BİLGİ GÜVENLİĞİ POLİTİKASI

OCAK 2019

İÇİNDEKİLER

1. AMAÇ

S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma 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 S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi ve bağlı birimlerin sahip olduğu tüm bilgi varlıklarının korunması ve uygun biçimde yönetilmesinin sağlanmasıdır.

Aynı zamanda tüm ilgili taraflara S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma 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, S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi ve tüm bağlı birimleri kapsar. S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi Bilgi Güvenliği Politikası aşağıdaki varlık ve teknoloji kategorilerini kapsamaktadır:

3.1. Veri dosyaları, sözleşmeler ve benzeri tüm bilgi varlıkları,
3.2. Uygulama yazılımları, sistem yazılımları ve hizmetlerden oluşan yazılım varlıkları,
3.3. 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,
3.4. Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan oluşan hizmet varlıkları,
3.5. Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıkları,
3.6. Kurum tarafından üretilen, kullanılan ve/ve ya geliştirilen tüm verileri kapsar.

4. TANIMLAR

Bu politika ve esaslarında geçen,

S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi	:	S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi, Bağlı Ek Hizmet Binaları ve Bağlı Tüm Birim ve Servisleri ifade etmektedir.
Bağlı Birimler:	:	S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi Bağlı Ek Hizmet Binaları ve Bağlı Tüm Birim ve Servisleri ifade etmektedir
Bilgi Güvenliği Yönetim Sistemi (BGYS)	:	Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. Yönetim sistemi kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, sözleşmeleri, talimatları, prosedürleri, prosesleri ve tüm kaynakları içerir.
Varlık	:	S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma 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.
Bilgi güvenliği ihlal olayı:	:	İş operasyonlarını tehlikeye atma, bilgi akışını engelleme veya yavaşlatma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen/ beklenmeyen olay ya da olayları ifade etmektedir.
Bilgi Güvenliği Sorumluları	:	Bilgi Sistemlerinden sorumlu Başhekim, Başhekim Yardımcısı, Müdür, Müdür Yardımcısı, Koordinatör
SBSGM:		T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğünü ifade etmektedir.

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 güvenliği 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 işe yeni başlayan 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. S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi çalışanları kullandıkları tüm bilgi sistemlerinde **"Parola Politikası"**na uygun hareket edeceklerdir.

5.12. S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi çalışanları internet sistemlerini kullanırken **"İnternet ve E-Posta Kullanım Prosedürü"**ne uygun hareket edeceklerdir.

5.13. Tüm birim yöneticileri bu esasların uygulanmasından birinci derecede sorumlu olacak 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 ve erişilebilirliğinin korunmasından varlık sahipleri sorumludur.

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

7. BİLGİ GÜVENLİĞİ ORGANİZASYONU

7.1. Bilgi Güvenliği Alt Komisyonu

7.1.1. S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi bünyesinde, bilgi güvenliği ve siber olaylara müdahale faaliyetlerini yürütmek ve koordine etmek üzere "Bilgi Güvenliği Alt komisyonu" oluşturulur.

7.1.2. Alt Komisyon çalışmalarında Hastane Başhekim Yardımcısı, İdari Mali İşler Müdür Yardımcısı, Bilgi İşlem Sorumlusu, Bilgi Güvenliği Yetkilileri, Kalite Yönetim Birimi ve Direktörü komisyon üyesi olarak yer alır. Ayrıca gerekli görülecek diğer personel de komisyon toplantılarına davet edilir.

7.2. Bilgi Sistemleri Koordinatörü

7.2.1. Alt Komisyonların çalışmaları en az başkan seviyesinde bir yönetici tarafından koordine edilir ve "Bilgi Sistemleri Koordinatörü" olarak görev yapar.

7.3. Bilgi Güvenliği Yetkilisi

7.3.1. S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi bünyesinde bilgi güvenliği faaliyetlerini yürütmek ve koordine etmek üzere "Bilgi Güvenliği Yetkilisi" görevlendirilir.

7.3.2. Bilgi güvenliği yetkilisi olarak; yönetim sistemleri konusunda tecrübeli, kurumda yürütülen iş süreçlerine hakim, kurum kültürüne vakıf, tercihen bilgi sistemleri konusunda teknik eğitim almış, bilgi güvenliği ile ilgili faaliyetleri yürütürken kurumda görev yapan tüm personel ile uygun yöntemlerle iletişim kurabilecek, gerektiğinde otorite kullanabilecek, mümkünse yönetici düzeyinde bir personel görevlendirilir.

7.3.3. Bilgi güvenliği yetkilisinin ana işlevi, bulunduğu kurumdaki bilgi güvenliği faaliyetlerini SBSGM ile koordineli bir şekilde yürütmektir.

7.4. Üst Yönetimin Sorumluluğu

7.4.1. Bilgi güvenliği politikalarının uygulanması üst yönetim tarafından takip edilir. Bilgi güvenliği politikası kapsamında, bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi üst yönetimin sorumluluğundadır.

7.4.2. Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projeler üst yönetim tarafından gözden geçirilir ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanır.

7.5. Hastaneler Bilgi Güvenliği Organizasyonu

7.5.1. S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi'ne bağlı Kamu Hastanelerinde bilgi güvenliği faaliyetlerinin koordine edilmesi amacıyla; ilgili kurum kendi bünyesinde üst yönetici düzeyinde **"Bilgi Güvenliği Koordinatörü"** ve koordinatöre bağlı olarak **"Bilgi Güvenliği Yetkilisi"** görevlendirir. Bilgi güvenliği yetkilisi asil ve yedek olmak üzere kurumun yönetim sistemleri konusunda tecrübeli, kurumda yürütülen iş süreçlerine hakim,

tercihen bilgi sistemleri konusunda teknik eğitim almış, gerektiğinde otorite kullanabilecek, mümkünse yönetici düzeyinde bir personel görevlendirilir.

7.5.2. Ayrıca bilgi güvenliği faaliyetlerinin yürütülmesi amacıyla kurumun kendi bünyesinde **"Bilgi Güvenliği Alt Komisyonu"** oluşturulması tavsiye edilir.

7.5.3. Görevlendirilen bilgi güvenliği yetkilisi, bulunduğu kurumdaki bilgi güvenliği faaliyetlerini S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi ile koordineli bir şekilde yürütür.

7.5.4. İlgili kurumların bilgi güvenliği organizasyonları; ayrıca BGYS Politikasını hazırlayacaklardır. Hazırlanan politika S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi "Bilgi Güvenliği Yönetim Sistemi Politikası"na aykırı olmayacak şekilde ilgili kurumun kendi faaliyet alanına göre detaylandırılmış olmalıdır.

8. İNSAN KAYNAKLARI GÜVENLİĞİ

8.1. İşe Alma Öncesinde Yapılacak Kontroller

8.1.1. İşe alınacak adaylar (kamu personeli, tam zamanlı ya da yarı zamanlı olarak çalışan sözleşmeli personel, yüklenici firma çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli vb.) iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilir (tarama yapılır). Bilgi güvenliği ve Sosyal Mühendislik zafiyetleri konularında eğitim verilir.

8.1.2. Tarama yapılırken yürürlükteki yasal mevzuata mutlak şekilde uyulur. Yasal ve etik olmayan tarama yöntemleri kullanılmaz. Tarama esnasında oluşturulan/elde edilen kayıtlar uygun şekilde saklanır. Saklanmasına ihtiyaç duyulmayan kayıtlar bekletilmeksizin imha edilir

8.1.3. İşe alınacak kişilerin eğitim, yeterlilik ve güvenilirlik yönleriyle kontrol edilmesi için aşağıdaki yöntemlerden biri ya da birkaçı birlikte kullanılabilir:

1- Kişi özgeçmişinin doğrulanması (belgelerin tamlığı),
2- Kişinin atanacağı görevle ilgili eğitim ve tecrübe açısından gerekli yeterliliğe sahip olmasının sağlanması,
3- Beyan edilen akademik ve işle ilgili niteliklerin doğrulanması (diplomaların, referans mektuplarının, bonservis belgelerinin doğru ve geçerli olduğunun teyit edilmesi),
4- 657 sayılı Kanunun 48/8 maddesi gereği Yönetim Hizmetleri Genel Müdürlüğünce, devlet memurluğuna atanacak kişiler ile ilgili olarak 12 Nisan 2000 tarihli ve 24018 sayılı Resmi Gazetede yayımlanan "Güvenlik Soruşturması ve Arşiv Araştırması Yönetmeliği" uyarınca "güvenlik soruşturması ve/veya arşiv araştırması" yaptırılması,
5- 657 sayılı Kanuna bağlı olmayan diğer personel için bağlı oldukları yasal mevzuatta yer alan hükümler uyarınca güvenlik incelemelerinin yaptırılması,
6- Yüklenici personeli, destek personeli vb. statüde çalışacak personelin adli sicil kayıtlarının istenmesi ve incelenmesi

8.1.4. Yükleniciler ile yapılan sözleşmelerde, idare tarafından yüklenici personeli için tarama yürütüleceği ve tarama sonuçlarının menfi olması durumunda alınacak önlemler (örneğin personelin değiştirilmesi vb.) belirtilir.

8.1.5. İşe başlamadan önce tüm personel ile **Bilgi Güvenliği Farkındalık Bildirgesi**, yükleniciler ile **kişisel ve/veya kurumsal gizlilik sözleşmesi** imzalanacağı ilgili taraflara bildirilir. İmzalatılacak sözleşmelerin içeriği ve ilgililerin yükümlülükleri detaylı olarak

açıklanır. Sözleşmelerde kişilerin ve idarenin bilgi güvenliği sorumlulukları açıkça belirtilir.

8.1.6. Kuruluşun güvenlik gereksinimleri dikkate alınmadığında çalışanlar ve yükleniciler için yürütülecek işlemler (disiplin kurallarının uygulanması, gerekiyorsa iş akitlerinin sonlandırılması, tedarik sözleşmesinin feshi vb.) önceden belirlenir ve taraflara duyurulur.

8.2. Çalışma Esnasında Uygulanacak Kontroller

8.2.1. Çalışma esnasında uygulanacak güvenlik kontrollerinin amacı çalışanların işlerini yaparken bilgi güvenliği ile ilgili sorumluluklarının farkında olmalarını ve beklenen şekilde yerine getirmelerini sağlamaktır.

8.2.2. İşe yeni başlayan personelin başlayış işlemlerinin eksiksiz olarak yapılmasını sağlamak için **"İşe Başlama Formu"** uygulanır.

8.2.3. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi sorumludur.

8.2.4. Bilgi güvenliği ile ilgili beklentiler ve sorumluluklar, çalışanların görev tanımlarına eklenmelidir. Tüm çalışanların **bilgi güvenliği farkındalık eğitimi** programlarına katılmaları sağlanmalıdır.

8.3. Görev/Birim Değişikliği ve İşten Ayrılma İçin Uygulanacak Kontroller

8.3.1. Görev değişikliği veya işten ayrılma ile ilgili güvenlik kontrollerinin amacı, ayrılma işlemleri esnasında yapılması gereken bilgi güvenliği ile ilgili tedbirlerin ortaya konulması ve çalışanların görevleri sona erse dahi bilgi güvenliği ile ilgili devam eden sorumlulukları hakkında bilgilendirilmesidir.

8.3.2. Kişi, görevi esnasında edinmiş olduğu bilgileri, görev yeri değişmesi veya ayrılması durumunda dahi sır olarak saklamaktan ve hiçbir şekilde yetkisiz olarak ifşa etmemekten sorumludur. Sır saklama yükümlülüğü süresizdir.

8.3.3. İşten ayrılan veya görev değişikliği yapan personelin ayrılma işlemlerinin eksiksiz olarak yapılmasını sağlamak için **"Personel İşten Ayrılma Onay Formu"** uygulanır.

8.3.4. Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan formda imzası bulunan Birimlerin yöneticileri sorumludur.

8.3.5. İşten ayrılan veya görev yeri değişen kişinin eski görevi ile ilgili bilgisayar hesapları ve uzaktan erişim için kullandıkları hesaplar kapatılır veya erişim yetkileri yeni görev yerinin gereksinimlerine göre yeniden düzenlenir.

8.3.6. Kişiye teslim edilmiş tüm bilgi varlıkları (bilgisayarlar, yazılı ortamda saklanan bilgi ve belgeler, bilgisayar ortamında tutulan dosyalar, lisans belgeleri, CD'ler vb.) sayım yapılarak iade alınır.

8.3.7. Kullandığı bilgi sistemlerine yönelik (TSİM, ÇKYS, EBYS, HBYS, MBYS, MKYS, USS vb.) kullanıcı adı ve şifreleri sistem yöneticisi tarafından pasif hale getirilmelidir.

8.3.8. Görevden ayrılan personel zimmetinde bulunan malzemeleri teslim etmelidir.

8.3.9. Ayrılan veya görev yeri değişen personel tarafından yürütülen faaliyetlerin aksamaması için birim sorumlusu tarafından gerekli tedbirler alınır.

8.3.10. Ayrılan kişiden teslim alınan bilgisayarlar güvenli silme işlemi yapılmadan bir başka kullanıcıya teslim edilemez.

8.3.11. İlgili form doldurulmadan personelin kurum ile ilişiği kesilmez.

9. FİZİKSELVE ÇEVRESEL GÜVENLİK

Fiziksel ve çevresel güvenlik, işyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.

9.1. Fiziksel Güvenlik Sınırı

9.1.1. Bilgi ve bilgi işleme tesislerini barındıran güvenli alanlar tespit edilmelidir ve bu alanların güvenlik sınırları tanımlanmalıdır.

9.2. Fiziksel Giriş Kontrolleri

9.2.1. Güvenli alanlar için sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları (kartlı geçiş sistemleri, turnikeler, kayar kapılar, kilitli odalar vb.) kurulmalıdır.
9.2.2. Tüm personelin rahatça teşhis edilmelerini sağlayacak kimlik kartları kullanılmalıdır.
9.2.3. Güvenli alanlara erişim hakları düzenli olarak gözden geçiriliyor olmalıdır.

9.3. Ofislerin ve Odaların Güvenliğinin Sağlanması

9.3.1. Ofis ve odalarla ilgili fiziksel güvenlik önlemleri alınmalıdır.
9.3.2. Personel güvenliği ve sağlığı için ilgili yönetmelikler uygulanmalıdır.
9.3.3. Binada bilgi işlem faaliyetlerinin yürütüldüğüne (Sunucu Odası vb.) dair işaret, tabela vb. bulundurulmamalıdır.

9.4. Harici ve Çevresel Tehditlerden Korunma

9.4.1. Yangın, sel, deprem, patlama ve diğer doğal afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.

9.5. Güvenli Alanlarda Çalışma

9.5.1. Dış taraf destek personeline güvenli alanlara veya gizli bilgi işleme tesislerine erişim izni, sadece gerekli olduğu durumlar için geçici süre ile verilmelidir.
9.5.2. Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir.
9.5.3. Sahipsiz güvenli alanlar fiziksel olarak kilitlenmelidir ve periyodik olarak gözden geçirilmelidir.
9.5.4. Güvenli bölgelere girişler (Sistem odası vb.) kayıt altına alınmalıdır.

9.6. Ekipman Güvenliği

9.6.1. Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğünün bozulmalarına ya da yok olmalarına sebep olabilir. Tüm bu veya daha fazla tehditleri yok edebilmek için aşağıda yer alan belli başlı temiz masa kurallarına çalışanlar tarafından uyulması sağlanmalıdır.

9.6.2. Belli başlı temiz masa kuralları

9.6.2.1. Hassas bilgiler içeren bilgi, belge ve evraklar masa üzerlerinde ya da kolayca ulaşılabilir yerlerde açıkta bulundurulmamalıdır. Bu bilgi ve belgeler kilitli dolap, çelik kasa ya da arşiv odası gibi fiziki koruması olan güvenli alanlarda muhafaza edilmelidir.

9.6.2.2. Yetkisiz kişilerin erişiminin engellenmesi için bilgisayar başından ayrılma durumunda ekran kilitlemesi yapılmalıdır. Otomatik ekran kilitlemesi devreye alınmalıdır.

9.6.2.3. Sistemlerde kullanılan parola, telefon numarası ve T.C. kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulundurulmamalıdır.

9.6.2.4. Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler belirtilen yöntemler ile imha edilmelidir.

9.6.2.5. Faks makinelerine gelen yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmaması için tedbir alınmalıdır.

9.6.2.6. Her türlü bilgiler, parolalar, anahtarlar ve bilginin sunulduğu sistemler, sunucular, kişisel bilgisayarlar ve benzeri cihazlar yetkisiz kişilerin erişebileceği bir şekilde parola korumasız ve fiziki olarak güvensiz bir şekilde gözetimsiz bırakılmamalıdır.

9.6.3. Ekipman Yerleşimi ve Koruması

9.6.3.1. Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararlar asgari düzeye indirilmelidir.

9.6.3.2. Ekipmanlar, gereksiz erişimleri asgari düzeye indirecek şekilde yerleştirilmelidir.

9.6.3.3. Nem ve sıcaklık gibi parametreler izlenmelidir.

9.6.3.4. Bilgi işlem araçlarının yakınında yeme, içme ve sigara kullanımı konularını düzenleyen kurallar olmalıdır.

9.6.4. Destek Hizmetleri

9.6.4.1. Elektrik, su, kanalizasyon ve iklimlendirme sistemlerinin, desteklediklerı bilgi işlem birimi için yeterli düzeyde olmalıdır.

9.6.4.2. Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.

9.6.4.3. Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.

9.6.4.4. Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.

9.6.5. Kablolama Güvenliği

9.6.5.1. Hatalı bağlantıların olmaması için ekipman ve kablolar açıkça etiketlenmiş ve işaretlenmiş olmalıdır.

9.6.5.2. Alternatif yol ve iletişim kanalları mevcut olmalıdır.

9.6.5.3. Fiber optik altyapı yapılandırılmalıdır.

9.6.5.4. Bağlantı panelleri ve odalara kontrollü erişim altyapısı kurulmuş olmalıdır.

9.6.6. Ekipman Bakımı

9.6.6.1. Kurumda kullanılmakta olan ekipmanların yıllık bakım planları oluşturulmalıdır.

9.6.6.2. Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılır.

9.6.6.3. Bakım işlemleri sadece yetkili personel tarafından yerine getirilmelidir.

9.6.6.4. Tüm şüpheli ve mevcut arızalar ile bakım çalışmaları için kayıt tutulmalıdır.

9.6.6.5. Ekipman bakım için kurum dışına çıkarılırken kontrolden geçirilmelidir. Bu kapsamda diskler sökülür ya da yedek alınarak diskte yer alan bilgiler kalıcı olarak silinmelidir.

9.6.6.6. Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınmalı ve takip edilmelidir.

9.6.7. Kurum Dışındaki Ekipmanın Güvenliği

9.6.7.1. Bu şekilde kullanılan ekipmanların ve kullanıcıların listesi oluşturulmalı ve takip edilmelidir.

9.6.7.2. Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenmelidir.

9.6.7.3. Tesis dışına çıkarılan ekipmanın gözetimsiz bırakılmamasına ve seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir.

9.6.7.4. Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulmalıdır.

10. TEDARİKÇİ İLİŞKİLERİ

10.1. Mal ve Hizmet Alımı Güvenliği

10.1.1. Satın alma faaliyetine konu olan iş kapsamında; yükleniciye veri/bilgi teslim edilmesi, kurum fiziki alanlarında personel çalıştırılması veya kurum bilgi sistemlerine erişim ihtiyacı olması halinde; satın alma için hazırlanan teknik ya da idari şartnamelere "Bilgi Güvenliği Gereksinimleri" başlığı altında asgari olarak aşağıdaki hususlar eklenmelidir:

10.1.2. Yüklenici sözleşmeye konu yükümlülüklerini ifa ederken, Kurum Bilgi Güvenliği politikalarına uymak zorundadır.

10.1.3. Kurum BGYS Politikaları uyarınca, idareye ait bilgilerin korunması maksadıyla, yükleniciler ile "**Kurumsal Gizlilik Taahhütnamesi**" ve söz konusu iş kapsamında çalışacak olan yüklenici personeli ile "**Personel Gizlilik Sözleşmesi**" imzalanmalıdır.

10.1.4. Teknik/idari şartnamelere veya tedarikçiler ile imzalanacak gizlilik sözleşmelerine aşağıdaki konular eklenerek garanti altına alınmalıdır:

10.1.4.1. Alınan hizmetle ilgili olarak güvenlik kontrol gereksinimleri, hizmet seviyeleri ve yönetim gereksinimleri,

10.1.4.2. Yükleniciye verilecek veya erişilecek bilgilerin tanımları ile bu bilgilerin sağlanma veya erişim metotları,

10.1.4.3. Yüklenici ile paylaşılacak olan bilgilerin kabul edilebilir kullanım kuralları ve gerekiyorsa kabul edilemez kullanım durumları,

10.1.4.4. Yüklenici personeli için erişim yetkilendirme ve yetki kaldırma prosedürleri,

10.1.4.5. Bilgi güvenliği olay müdahale prosedürleri (özellikle olay bildirimi ve olay müdahalesinde işbirliği kuralları).

10.1.5. Alınacak mal veya hizmetin tahmini bedelleri bağlamında idare tarafından yapılan yaklaşık maliyet çalışması, ihale aşamasına kadar gizli tutulmalıdır.

10.1.6. Söz konusu alım için gerekli iş tanımı ölçütleri, personel istihdam edilecekse ilgili personel özellikleri açıkça belirtilmelidir.

10.1.7. Tedarikçinin çalıştırılacağı personelin adli sicil kayıtlarını sorgulatıp, bunları idareye bildirmesi istenmelidir.

10.1.8. Satın alma faaliyetine konu iş uygulama/yazılım geliştirme ise; uygulama ile ilgili gerekli dokümantasyonun hazırlanması, ilgili projeye ait kaynak kodların teslim edilmesi gibi hususlar ile kişisel veriler işlenecek ise KVKK'nın 2018/10 sayılı kararında belirtilen ilave güvenlik tedbirleri ile ilgili hususlar; özel nitelikli teknik şartnamelere eklenmelidir.

10.1.9. Tedarikçilere verilen fiziksel ve mantıksal erişimler, kurumların bilgi güvenliği alt komisyonlarında gözden geçirilmelidir. İhtiyacın bitmesi durumunda, verilen yetkiler kaldırılmalıdır.

10.1.10. Ürünlerin satın alınmadan önce kurumsal olarak belirlenen güvenlik gereksinimleri için risk oluşturmadığından emin olunması için test edilmesi sağlanmalıdır.

10.2. SBYS Firmaları ile İlişkilerde Dikkat Edilecek Hususlar

10.2.1. SBYS (Sağlık Bilgi Yönetim Sistemi) yazılımlarının (HBYS, AHBS, LBYS, PACS/RIS vb.) Bakanlık tarafından yayımlanan sağlık bilişimi standartlarına ve veri gönderim servislerine uyumlu olmaları gerekmekte olup, SBYS üreticisi firmalar, Bakanlık tarafından talep edilen geliştirmeleri ve güncellemeleri belirtilen süreler içerisinde sistemlerine yansıtmalıdır.

10.2.2. KTS (Bakanlık Kayıt Tescil Sistemi) yetki belgesi olmayan, geçersiz yetki belgesi ibraz eden ya da KTS web sayfasında pasif listede yer alan SBYS yazılım üreticileri ile sözleşme imzalanmamalıdır.

10.2.3. Sağlık kuruluşları ile SBYS yazılım üreticisi arasında yaşanabilecek uyuşmazlıklarda uygulanacak cezai şartların SBYS yazılım üreticisi ile yapılacak sözleşmelerde yer alması sağlanmalıdır.

10.2.4. SBYS'lerin ilk kurulumu esnasında uzaktan destek ile kurulum talepleri kabul edilmemelidir.

10.2.5. SBYS yazılım üreticisi, ilk kurulum esnasında çalıştıracağı personel ile ilgili planlamayı kurulum ve proje planında detaylı olarak açıklamalıdır.

10.2.6. Sözleşme imzalandıktan sonra SBYS'nin işletmeye alınacağı tarih, sağlık kuruluşları tarafından hazırlanan şartnamelerde belirtilmelidir.

10.2.7. Sağlık kuruluşları, HBYS tedarikçilerinden en az altı ayda bir kez olacak şekilde son alınan yedek üzerinden veri kurtarma testi yapmasını istemeli ve gerekli kontrolleri yapmalıdır.

10.2.8. Herhangi bir sebeple mevcut SBYS yazılımının kullanımına son verilirse, verilerin tamamı orijinal veri tabanı formatında, kolay ve sorunsuz okunabilir bir medya ortamında, 3 (üç) kopya halinde sağlık kuruluşuna teslim edilmelidir.

10.2.9. Kritik alanlardaki değiştirme ve silme işlemlerinin, ancak yetki ölçüsünde yapılmalı, değişikliklere sonradan erişim ve geri düzeltme için mutlaka iz kaydı dosyaları detayları olarak tutulmalı veya VTYS katmanındaki denetleme (audit) uygulama yazılımından da desteklenir olmalıdır.

10.2.10. Kişisel sağlık verileri özel nitelikli kişisel veriler kapsamında olması sebebiyle; sözleşme süresince veya sonrasında kayıtlı tüm veriler hiçbir surette, hiçbir zaman SBYS üreticisinde kalmak üzere kopyalanamaz, çıktı alınamaz, firma sunucularına aktarılamaz, ifşa edilemez olmalıdır.

10.2.11. SBYS'de kullanıcıların otomasyona giriş-çıkış zamanları ve geçersiz giriş denemeleri istenildiğinde raporlanabilmelidir.

10.2.12. Poliklinik, Klinik, Laboratuvar bazında yetkilendirmeler yapılabilmelidir. Kullanıcının yetki verilmeyen bir polikliniktekı hasta listesine erişimi engellenmelidir.

10.2.13. SBYS yazılımlarında "Parola Güvenliği" ile ilgili bölümde belirtilen parola özellikleri tanımlanabilmeli ve bu kurala uymayan parolalar kabul edilmemelidir.

10.2.14. Sağlık kuruluşu ile ilişiği kalıcı olarak kesilen tüm personelin SBYS erişim yetkisi tamamen ve otomatik olarak iptal edilmelidir.

10.2.15. Geçici olarak sağlık kuruluşunda bulunmayan (izin, rapor, geçici görev kurs, eğitim vb.) personelin SBYS'ye girişi otomatik olarak engellenmelidir.

10.2.16. Sunucu işletim sistemi, sunucu yazılımları, veri tabanında yapılacak yapısal değişiklikler gibi tüm sistemi etkileyen güncellemeler mesai saatleri dışında veya hasta yoğunluğunun en az olduğu saatlerde yapılmalıdır. Acil müdahale edilmesi gereken bir arıza durumunda ise mesai saatleri içinde güncelleme yapılabilmelidir.

11. BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

11.1. Bilgi Güvenliği İhlal Olayı

Kurumun bilgilerinin gizliliğini, bütünlüğünü veya kullanılabilirliğini herhangi bir biçimde etkileme potansiyeline sahip herhangi bir olaydır. Aşağıdaki hususlardan kaynaklanacak ihlaller Bilgi Güvenliği İhlali Olarak kabul edilmiştir:

11.1.1. Kullanılan bilgi varlıklarının çalınması, kaybolması ya da kırılması

11.1.2. Bilginin Gizlilik, Bütünlük, Erişilebilirlik beklentilerindeki ihlaller

11.1.3. İnsan hatalarından kaynaklanan ihlaller

11.1.4. Genel Müdürlük ve Bakanlık tarafından yayımlanmış Bilgi Güvenliği Yönergesi, Politikalar ve Prosedürlere göre iş ve işlemlerin yürütülmemesi

11.1.5. Fiziksel Güvenlik düzenlemelerinin ihlali

11.1.6. Kontrolsüz sistem değişiklikleri

11.1.7. Yazılım ya da donanım arızaları

11.1.8. Erişim ihlalleri (yetkisiz erişim), yetkisiz bilgi kullanımına izin veren uygun olmayan erişim denetimleri

11.1.9. Siber saldırılar (Virüs, izinsiz giriş, Truva atı, casus yazılım vb. bulgular, sistem sunucu servis problemleri)

11.1.10. Gizli bilginin yetkisiz kişilerce ifşa edilmesi

11.2. Olay Tanımları

11.2.1. Servis Dışı Bırakma (DDOS): Çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur, bunlar genellikle bir veya birden fazla web sunucusudur. Bu sistemler saldırganlar tarafından çeşitli yöntemler kullanılarak bağdaştırılır.

11.2.2. Bilgi Sızdırma (Data Leakage): Kurumun bilişim teknolojileri ile kullandığı, işlediği ya da ürettiği verilerin bilinçli ya da bilinçsiz bir şekilde kurum dışına taşınarak, belirlenmiş "bilgi güvenliği" politikalarının ihlali.

11.2.3. Zararlı Yazılım (Malware): Bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara genel olarak verilen ad.

11.2.4. Dolandırıcılık (Fraud): Aldatma amacı ile yapılan kasıtlı eylemdir.

11.2.5. Port Tarama: Sunucu üzerinde çalışan servislerin hizmet verdiği mantıksal bağlantı noktalarını ve durumlarını tespit etmek için yapılan işlemdir.

11.2.6. Veri Tabanı Saldırısı: Veri tabanı yazılımlarının kullanımından oluşabilecek zafiyetlerinden veri tabanının ele geçirilmesi, yönetilmesi ya da yetki yükseltilmesi şeklindeki saldırılardır.

11.2.7. Web Uygulamaları Güvenlik İhlalleri: ARP sızdırma, işlevselliğin kötüye kullanımı, içeriğe sızma, DNS çalınması vb. metotlar ile web sitesinin güvenliğinin tehdit edilmesi veya sağlanamaması durumlarıdır.

11.2.8. Sosyal Mühendislik: İnternette insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir. Gizli bilgilerin e-posta aracılığı ile iletimi, ağ üzerinden iletilen bilgilerin yetkisiz ya da yanlış alıcıya iletimi, internet üzerinden güvenli olmayan kanallar aracılığıyla veri iletimi, ortak kullanım yazıcılarından alınan çıktıların sahiplenilmemesi ya da güvenliğine önem verilmemesi, masa üstü ya da ortak alanlarda basılı kopyaların denetimsiz bırakılması vb. durumlarda tüm çalışanlar verilerin güvenliğini ve bütünlüğünü korumanın önemini göz önünde bulundurarak bilinçli hareket etmeli, ihlal durumlarını rapor etmesi gerekir.

11.2.9. Zararlı Elektronik Posta (Spam): İsteğiniz olmadan, size gönderilen ticari içerikli oyada politik bir görüşün propagandasını yapmak ya da bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileridir.

11.2.10. Parola ele geçirme: Depolanmaması gereken bir yerde depolanan parolaların tespiti ya da sızması durumudur. Ya da herhangi bir saldırı yöntemi ile parolaların ele geçirilmesidir.

11.2.11. Taşınır Cihaz Kaybı: CD / DVD, DAT (manyetik ses bandı), veri depolamak için USB taşınabilir veri depolama / HD sürücüler gibi taşınabilir ortamların kullanılması, kullanıcının bu tür cihazları kullanma sorumluluklarının tamamen farkında olmasını gerektirir. PC'lerin, dizüstü bilgisayarların, tabletlerin ve diğer taşınabilir aygıtların kullanılması, verilerin

izinsiz erişime açık hale gelmesine neden olabilir. Kasıtlı ya da kazayla, herhangi bir taşınabilir aygıtın yetkili kullanıcısı (taşınabilir medya dâhil) dışında kullanımı, kaybı veya bulunması durumunda İhlal Olay Raporlama prosedürleri aracılığıyla BGYS Birimine bildirilir.

11.2.12. Kimlik taklidi: Kişilerin fiziksel, telefon ya da dijital ortamda olmadığı bir kişi gibi davranıp, onun yetkilerini bilgisi dışında kullanmasıdır.

11.2.13. Oltalama: Dolandırıcıların kullanıcı hesaplarına rastgele e-posta göndererek bilgi sızdırmaya yönelik çevrimiçi saldırı türüdür.

11.2.14. Kişisel bilgilerin kötüye kullanımı: Tüm kişisel nitelikteki bilgileri görüntülemek, ifşa etmek veya dağıtmak 6698 sayılı Kişisel Verilerin Korunması Kanunu (Dış Kaynaklı Doküman Listesi) usul ve esaslarına aykırıdır. Herhangi kasıtlı ya da hata ile oluşacak kişisel bilgilerin kötüye kullanımı durumların raporlanması zorunludur.

11.2.15. Diğer ihlal olayları: Yukarıda tanımlanan ihlal olaylarının dışında bilgi güvenliğini tehdit eden diğer ihlallerdir.

11.3. Uygulama

11.3.1. İhlal bildirimleri, **Olay Bildirim ve Müdahale Formu** aracılığı ile gerçekleştirilir.

11.3.2. Bakanlık çalışanları ve vatandaşlar tarafından tespit edilen Sağlık Bakanlığı ile ilgili her türlü bilgi güvenliği ihlal olayı https://bilgiguvenligi.saglik.gov.tr/ adresinde yer alan merkezi ihlal bildirim sistemine girilir.

11.3.3. Küçük çaplı, yalnızca kendi kurumunu ilgilendiren ve bilgi güvenliği yetkilisi ya da kurumsal SOME tarafından kendi imkânları ile yerel olarak çözülebilecek olaylara kurumun SOME'si veya bilgi işlem personeli tarafından gerekli müdahale yapılır. Müdahale sonrasında "Olay Müdahale" Formunun 2. bölümü doldurularak e-Posta ile bilgiguvenligi@saglik.gov.tr adresine gönderilir.

11.3.4. BGYS Birim sorumlusu bildirimin bilgi güvenliği ihlal olayı olup olmadığını tespit eder, analizini yaparve yayılmasını önlemek için alınması gereken acil eylem gerekli ise süreci başlatır. Olayın ciddiyeti değerlendirilip yasal işlem öngörülmekte ise, ilgili hukuki ya da güvenlik otoriteleri sürece dâhil edilir.

11.3.5. İhlal olayının çözümü için kullanılacak bildirim yöntemi e-posta ya da telefondur.

11.3.6. BGYS Birimi tarafından yapılan değerlendirme sonucunda ihlal olayının çözümü için ilgili sorumlu tarafa (üst yönetime) ivedi bir şekilde iletişime geçerek olayın çözümü için harekete geçilir.

11.3.7. Kapsam dâhilinde ya da taşra teşkilatından bildirilen ihlal olayları web sitesi üzerinden sadece yetkilendirilmiş BGYS ekibi tarafından izlenmek ve rapor edilmek üzere saklanır.

11.3.8. Bildirilen ihlal olayının çözümü için atılan adımlar her bir ihlal olay kaydı için ayrı ayrı yazılarak olay kapatılır.

11.3.9. Bildirilen ihlal olayları çerçevesinde yapılan bildirimler sonucu çözümleri, her hangi bir maliyet gerektiriyor ise sorumluluk ihlalin çözümünü üretecek birime aittir. BGYS Birimi sadece olayı ilgili taraflara bildirmek suretiyle çözülmesini sağlayacaktır.

11.3.10. Bilgi Güvenliği ihlal olayları, BGYS Birimi tarafından kaydedilerek, gerekli ise Düzeltici Faaliyet planlanır ve/veya farkındalık e-postaları gönderilir. Ayrıca, yılda bir kez yapılan BGYS farkındalık eğitimleri için olay kayıtları girdi oluşturur.

12. SOSYAL MÜHENDİSLİK VE SOSYAL MEDYA GÜVENLİĞİ

12.1. Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanır. Başka bir tanım ise insanoğlunun zaaflarını kullanarak istenilen bilgiyi, veriyi elde etme sanatıdır.

12.2. Sosyal mühendislik yapan kötü niyetli kişiler, sosyal medya ve analiz yöntemlerini kullanarak hedef kişiler hakkında bilgi toplarlar. Sonrasında sosyal mühendislik tekniklerini kullanarak insanların zaaflarından faydalanıp istedikleri bilgilere ulaşmak için çalışma yaparlar.

12.3. Sosyal mühendislik saldırılarından korunmak için kişisel olarak dikkat edilmesi gereken hususlar şu şekildedir:

12.3.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.

12.3.2. Bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.

12.3.3. Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat edilmelidir.

12.3.4. Özellikle telefonda, e-Posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgileriniz kesinlikle paylaşılmamalıdır.

12.3.5. Parola kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-Posta ile parolanız hiç kimseyle paylaşılmamalıdır.

12.3.6. Oluşturulan dosyaya erişecek kişiler ve hakları, “bilmesi gereken” prensibine göre belirlenmeli ve erişim kontrol tedbirleri uygulanmalıdır.

12.3.7. Verilen erişim hakları belirli dönemlerde kontrol edilmelidir.

12.3.8. Çöpe atılan kâğıtlara dikkat edilmelidir. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtlar, kâğıt kırpma makinesinde imha edilmelidir.

12.3.9. Çok acele bilgi istendiği zaman istenen bilginin niteliğine göre teyit mekanizması kullanılmalıdır.

12.3.10. Bilgisayarınız yabancı bir kişiye kullandırılmamalıdır. Bu kişiler tarafından bilgisayarınıza takılacak olan USB depolama aygıtları ya da harici disklerden bilgisayarınıza zararlı yazılım bulaştırılabilir.

12.3.11. Hediye olarak verilen USB depolama aygıtları kullanmadan önce mutlaka virüs taramasından geçirilmelidir.

12.3.12. Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalar farklı seçilmelidir.

12.3.13. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmamalıdır.

12.3.14. Kuruma ait gizli bilgiler, resmi yazılar, çeşitli gelişmeler sosyal medya ortamında yayımlanmamalıdır.

12.3.15. Eğitimlerde sosyal medya güvenliği ile ilgili hususlara yer verilmelidir.

13. DESTEK POLİTİKA ve PROSEDÜRLER

13.1. Parola Politikası

13.1.1. Kurumların Bilgi Güvenliği Yetkililerince kendi kurumlarına özgü "Parola Politikası" oluşturulur ve Bilgi Güvenliği eğitiminde tüm çalışanlara duyurulur.

13.1.2. Parola politikaları belirlenirken, sistem ve uygulamaların, kullanıcıları asgari olarak aşağıdaki kurallara uygun parola kullanmaya zorlamaları sağlanır.

13.1.3. Parolalar en az 8 (sekiz) karakterden oluşur. Sistem yönetim işlemlerinde kullanılan parolaların (root, administrator, sysadmin vb.) en az 12 karakterden oluşması tavsiye edilir.

13.1.4. İçerisinde en az 1 (bir) tane büyük ve en az 1(bir) tane küçük harf bulunur.

13.1.5. İçerisinde en az 1 (bir) tane rakam bulunur.

13.1.6. İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !,?,A,+,$,#,&,/,{,*,- ,],=,...)

13.1.7. Kullanıcının son 3 (üç) parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenir.

13.1.8. Kullanıcı hesaplarına ait parolalar (örnek: HBYS, e-Posta, web, masaüstü bilgisayar vb.) en geç 6 (altı) ayda bir değiştirilmesi önerilir.

13.1.9. Sistem yöneticileri ayrıcalıklı işlemleri normal kullanıcı adı ve parola ile yapmaz. Bu maksatla farklı kullanıcı adı ve parola kullanılır.

13.1.10. Parolalar, e-Posta iletilerine veya herhangi bir elektronik forma eklenmez.

13.1.11. Parolalar gizli bilgi olarak muhafaza edilir. Kişiye özeldir ve her ne suretle olursa olsun başkaları ile paylaşılmaz. Kâğıtlara ya da elektronik ortamlara yazılamaz.

13.1.12. Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu bölümde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.

13.1.13. İnternet tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.

13.2. Yedekleme Politikası

13.2.1. Kurum bünyesindeki belirlenen bütün yedekleme işlemlerinden, yetkilendirilmiş sistem yöneticileri ve Birim yetkilileri sorumludur.

13.2.2. Bilgi sistemlerinde oluşabilecek hatalar karşısında sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için sistem ve kurumsal verilerin düzenli olarak yedeklenmesi sağlanmalıdır.

13.2.3. Sistem yöneticileri dâhilinde yedeğinin alınması gereken tüm veriler ve yedekleme konusunda yetkili çalışanlar da bu politikanın kapsamında yer almalıdır.

13.2.4. Bilgi sistemlerinde oluşabilecek beklenmedik durumlar karşısında, sistemlerin kesinti sürelerini ve olası veri kayıplarını en az düzeye indirmek için sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmelidir.

13.2.5. Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak da BACKUP Server ve Harici Disk ortamlarında yedekleri alınacaktır.

13.2.6. Yedekleme, bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili net sorumluluklar tanımlanmalıdır.

13.2.7. Kritik verilerin varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.

13.2.8. Oluşturulacak varlık envanterinde, hangi sistemlerde ne tür uygulamaların çalıştığı, yedeği alınacak dizin ve dosyalar, yetkili personel ve yetki seviyeleri yer almalıdır.

13.2.9. Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.

13.2.10. Yedek üniteleri üzerinde gereksiz yer işgal edilmemesi için kritiklik düzeyi düşük olan ve sürekli büyüyen log dosyaları yedekleme listesine dahil edilmemelidir.

13.2.11. Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.

13.2.12. Yeni sistem ve uygulamalar devreye alındığında yedekleme listeleri güncellenmelidir.

13.2.13. Yedekleme işlemi için yeterli sayı ve kapasitede yedekleme medyaları temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

13.2.14. Yedekleme medyaları acil durumlarda kullanılması gerekebileceğinden güvenilir ürünlerden seçilmesi ve düzenli periyotlarda test edilmesi gerekmektedir.

13.2.15. Geri yükleme prosedürlerinin düzenli olarak kontrol edilmesi ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dâhilinde tamamlanabileceğinden emin olunması gerekmektedir.

13.2.16. Yedekleme medyalarının bulundurulduğu ortamların fiziksel uygunluğu ve güvenliği sağlanmalı ve bilgi işlem odalarından faklı odalarda veya binalarda saklanmalıdır.

13.2.17. Yedekleme medyaları herhangi bir felaket anında etkilenmeyecek bir ortamda bulundurulması gerekmektedir.

13.3. İnternet ve E-Posta Kullanım Prosedürü

13.3.1. Elektronik Posta Güvenliği

13.3.1.1. Tüm Kullanıcılar kurumsal işlemlerde resmi olarak tahsis edilen @saglik.gov.tr uzantılı e-posta adresini kullanmak zorundadırlar.

13.3.1.2. Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.

13.3.1.3. İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.

13.3.1.4. Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.

13.3.1.5. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.

13.3.1.6. Internet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta adresi bu mesajlarda kullanılamaz. Ancak iş gereği üye olunması yararlı Internet haber grupları için yöneticisinin onayı alınarak kurumun sağladığı resmi e-posta adresi kullanılabilir.

13.3.1.7. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e- posta adresini yazamaz.

13.3.1.8. Personel KONU alanı boş bir e-posta mesajı göndermemelidir.

13.3.1.9. KONU alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.

13.3.1.10. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip ve/ya rar formatında) mesaja eklenecektir.

13.3.1.11. Bakanlık ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

13.3.1.12. Kullanıcı, Kurumun e-posta sistemi üzerinden taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.

13.3.1.13. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.

13.3.1.14. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yönetimine haber verilmelidir.

13.3.1.15. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt verilmemelidir.

13.3.1.16. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

13.3.1.17. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.

13.3.1.18. Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.

13.3.1.19. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Yönetimine haber vermelidir.

13.3.1.20. Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

13.3.1.21. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar Sistem Yönetimine haber verilmelidir.

13.3.1.22. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Sistem Yönetimine haber vermelidir.

13.3.2. İnternet Kullanımı

13.3.2.1. İnternet kullanımı, kurumdaki çalışan profillerine göre belirlenmelidir.

13.3.2.2. Normal kullanıcıların asgari olarak, Sağlık Bakanlığı uygulamaları, MEDULA ve sağlık hizmetlerinin yürütülebilmesi için ilgili sitelere erişim verilecektir. Bunların dışında, güvenilir olarak tanımlanan veya açılmasında sakınca bulunmayan sitelerin açılması (bankacılık, gazete vb.) sağlık müdürlüğü tarafından yönetilecektir.

13.3.2.3. Güvenlik duvarından geçmeyen internet erişim yöntemleri kesinlikle kullanılmamalıdır. (Adsl modem vb,) Bu konuda bakanlığın SBA (Sağlık Bilişim Ağı) devreleri kullanımıyla ilgili yönetmelikler uygulanacaktır.

13.3.2.4. Kurum içerisinde, kullanıcı profillerine göre internet erişimi sağlanacaktır. Güvenlik duvarı üzerinde uygulanan erişim kuralları çok fazla esnek olmamalıdır. Uygulanan kurallar, Güvenlik duvarı üzerindeki kategorilere göre ayrılacaktır.

13.3.2.5. Ses ve görüntü medyaları yasaklı olmalıdır veya bu trafiğe QoS uygulanmalıdır.

13.3.2.6. İnternet üzerinden eğitim isteklerinde, izin verilecek olan eğitim sadece Sağlık Bakanlığı tarafından yayınlanan eğitimler olmalıdır.

13.3.2.7. Özel erişim istekleri, S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi, İstatistik ve Bilgi İşlem Birimi'ne resmi yazı ile gerekçe yazılarak yapılmalıdır.

13.3.2.8. İnternet Erişimleri 5651 kanununa göre loglanmalıdır.

13.3.2.9. İnternet üzerinden kurumun verileri, üçüncü kişiler ile paylaşılmayacaktır.

13.3.2.10. Misafir erişimleri, sadece hotspot gibi çözümler kullanan tesislerde kullanılabilir. Misafir erişimleri ile kurum kaynakları aynı network de kesinlikle olmamalıdır. Aynı network üzerine verilen kablosuz erişimler kesinlikle kullanılmamalıdır.

13.4. Erişim Kontrol Politikası

13.4.1. Bilgi Sistemlerini kullanan tüm kurum personeli, hizmet sağlayıcı kurum dışı personel ve diğer üçüncü şahıslar Erişim Kontrol Talimatına uymakla yükümlüdürler.

13.4.2. Her kullanıcı, kendine ait hesabı kullanarak işlemlerini yürütür. Kullanıcılar kendi hesaplarının güvenliğini; şifrelerini saklayarak, başkalarının kendi hesabını kullanmasına izin vermeyerek ve gerektiğinde oturum kilitleme gibi özellikleri kullanarak korumakla yükümlüdürler.

13.4.3. İşten ayrılan personel için gerekli hesap kapatma, birim değiştiren kullanıcıların ise erişim haklarının düzenlemesi işlemleri hemen yapılmalıdır.

13.4.4. Gereksiz kullanıcı hesaplarının kontrol edilmesi ve kaldırılması işlemi ayda en az bir defa yapılmalıdır.

13.4.5. Kullanıcıların erişim hakları her değişiklikten sonra veya belirli aralıklarla gözden geçirilmelidir.

13.4.6. Ayrıcalıklı hesapların şifrelerinin belirli aralıklarla parola politikasına uygun şekilde değiştirilmesi sağlanır.

13.4.7. Kurum içi personelin internet yetki seviyeleri Bilgi İşlem Biriminin uygun görüşü ile Bilgi Güvenliği Alt Komisyonu tarafından belirlenir. En az 2 tür yetki seviyesi bulunmalıdır (Standart/Yetkili). Yetki talepleri imzalı olarak talep formu şeklinde alınmalıdır.

13.4.8. Sunuculara erişim için IP/SEC, SSL VPN veya RDP Protokolleri kullanılmalıdır. Bu protokollere açılan portlar ön tanımlı olmalıdır.

13.5. Uzaktan Erişim Prosedürü

13.5.1. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar (kablolu ve ya kablosuz), yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahip olmalıdır.

13.5.2. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN yada RDP teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlaması açısından önemlidir. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. protokollerinden birini içermelidir.

13.5.3. Uzaktan erişim güvenliği sıkı şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one-time passwordauthentication, örnek; Token Device) veya güçlü bir passphrase (uzun şifre) destekli public/privatekey sistemi kullanılması tavsiye edilmelidir. Daha fazlası için parola politikasına bakınız.

13.5.4. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

13.5.5. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

13.5.6. Mobile VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır

13.5.7. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.

13.5.8. Uzak erişimde yapılan tüm network hareketleri loglanmalıdır.

13.5.9. Uzak erişim için kullanılacak olan servisler ve protokoller ön tanımlı olmalıdır.

13.5.10. Uzak erişim verilecek olan kullanıcılara sözleşmesine göre günlük saatlik izinler verilmelidir. Sınırsız izin verilmekten kaçınılmalıdır.

13.5.11. VPN ile erişecek olan kullanıcı VPN Erişim formunu doldurmak zorundadır.

13.5.12. Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre limitlenmelidir.

13.6. Taşınabilir Ortam Yönetimi Prosedürü

13.6.1. Kuruma ait veriler, kişilere ait medyalar üzerinde saklanamaz. Verilerin bir taşınabilir ortama aktarılması ihtiyacı kaçınılmaz ise bu maksatla kuruma ait medyalar kullanılır.

13.6.2. Kuruma ait medyalar varlık envanteri içinde listelenir ve kimler tarafından kullanıldığı kayıt altına alınır. Görev devir teslimlerinde veya işten ayrılışlarda, kişilere teslim edilmiş olan medyaların iade edilmesi istenir veya ne şekilde sarf edildiği bilgisi sorgulanır.

13.6.3. ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL veriler, taşınabilir ortamda saklanamaz. Özellikle bu tür ortamlarda saklama zorunluluğu var ise ortamdaki veriler şifreli olarak saklanır.

13.6.4. Veriler çok kıymetli ise yedeklenen medya ortamı, doğal afet vb. tehditlere karşı önlem olmak üzere fiziksel olarak farklı bir yerde muhafaza edilir.

13.6.5. Yeni medya teknolojilerinin ortaya çıkması nedeniyle üç yıldan uzun süredir eski teknolojilerin kullanıldığı bir medya ortamında saklanan verilerin daha yeni bir medya ortamına taşınması tavsiye edilir.

13.6.6. Gizlilik derecesi taşıyan kurumsal verilerin saklandığı medya ortamları, kişisel (şahsın kendisine ait) bilgisayarlarda kullanılamaz. Bu tip veriler kişisel bilgisayarlarda işlenemez.

13.6.7. Tüm ortamlar üretici talimatında belirtildiği şekilde toz, nem vb. çevresel şartlardan etkilenmeyecek şekilde güvenli bir ortamda saklanır.

13.6.8. Elektronik medya da dâhil tüm taşınabilir ortamlar, kullanılmadığı zamanlarda içinde bulunan verilerin gizlilik derecesi dikkate alınarak fiziki güvenlik tedbirleri alınmış kasa, dolap, çekmece gibi ortamlarda saklanır.

13.7. Bilgi Saklama Ortamları Yok Etme Prosedürü

13.7.1. Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik veya fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dışı bırakılmasına karar verilen bilgi sistem cihazları ile ilgili kayıt silme işlemleri 2006/11545 sayılı Taşınır Mal Yönetmeliğinde belirtilen usul ve esaslar çerçevesince ilgili birimler ve komisyonlar tarafından yapılır.

13.7.2. Kaydı silinen bilgi sistem cihazlarına ait veri depolama üniteleri, içerisinde gizlilik dereceli bilgi bulundurma ihtimali nedeniyle usulüne uygun olarak imha edilir veya güvenli silme işlemi yapılır.

13.7.3. Kaydı silinen bilgisayarların sabit diskleri, ilgili teknik birimlerden destek alınmak suretiyle sökülür.

13.7.4. Sökülen sabit disklerden daha önce ilgili teknik birimler tarafından "onarımı mümkün değil" şeklinde rapor verilenler ile sağlam olmakla birlikte "yeniden kullanımı düşünülmeyen" cihazlar aşağıda belirtilen yöntemlerden biri ya da birkaçı birlikte kullanılmak suretiyle imha edilir:

13.7.5. De-manyetize Etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz hale getirilmesi suretiyle bozulması işlemidir.

13.7.6. Fiziksel Yok **Etme:** Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.

13.7.7. Disk imha işlemleri, bizzat disklerin sahipleri veya taşınır mal sorumlularının nezaretinde yapılır.

13.7.8. Ağ (anahtarlama cihazı, yönlendirici vb.) cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. Uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

13.7.9. Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa silme komutunu kullanarak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemi maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

13.7.10. Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp demanyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

13.7.11. Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

13.7.12. Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta ancak çoğunda yok etme komutu bulunmamaktadır. Ortamın Yok Edilmesi maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

13.7.13. Optikdiskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir.

13.7.14. Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre Ortamın Yok Edilmesi maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

13.7.15. Verikayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. Ortamın Yok Edilmesi maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

13.7.16. Kâğıt ve mikrofiş ortamlarındaki veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

13.7.17. Orijinalkâğıt formattan tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise bulundukları elektronik ortama göre Ortamın Yok Edilmesi maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

13.7.18. Arızalanan ya da bakıma gönderilen cihazlarda yer alan hassas verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

13.7.18.1. İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan verilerin (yedeklerinin alınarak) Ortamın Yok Edilmesi maddesinde belirtilen yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,

13.7.18.2. Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

13.7.18.3. Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, hassas verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

14. POLİTİKANIN YÜRÜRLÜĞE GİRİŞİ

İşbu "Bilgi Güvenliği Politikası" S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesince onaylanmasının ardından yürürlüğe girer ve tüm S.B.Ü Bursa Yüksek İhtisas Eğitim ve Araştırma Hastanesi personelince uyulması gereklidir.

15. POLİTİKANIN DUYURULMASI

İşbu "Bilgi Güvenliği Politikası" yürürlüğe girmesinin ardından tüm çalışanlara Bilgi Güvenliği Eğitiminde ve Kullanıcı adı ve Şife Talep Formlarında kişilere iletilir.

16. POLİTİKA GÖZDEN GEÇİRME KURALLARI

Bilgi Güvenliği Politikası, Bilgi Güvenliği Sorumluları tarafından periyodik olarak altı ayda bir kez, üst yönetim tarafından ise 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.

17. KAYNAKLAR/REFERANSLAR

- 02.05.2018 tarih ve 98813779.719.54 sayılı Bilgi Güvenliği Politikaları Yönergesi
- Bilgi Güvenliği Politikaları Kılavuzu Sürüm 2.0. (2018)
- ISO/IEC 27001, ISO 22301 standartları

HAZIRLAYAN	KONTROL EDEN		ONAYLAYAN
Bilgi İşlem Birim Personeli	Bilgi Güvenliği Yetkilisi	Bilgi Sistemleri Koordinatörü	Başhekim