faaliyet yürütür.
2. Hastane üst yönetiminden bir kişi ekibe başkanlık eder.
3. Bilgi güvenliği ile ilgili mevcut durumu tespit eder,
4. Bilgi güvenliği için olası riskleri belirler,
5. Tanımlı kullanıcılar için yapılan yetki değişikliklerini izler.
6. Gerektiğinde düzeltici önleyici faaliyetleri başlatır.

5. ESASLAR

5.1.İş süreçlerinin gereksinimi olarak her türlü bilgi en az kesintiyle; hizmet alanlar, hizmet verenler ve yetkilendirilmiş üçüncü taraflarca erişilebilir olacaktır.

5.2.Bilgilerin gizliliği, bütünlüğü ve erişilebilirliğinin sürekli olarak sağlanması için azami derecede çalışmalar yapılacaktır.

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

5.4.Sadece kendine erişim yetkisi verilmiş bilgilere, yetkisi dâhilinde erişilecek; bilgi yetkisiz erişime karşı korunacaktır.

5.5.Kişisel ve elektronik iletişimde ve dış taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin güvenliğini sağlanacaktır,

5.6.Kritiklik düzeylerine göre işlenen bilgi yedeklenecektir,

5.7.Bilgilerin etkileşimde bulunduğu varlıklar ile ilgili açıklıklar, bu açıklıklara yönelik tehditler ve bu tehditlerin gerçekleşme olasılığı ile gerçekleşmesi sonucunda oluşacak zararların önlenmesi veya en aza (kabul edilebilir düzeye) indirilmesi için yapılacaklar planlanacaktır.

5.8.Türkiye Cumhuriyeti yasaları, yönetmelikler, genelgeler ve sözleşmeler ile belirlenmiş gereksinimler karşılanacaktır.

5.9.Personelin bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını teşvik edecek eğitimler düzenli olarak kurum çalışanlarına ve yeni işe giren çalışanlara sağlanacaktır.

5.10.Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilecek; ihlallere sebep olan uygunsuzluklar tespit edilecek, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınacaktır.

5.11.Turhal Devlet Hastanesi çalışanları kullandıkları tüm bilgi sistemlerinde "Parola Kullanma Politikası"na uygun hareket edeceklerdir.

5.12. Turhal Devlet Hastanesi çalışanları kurum ağ ve internet sistemlerini kullanırken "İnternet ve Ağ Kullanım Politikası"na uygun hareket edeceklerdir.

5.13.Tüm birim yöneticileri bu esasların uygulanmasından birinci derecede sorumlu olacaklar ve personelinin esaslara uygun olarak çalışmasını sağlayacaktır.

6. ROLLER VE SORUMLULUKLAR

Bilgi Güvenliği Politikası kapsamındaki temel rol ve sorumluluklar aşağıda tanımlanmıştır:

6.1.Kapsam dâhilindeki tüm Kurum personeli, paydaş ve üçüncü taraflar Bilgi Güvenliği Politikasına uymak zorundadır.

6.2.Kapsam dâhilindeki tüm personel güvenlik olaylarını, fark edilen güvenlik açıklıklarını ve güvenlik kuralları ihlallerini en kısa sürede Bilgi Güvenliği Sorumlularına raporlamaktan sorumludur.

6.3.Bilgi Güvenliğinin yönetiminden Bilgi Güvenliği Sorumluları, devamlılığının sağlanmasından ve gözden geçirilmesinden Kurum Yönetimi sorumludur.

6.4.Bilgi Güvenliği Sorumluları bilgi güvenliği politikasının uygulanmasını sağlamakla ve gözden geçirmekle sorumludur.

6.5.Kurum Yönetimi çeşitli kurallar ve süreçler ile bu politikanın uygulanmasını desteklemekle sorumludur.

6.6.Bilgi varlıklarının gizlilik, bütünlük, erişilebilirliğinin korunmasından varlık sahipleri sorumludur.

6.7.Tüm çalışanların bilgi güvenliği bilincini arttırmak için belirli aralıklarla farkındalık eğitimlerinin verilmesi Bilgi Güvenliği Sorumlularının sorumluluğundadır.

7. İNSAN KAYNAKLARI ZAFİYETİ YÖNETİMİ

7.1.Kurum Personeline ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
7.2.İmha edilmesi gereken müsvedde halini almış ya da iptal edilmiş yazılar vb. kâğıt kesme makinesinde imha edilmelidir.
7.3.ÇKYS Sisteminde kişiyle ilgili bir işlem yapıldığında ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
7.4.Tüm personelin kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
7.5.Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
7.6.Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye teslim edilmelidir.
7.7.Güvenlik zafiyetlerine karşı son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır.
7.8.Son kullanıcılar güvenlik zafiyetlerine neden olmamak için bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.
7.9.Son kullanıcılar bilgisayarlarında veya sorumlusu oldukları sistemler üzerinde USB flash bellek ve/veya harici hard disk vb. bırakmamalıdır.
7.10.Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.

7.11.Kurum, mevcut envanteri haricindeki donanımların kurum bilgisayarlarında kullanımını engellemelidir.
7.12.Son kullanıcılar mesai bitiminde bilgisayarlarını kapatmalıdır.

8. İŞE BAŞLAYIŞ VE İŞTEN AYRILMA PROSEDÜRÜ

8.1.İşe Başlayış Prosedürü

• İşe başlayan her personele (kadrolu ve hizmet alımı dâhil) bilgi güvenliği ve sosyal mühendislik zafiyetleri konularında eğitim verilmelidir.
• Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Her çalışan personel Gizlilik Sözleşmesini (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzalamakla yükümlüdür.
• Var ise kullanacağı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri tanımlanmalıdır.
• EBYS üzerinden yazışma yapabilmesi ve ya yazışmaları takip edebilmesi için ilgili personele saglik.gov.tr uzantılı e-mail adresi tanımlanmalıdır. İl içi yer değişikliklerinde ise sistem üzerinden kurum/birim değişikliği tanımlaması yapılmalıdır.
• Tüm personele kurum kimlik kartı çıkartılmalıdır.

8.2.İşten Ayrılış Prosedürü

• Görevden ayrılan personelin kurum kimlik kartı ve yaka kartı alınmalıdır.
• Kullandığı bilgi sistemlerine yönelik (ÇKYS/TSIM, EBYS vb.) kullanıcı adı ve şifreleri ilgili sistem yöneticileri tarafından iptal edilmeli ya da pasif hale getirilmelidir.
•Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
• Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.

9. MAL VE HİZMET ALIMI GÜVENLİĞİ

9.1.Kurum olarak mal ve hizmet alımlarında ilgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak rekabeti engellemeyecek şekilde gerekli güvenlik düzenlemeleri Teknik şartnamelerde belirtilmelidir.

9.2.Dış kaynak kullanımı ve üçüncü taraf hizmet sunumunun diğer formları arasındaki farklılıkların bazıları; Sorumluluk, geçiş durumu planlama ve işlemler süresince potansiyel kesinti süresi, acil durum planlaması yönetmelikleri ve durum tespitinin gözden geçirilmesi, güvenlik olayları hakkında bilgi toplanması ve yönetimi konularında sorular içerecektir. Bu nedenle, dış kaynaklı bir yönetmelik geçişinde; kuruluş değişiklikleri yönetmek için uygun süreçlere ve anlaşmaların yeniden müzakere edilmesi ya da fesih edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.

9.3.Üçüncü taraflarla yapılan anlaşmalar diğer tarafları içerebilir. Üçüncü taraflara erişim hakkı verilmeden önce, erişim hakkı ve katılım için diğer tarafların ve koşulların belirlenmesi amacıyla anlaşmaya varılması gerekir.

10. BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ

10.1.Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı 'na uygun olarak muhafaza edilmesi gerekmektedir.
10.2.Yasal bekleme süreleri sonunda tasfiyeleri sağlanmalıdır. Burada Özel ve Çok Gizli evraklar "Devlet Arşiv Hizmetleri Yönetmeliği" hükümleri gereği oluşturulan "Evrak İmha Komisyonu" ile karar altına alınmalı ve imha edilecek evraklar kırpma veya yakılarak imhaları yapılmalıdır. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.
10.3.Bilgi Teknolojilerinin (Disk Storage Veri tabanı dataları vb.) 14 Mart 2005 Tarihli 25755 sayılı Resmi Gazete 'de yayınlanmış, sonraki yıllarda da çeşitli değişikliklere uğramış katı atıkların kontrolü yönetmeliğine ve Basel Sözleşmesine göre donanımların imha yönetimi gerçekleşmelidir. Komisyonca koşullar sağlanarak donanımlar parçalanıp, yakılıp (Özel kimyasal maddelerle) imha edilmelidir.
10.4.İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
10.5.Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.
10.6. Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
10.7.Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
10.8.Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.
10.9.Hacimsel küçültme işlemi için parçalanmalıdır.
10.10. Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

11. SOSYAL MÜHENDİSLİK ZAFİYETLERİ

İnsanların zafiyetlerinden faydalanarak çeşitli etkileme, ikna ve kandırma yöntemleriyle istenilen (normalde paylaşmamaları gereken) bilgileri elde etmeye çalışmaktır.

11.1.Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
11.2.Arkadaşlarımızla paylaştığımız bilgileri seçerken dikkat edilmelidir.
11.3.Telefon, e-posta veya sohbet yoluyla yapılan haberleşmelerde Kullanıcı adı ve özellikle şifre bilgileri paylaşılmamalıdır. Şifre kişiye özel bilgidir. Sistem yöneticileri dâhil telefonda veya e-posta yazışmalarında şifremizi paylaşmamalıyız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
11.4.Kazaa, eMule gibi dosya paylaşım yazılımları kullanılmamalıdır.
11.5. Sadece yetkili kişilerin kurum içerisindeki sınırlı bölümlere erişim izni olduğundan emin olmak için uygun erişim kontrol mekanizmaları olması gerekir.
11.6.Kurum Web Sayfasında kurum ile ilgili paylaşılan bilgilere son derece dikkat edilmeli ve bu sürekli izlenmelidir.
11.7.Elektronik posta ile yapılan yazışmalarda saglik.gov.tr uzantılı e-posta hesapları kullanılmalıdır.
11.8.E-Postalara gelen kaynağı belli olmayan, şüphe uyandıran e-postalar açılmamalı ve ilgili sorumlulara bilgi verilmelidir.

12. SOSYAL MEDYA GÜVENLİĞİ

12.1.Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.
12.2.Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.
12.3.Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

13. İHLAL YÖNETİMİ VE YAPTIRIMLAR

13.1. Bilgi Güvenliği İhlal Yönetimi TURHAL Devlet Hastanesi ve tüm Bağlı Birimleri kapsamı dâhilinde yaşanabilecek Bilgi Güvenliği ihlal durumlarında sürecin nasıl yönetileceğini ifade eder.

Yönetim Uygulama:

Bilgi Güvenliği olayları derhal rapor edilmelidir. Bilgi Güvenliği kapsamındaki olaylar, raporun iletileceği yetkili birim ve kişiler aşağıda belirtilmiştir. Kurumsal Bilgi Güvenliği Politikasına uymayan her tür davranış, Bilgi Güvenliği prensiplerine aykırı her tür bilgi paylaşımı, uygunsuz PC/Notebook kullanımı, yetkisiz personellerin yetkili olmadıkları yerde görülmeleri/bulunmaları, Bilgisayar ve varlıkları ile ilgili her tür hırsızlık, kaybolma vb. olumsuz durumlar Bilgi Güvenliği olayı kapsamına girmektedir.

İşletim sistemi arızaları, sistemin yavaşlaması, cihazların fazla ısınması, spam olarak gelen e-postaların artması, yetkisiz girişe uygun olmayan alanlara yetkisiz girişlerin yapılması veya girişlerinin açık görülmesi/bulunması, kilitlenmeyen dolaplar, kapatılmayan oturumlar/bilgisayarlar, halka açık ve ya üçüncü şahısların görmemesi gerektiği ancak görebileceği ortamlarda bulunan belgeler/evraklar/dokümanlar diğer Bilgi Güvenliği İhlal olayları arasında yer almaktadır.

Olay halinde ilk müdahale ilgili/yetkili Birim tarafından yapılır. Olayı rapor eden personelin yetkililerin müdahalesine kadar hiçbir şeye dokunmaması gerekmektedir.

OLAY TANIMI	YETKİLİ BİRİM	YETKİLİ PERSONEL
Yetkisiz giriş	BİLGİ SİSTEMLERİ BİRİMİ	İDARİ HİZMETLER BAŞKANLIĞI
Yazılım arızası		
Virüs / Solucan / Trojan		
Spam		
Web Sitesinin Hack Edilmesi		
Tehdit / E-Posta Bombardımanı		
Müstehcen veya Çirkin Mesaj Gelmesi		
Güvenlik Açıklarından Faydalanma		
Diğer		

13.2.Yaptırımlar

Bilgi Güvenliği Politikası kapsamında oluşturulmuş kural ve süreçleri ihlal eden personel, paydaş ve üçüncü taraflar hakkında adli ve idari yasal takibat başlatılarak; 657 sayılı Devlet Memurları Kanununun 125. Maddesi gereğince işlem yapılabilir ve /ve ya ilgili sözleşmelerde yer alan yaptırımların 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. POLİTİKANIN YÜRÜRLÜĞE GİRİŞİ

İşbu "Bilgi Güveliği Politikası" TURHAL Devlet Hastanesi Başhekimliğince onaylanmasının ardından yürürlüğe girer ve tüm ERBAA Devlet Hastanesi personelince uyulması gereklidir.

15. POLİTİKANIN DUYURULMASI

İşbu "Bilgi Güveliği Politikası" yürürlüğe girmesinin ardından Tüm birimlere yazılı olarak iletilir. Politikanın tüm personelce okunup okunmadığı ayrı ayrı her bir birimin amiri sorumluluğundadır.

16. POLİTİKA GÖZDEN GEÇİRME KURALLARI

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

17. POLİTİKA REVİZYON GEÇMİŞİ

No	Revizyon Tarihi	Revizyon Detayı
00	12.10.2014	İlk Versiyon
01	23.11.2015	İkinci Versiyon
02	25.05.2018	Üçüncü versiyon

18. KAYNAKLAR/REFERANSLAR

❖ 28/02/2014 Tarih ve 5181.1272 sayılı Bilgi Güvenliği Politikaları Yönergesi

❖ Bilgi Güvenliği Politikaları Kılavuzu

❖ ISO/IEC 27001, ISO 22301 standartları

19. DESTEK POLİTİKALAR

Kurumumuz "Bilgi Güvenliği Politikası" 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 Politikası

❖ Parola Kullanım Politikası

❖ Anti virüs Politikası

❖ İnternet ve Ağ Kullanım-Erişim Politikası

❖ Genel Kullanım Politikası

❖ Gizlilik Sözleşmesi

19.1. E-Posta Kullanım Politikası

19.1.1. Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
19.1.2. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren epostalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
19.1.3. Kişisel kullanım için İntem et'teki listelere üye olunması durumunda kurum eposta adresleri kullanılmamalıdır.
19.1.4. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt verilmemelidir.
19.1.5. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
19.1.6. Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

19.1.7. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
19.1.8. Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
19.1.9. Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.
19.1.10. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu mailler virüs, e-mail bombaları ve truva atı gibi zararlı kodlar içerebilirler.
19.1.11. Kurum dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.
19.1.12. Elektronik postalar sık sık gözden geçirilmeli, gelen mesajlar uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki bir kişisel klasöre çekilmelidir.
19.1.13. Turhal Devlet Hastanesiçalışanlarının 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.
19.1.14. 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.
19.1.15. 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.

19.2. Parola Kullanım Politikası

19.2.1. 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.
19.2.2. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
19.2.3. Şifreler başkası ile paylaşılmamalı, kâğıtlara ya da elektronik ortamlara yazılmamalıdır.

19.2.4. Şifreler, küçük ve büyük karakterlere (örnek, a-z, A-Z), hem rakam hem de noktalama karakterlerine (örnek, 0-9, !'A+%&/()=?_;*) sahip olmalıdır.
19.2.5. En az sekiz adet alfa nümerik karaktere sahip olmalıdır.
19.2.6. Herhangi bir dilde argo, lehçe veya teknik bir kelime olmamalıdır.
19.2.7. Aile isimleri kullanılmamalıdır.
19.2.8. Herhangi bir kişiye telefonda şifre verilmemelidir.
19.2.9. Şifreler aile bireyleriyle paylaşılmamalıdır.
19.2.10. Şifreler, işten uzakta olunduğu zamanlarda iş arkadaşlarına verilmemelidir.
19.2.11. Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.
19.2.12. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

19.3. Anti virüs Politikası

19.3.1. Bütün bilgisayarlarda kurumun lisanslı antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.
19.3.2. Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamak ve hemen Bilgi İşlem Birimine haber verilmelidir.
19.3.3. Zararlı programlan (virüsler, solucanlar, truva atı, e-mail bombaları vb) kurum bünyesinde oluşturmak ve dağıtmak yasaktır.
19.3.4. Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını sisteme kuramaz.

19.4. Internet ve Ağ Kullanım-Erişim Politikası

19.4.1. Hiçbir kullanıcı eş bilgisayarlar arası (peertopeer) bağlantı yoluyla yani bir başka kullanıcının bilgisayarı ile doğrudan dosya alış verişi yapmayacak, bu paylaşıma izin veren herhangi yazılım kullanmayacaktır. (Örnek yazılımlar: Kazaa,eDonkey, Gnutella, Napster, Aimster, Madster, FastTrak, Audiogalaxy, MFTP, eMule, Ovemet, NeoM odus, Direct Connect, Asquisition, BearShare, Gnucleus, GTKGnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, OpenNapvb)
19.4.2. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağıma bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.
19.4.3. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde ICQ, MIRC, Messenger vb. mesajlaşma ve sohbet (chat) programları kullanılmamalıdır. Bu sohbet programları üzerinden dosya alışverişinde bulunulmamalıdır.
19.4.4. Hiçbir kullanıcı internet üzerinden Multimedia Streaming (video, mp3 yayını ve iletişimi)yapmayacaktır.

19.4.5. Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır. 19.4.6. İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (dovvnload) yasaktır.
19.4.7. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.
19.4.8. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
19.4.9. Üçüncü şahısların kurum içerisinden interneti kullanımları Bilgi İşlem Birim Sorumlusunun izni ve bu konudaki kurallar dâhilinde gerçekleştirilebilecektir.
19.4.10. 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.
19.4.11. Bilgi İşlem Birimi, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir.
19.4.12. 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.

19.5. Genel Kullanım Politikası

19.5.1. Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.
19.5.2. Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
19.5.3. 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.
19.5.4. Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimine haber verilmelidir.
19.5.5. Bütün kullanıcılar kendi bilgisayarlarının güvenliğinden sorumludur. Açık bırakılması halinde ve ya kullanıcı oturum şifrelerinin ikinci şahıslarca biliniyor olması durumlarında bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) bilgisayarın sahibi sorumludur.
19.5.6. Kurumun bilgisayarları kullanılarak taciz veya yasadışı olaylara karışılmamalıdır.
19.5.7. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packetsniffing, packetspoofing, denial of service vb.) eylemlere girişilmemelidir.

19.5.8. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DOS saldırısı, port,network taraması vb. yapılmamalıdır.
19.5.9. Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.
19.5.10. Cihazlar, yazılımlar ve veriler izinsiz olarak kurum dışına çıkarılmamalıdır.
19.5.11. Port veya ağ taraması yapılmamalıdır.
19.5.12. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
19.5.13. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
19.5.14. Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programlar (Dergi CD'leri veya internetten indirilen programlar vs.) kurulmamalı ve kullanılmamalıdır.
19.5.15. 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.
19.5.16. Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliği ile sorumludur.
19.5.17. Bilgi İşlem Birimi tarafından yetkili kişiler kullanıcıya haber vermek kaydı ile yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel bağlanılan bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.
19.5.18. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
19.5.19. Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
19.5.20. Kurumda Bilgi İşlem Biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.
19.5.21. 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.
19.5.22. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisansız yazılımı bilgisayarında barından personel ilgili mevzuat çerçevesinde kendisi sorumludur.
19.5.23. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
19.5.24. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir.

20. FORMLAR

20.1. İşten Ayrılış Onay Formu

İşten Ayrılacak Personelin	
Adı SOYADI:	Birimi:
Ünvanı/Görevi:	Ayrılış Tarihi:

Personelin Yetkisi Bulunan	
İNSAN KAYNAKLARI☐	İdr.ve Mali Hizmt. Müd. İmza
Yukarıda sahip olduğu yetkiler alınmıştır. Ayrılmasında bir mahzur yoktur.	

Personelin Zimmetinde	
Bilgisayar☐ Yazıcı☐ Tarayıcı☐ Telefon☐ Telsiz☐ Kurum Kimliği ☐ Yaka Kartı☐ Herhangi bir eşya bulunmamaktadır☐	
İlgili personel adına kayıtlı ..... kayıp / bozulma vb. nedenler dolayısı ile teslim edememiştir. İlgili demirbaşın bugünkü değeri olan ..... TL' nin kendisinden mahsup edilmesi gerekmektedir. Yukarıdaki prosedür gerçekleştirilmiştir. Ayrılmasında bir mahzur yoktur.	İdr. ve Mali Hizmt. Müd. İmza

Personelin Yetkisi Bulunan	
SAĞLIK NET ☐ EBYS ☐ ÇKYS/TSIM☐ E-POSTA☐ KULLANICI OTURUMU ☐ SİSTEM ERİŞİM YETKİSİ ☐	Bilgi İşlem Sorumlusu İmza
Yukarıda sahip olduğu yetkiler alınmıştır. Ayrılmasında bir mahzur yoktur.	

20.2. İhlal Bildirim Formu

KİŞİSEL BİLGİLER Adı :…… Soyadı :……..…….. Telefon:……..…… Eposta :……..… Kurum :…….. Birim :……..….. Tarih :……..….	**İHLAL TANIMLARI** **İHLAL AÇIKLAMASI**	**OLAY AYRINTILARI** □ Yetkisiz Giriş □ Kapatılmayan Oturum ve Bilgisayarlar □ Kurumdaki Dolapların Açık Bırakılması □ Kurumdaki Belge ve Evrakların Gizliliğinin İhlali □ Yazılım Arızası □ Virüs/Solucan/Trojan □ Web Sitesinin Hack Edilmesi □ Tehdit/E-Posta Bombardımanı □ Copyright Usulsüzlüğü □ Fraud/Spam □ Müstehcen veya Çirkin Mesaj Gelmesi □ Güvenlik Açıklarından Faydalanma □ Diğer

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
Bilgi İşlem Sorumlusu		