1. BGYS POLİTİKASI

BGYS politikası, Almus Devlet Hastanesi bünyesinde yürütülen bilgi güvenliği yönetim sistemi çalışmalarının kapsamını, içeriğini, yöntemini, mensuplarını, görev ve sorumlulukları, uyulması gereken kuralları içeren bir dokümandır. Bu politikada tüm bölümleri ilgilendiren maddeler olduğu gibi sadece bazı bölümleri ilgilendiren maddeler de bulunmaktadır.

2. AMAÇ:

Bilgi güvenliği yönetim sisteminin amacı tüm bilgi varlıklarımızın gizliliği, bütünlüğü ve gerektiğinde yetkili kişilerce erişilebilirliğini sağlamaktır. Bilgi güvenliği sadece bilgi teknolojileri çalışanlarının sorumluluğunda değil eksiksiz tüm çalışanların katılımı ile başarılabilecek bir iştir. Ayrıca bilgi güvenliği sadece bilgi teknolojileri ile ilgili teknik önlemlerden oluşmaz. Fiziksel ve çevresel güvenlikten, insan kaynakları güvenliğine, iletişim ve haberleşme güvenliğinden, bilgi teknolojileri güvenliğine birçok konuda çeşitli kontrollerin risk yönetimi metoduyla seçilmesi uygulanması ve sürekli ölçülmesi demek olan bilgi güvenliği yönetim sistemi çalışmalarımızın genel özeti bu politikada verilmektedir. Uygulama detay bilgileri için sistem dokümantasyonuna, ilgili prosedürlere, rehberlere, planlara ve raporlara bakılmalıdır. Bu politika bilgi güvenliği politikası ve detaylı kullanım politikalarını da kapsayan bir üst dokümandır. Yönetim tarafından onaylanmış ve yayınlanmıştır. Bilgi güvenliği komitesi tarafından yılda en az bir kez olmak üzere düzenli olarak gözden geçirilmektedir.

3. KAPSAM:

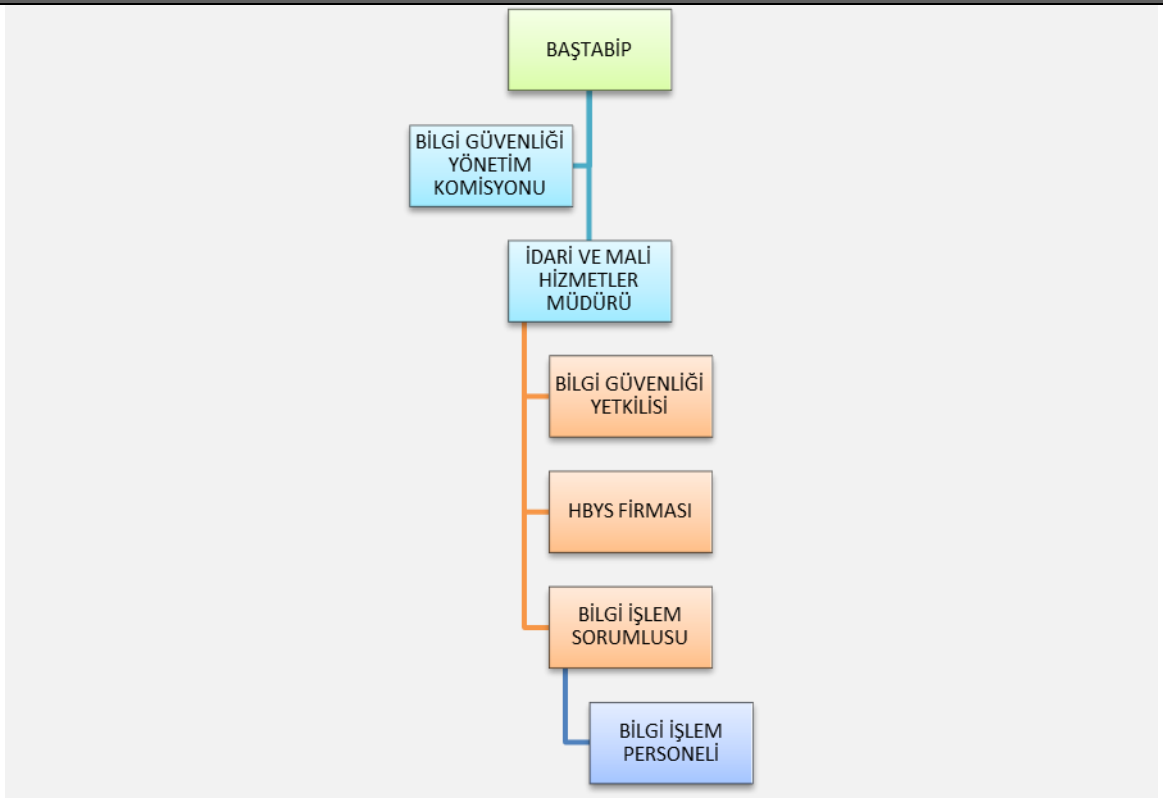
Bilgi güvenliği yönetim sistemleri politikası dökümanında yer alan kriterler Almus Devlet Hastanesi bilgi işlem alt yapısını kullanmakta olan tüm birimleri ,üçüncü taraf bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım ve donanım sağlayıcılarını kapsamaktadır.

4. HEDEF:

Bilgi Güvenliği Politikası, Almus Devlet Hastanesi çalışanlarına hastanenin güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini artırmak ve bu şekilde firmada oluşabilecek riskleri minimuma indirmek, hastanenin güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, teknik güvenlik kontrollerini uygulamak, hastanenin temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla hastanenin tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını korumayı hedefler.

5. BİLGİ GÜVENLİĞİ YAPISI VE ORGANİZASYONU:

Komisyon Başkanı	Dr.Gazi ATASEVEN	Baştabip
Üye	Eyüp SEFEROĞLU	İdari ve Mali Hiz. Müd.
Üye	Ender YERLİKAYA	Kalite Yönetim Direktörü
Üye	Hatice BAYIR	Hasta Hakları Sr./ Kalite Birimi
Üye	Ahmet ÇİĞDEM	Veri Giriş Kontrol İşletmeni
Üye	M.Mansur AYTAÇ	HBYS Firma Temsilcisi



6. TANIMLAR VE KISALTMALAR:

6.1. BGYS: Bilgi Güvenliği Yönetim Sistemi

6.2. Bilgi Güvenliği: Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkar edememe ve güvenilirlik gibi diğer özellikleri de kapsar.

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

6.4. 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, prosedürleri, prosesleri ve kaynakları içerir.

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

6.6. PUKÖ: Planla, Uygula, Kontrol Et, Önlem Al

7. GÖREV TANIMLARI:

7.1. BGYS KOMİSYON BAŞKANI GÖREV, YETKİ VE SORUMLULUKLARI:

7.1.1. Bilgi Güvenliği konularının altyapısını oluşturacak Çalışmaların yürütülebilmesi için gerekli komisyonları, çalışma gruplarını oluşturmak ve görev tanımlarını yapmak.

7.1.2. BGYS Komisyonuna başkanlık etmektir.

7.1.3. Almus Devlet Hastanesi bünyesinde verilen hizmetleri yasal mevzuat iş gerekleri ve gereksinimlerine uygun olarak uluslararası standartlar seviyesinde gerekliklerin yerine getirilmesi için çalışmaları yapmak.

7.1.4. BGYS Biriminden, BGYS Komisyonundan gelen istek ve talepleri değerlendirmek.

7.1.5. Referans alınan standartların temel gereksinimlerinden olan Bilgi Güvenliği Yönetim Sistemi gerekliliklerini oluşturmak ve yönetmek.

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

7.1.7. Çalışmaların yürütülebilmesi için Almus Devlet Hastanesi ve diğer birimleri ile taşra teşkilatı ve yüklenici firmalara yönelik gerekli tüm resmi yazışmaların yapılmasını, izinlerin alınmasını sağlamak ve onaylamak.

7.1.8. Projelerin yürütülebilmesi için gerekli olan yönetim hizmetleri çerçevesinde ihtiyaçların temin edilmesinin sağlanması

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

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

7.1.11. BGYS Birim personelinin kişisel gelişimleri için gerekli görülen eğitimleri düzenlemek ya da dış taraflarda düzenlenmiş eğitimlere gönderilmesini sağlamak konu ile ilgili tüm yasal izin ve finansal kaynağın sağlanmasını organize etmek.

7.2. BGYS KOMİSYONU GÖREV, YETKİ VE SORUMLULUKLAR:

7.2.1. BGYS Komisyonu BGYS Yönetim Temsilcisi tarafından oluşturulur, kurum yöneticisi tarafından onaylanır.

7.2.2. Baştabip bu komisyona başkanlık eder.

7.2.3. Bilgi Güvenliği konularının altyapısını oluşturacak projelerin yürütülebilmesi için gerekli onay vermek. Almus Devlet Hastanesinde uygulanması gereken Bilgi Güvenliği politikalarının geliştirilmesi için hazırlanan projelere katkı sunmak.

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

7.2.5. BGYS birimi tarafından hazırlanan projelerin gerekliliği olan, birim çalışanlarının, danışmanların ve yüklenici firma personellerinin farkındalık düzeylerinin artırılmasına yönelik organize edilen çalışmaların tüm tabana yayılması için gerekli desteği vermek.

7.3. BGYS ve YÖNETİM GÖZDEN GEÇİRME(YGG):

7.3.1. BGYS Biriminin ve üst yönetimin bilgi güvenliğinin uygunluğu, verimliliğini, risk yönetiminin işlevselliğini, tetkik sonuçlarını, düzeltici ve önleyici faaliyetleri ele aldığı yılda en az bir defa düzenlenen bir toplantıdır. Bu toplantıda yönetim risk kabul kriterlerini ve kaynak ihtiyaçlarını değerlendirir. Çalışmaların, risk değerlendirme ve işleme faaliyetlerinin verimliliğini inceler. bu toplantılarda standartlara göre girdi ve çıktılar toplantı tutanağı formu ile kayıt altına alınır.

8. BİLGİ HASSASİYETİ VE RİSKLER:

8.1. Bilgi Varlıklarımız: Almus Devlet Hastanesi bünyesinde tüm fiziki alanlardaki birimlerde üretilen bilgiler bilgi varlıklarımızı oluşturmaktadır. Masaüstü bilgisayarlar, laptoplar, CD ve DVD ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, e-mail, telefon vb.) yer alan tüm veriler ve sözlü olarak beyan edinilen bilgiler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

8.2. BİLGİ SINIFLANDIRMASI:

1

BİLGİ SINIFLANDIRMA KILAVUZU		SAKLANMA YERİ
Gizli	En kritik bilgilerdir, sadece yönetim kadrosunun erişimi vardır. Bu tür bilgilerin yetkisiz erişilmemesi, ifşa edilmemesi veya paylaşılmaması kurum açısından çok önemlidir. Gizlilik ön plandadır.	Hazırlayan kişi tarafından kontrol edilen ve kapalı odalarda bulunan kilitli dolaplar ve kişisel bilgisayarlar
İç Kullanım	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır.	Departmanın kilitli dolapları, Kişisel bilgisayarlar
Kişisel	Birim çalışanlarının kişisel çalışmaları ile ilgili bilgilerdir. Kurum işlevleri için yapılan kişisel çalışmalar burada tutulabilir. PC, Laptop veya Dolaplarda işle ilgili olmayan diğer kişisel bilgiler tutulamaz. Erişilebilirlik ön plandadır.	Çalışma masalarının kilitli çekmeceleri
Kuruma Açık	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın kilitli ortak dolapları
Halka Açık	Bu bilgiler T.C. Sağlık Bakanlığına bağlı tüm teşkilatına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Dolaplar ve dolap dışlarında

[1]Kurum içinde her çalışan bu sınıflandırma çerçevesinde kendi kullanımında olan veya kendi ürettiği bilgileri sınıflandırmalıdır. Bu sınıflandırmaya göre halka açık dokümanlar web sitesinde yayınlanan ve işlem için üçüncü taraflara verilen kağıt veya elektronik ortamdaki başvuru formu, duyurular vb. bilgilerdir.

9. BİLGİ GÜVENLİĞİ POLİTİKASI VE KILAVUZU:

T.C. Sağlık Bakanlığı tarafından yayımlanan Bilgi Güvenliği Politikaları Yönergesi ve kılavuzu çerçevesinde, Bilgi sistemleri tarafından yayınlanan bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır. Her çalışan bu dokümanda belirtilen kurallara uymakla sorumludur.

10. BİLGİ GÜVENLİĞİ SÖZLEŞMELERİ :

Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.

11. BİLGİ GÜVENLİĞİ EĞİTİMLERİ:

2018 yılı Almus Devlet Hastanesi hizmet içi eğitim planına Bilgi Güvenliği Farkındalık Eğitimleri de dahil edilmiştir. Bağlı Sağlık tesislerimiz bilgi güvenliği yetkililerine eğitim verilmiştir. Bilgi Güvenliği yetkililerinin kendi kurumları bünyesinde tüm personele eğitim vermesi sağlanacaktır. Birliğe bağlı kurum personeline farkındalık eğitimi verilmesi sağlanacaktır. Ayrıca web sayfası üzerinden yazılı olarak bilgilendirme dokümanları (.doc, .pdf, veya .pptx formatında) yayınlanacaktır.

12. İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ:

12.1. Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.

12.2. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.

12.3. ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(icra-izin kağıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.

12.4. Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.

12.5. İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) okunmayacak şekilde imha edilmelidir.

12.6. Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
12.7. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
12.8. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
12.9. Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.
12.10. 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.
12.11. Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yöneticisinehaber verilmelidir.
12.12. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.
12.13. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Sistem Yöneticisine haber verilmelidir.

13. İŞE BAŞLAYIŞ PROSEDÜRÜ:

13.1. İşe başlayan her personele (Kadrolu ve Sürekli İşçi Kadrosu dahil) bilgi güvenliği ve sosyal mühendislik zafiyetleri konularında eğitim verilmelidir. Bu eğitimler uyum eğitimlerine dahil edilmelidir.
13.2. Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir.
13.3. Kullanacağı bilgi sistemlerine yönelik kullanıcı adı ve şifreleri tanımlanmalıdır.
13.4. Ebys tanımlaması için ilgili personellere saglik.gov.tr uzantılı e-mail adresi tanımlanmalıdır. İl içi yer değişikliklerinde ise sistem üzerinden kurum/birim değişikliği tanımlaması yapılmalıdır.
13.5. Tüm personele kurum kimlik kartı çıkartılmalıdır.
13.6. Tüm personele tanıtıcı yaka kimlik kartı çıkartılmalıdır.

14. İŞTEN AYRILIŞ PROSEDÜRÜ

14.1. Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.
14.2. Kullandığı bilgi sistemlerine yönelik (Tsim, Çkys, Ebys vb.) kullanıcı adı ve şifreleri sistem yöneticisi tarafından pasif hale getirilmelidir.
14.3. Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
14.4. Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
14.5. Görevden ayrılan personel işten ayrılma onay formunu doldurarak bağlı bulunduğu kurumun insan kaynakları birimine teslim etmelidir.
14.6. İlgili form doldurulmadan personelin kurum ile ilişiği kesilmez.
14.7. Kurumdan ayrılan personele ait "İşten ayrılma onay formu" resmi yazı ile "Bilgi Güvenliği Yetkilisi" ne gönderilmelidir.

15. PAROLA GÜVENLİĞİ POLİTİKASI

15.1. Güvenliğin oluşturulacağı birim için kullanılan programlarda uygulanan parola standardı belirlenmeli, bu parola sistemi aşağıdaki unsurları içerecek standarda getirilmelidir.
15.2. Bilgi Güvenliği Yetkilisinin devreye girmesi ile parola standardı belirlenerek uygulanmaya başlanmalı, geliştirilerek aşağıdaki yapıya çekilmesi konusunda plan yapılmalıdır.
15.3. Parola en az 8 karakterden oluşmalıdır.
15.4. Harflerin yanı sıra, rakam ve "? @, !, #, %, +, -, *, %" gibi özel karakterler içermelidir.
15.5. Büyük ve küçük harfler bir arada kullanılmalıdır.

15.6. Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

15.7. Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır.

15.8. (Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi)

15.9. Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.

15.10. Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

15.11. Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.

15.12. Basit bir cümle ya da ifade içerisindeki belirli kelimeler özel karakter veya rakamlarla değiştirilerek güçlü bir parola elde edilebilir.

'B' yerine 8	**'Z' yerine 2**	**Örneğin** Balıkçıl-Kazak 8a11kç11-Ka2ak Solaryum! 501aryum!
I, i, L, l yerine 1	**'O' harfi yerine 0**	
'S' yerine 5 'G' yerine 6	**'g' yerine 9**	
'T', 't' yerine '+'	**'Ş', 'ş' yerine '$'**	**Örneğin** "Dün Kar Yağmış" : Dün*Yağm1$ "Şeker gibi bir soru sordu" : $eker~1?Sordu "Tek eksiğim bir güldü" : 1-ğim1:)dü "Yüzeysel bir soru eşittir eksi puan": %eysel1?=-puan
"kar", "yıldız" yerine '*'	**"dolar", "para" yerine '$'**	
"Soru" yerine '?'	**gibi" yerine '~'**	
"gül" yerine ':)'	**"eksi" yerine '-'**	
"bir", "tek" yerine 1	**"yüz", "yüzde" yerine '%'**	

16. BİLGİ KAYNAKLARI VE ATIK İMHA YÖNETİMİ POLİTİKASI

16.1. Bakanlık ve Bağlı Kuruluşlar kendi bünyelerinde oluşturacakları arşivden sorumludur. Evraklar idari ve hukuki hükümlere göre belirlenmiş Evrak Saklama Planı'na uygun olarak muhafaza edilmesi gerekmektedir.

16.2. 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.

16.3. İmha edilemeyecek evrak tanımına giren belgeler geri dönüşüme devirleri yapılmalıdır.

16.4. 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.

16.5. İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.

16.6. Uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır.

16.7. Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.

16.8. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.

16.9. Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir.

16.10. Hacimsel küçültme işlemi için parçalanmalıdır.

16.11. Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.

16.12. Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

17. İHLAL BİLDİRİM VE YÖNETİMİ

17.1. Bilginin gizlilik, bütünlük ve kullanılabilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

17.2. Bilgi güvenlik olayı raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

17.3. Güvenlik olayının oluşması durumunda olay anında raporlanmalıdır.

17.4. İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

17.5. Güvenlik ihlaline neden olan çalışanlar, üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.

17.6. Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği olayını önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine veya hizmet sağlayıcılarına mümkün olan en kısa sürede rapor edilir.

17.7. Bilgi sistemi arızaları ve hizmet kayıpları, zararlı kodlar, dos atakları, tamamlanmamış veya yanlış iş verisinden kaynaklanan hatalar, gizlilik ve bütünlük ihlâlleri, bilgi sistemlerinin yanlış kullanımı gibi farklı bilgi güvenliği olaylarını bertaraf edecek tedbirler alınır.

18. İNTERNET VE ELEKTRONİK POSTA GÜVENLİĞİ

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

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

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

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

18.5. İnternet 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.

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

18.7. E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir.

18.8. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.

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

18.10. 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.

18.11. Kullanıcı, kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yöneticisine haber verilmelidir.

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

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

18.14. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmemelidir.

18.15. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.(657 Sayılı DMK: Madde 7 – (Değişik: 12/5/1982 - 2670/2 md.))

18.16. 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.

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

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

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

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

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

19. MAL VE HİZMET ALIMLARI GÜVENLİĞİ

19.1. Mal ve hizmet alımlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmelidir.

19.2. Belirlenen güvenlik gereklerinin karşılanması için aşağıdaki maddelerin anlaşmaya eklenmesi hususu dikkate alınmalıdır:

19.2.1. Bilgi güvenliği politikası,

19.2.2. Bilgi, yazılım ve donanımı içeren kuruluşun bilgi varlıklarının korunması prosedürleri,

19.2.3. Gerekli fiziki koruma için kontrol ve mekanizmalar,

19.2.4. Kötü niyetli yazılımlara karşı koruma sağlamak için kontroller,

19.2.5. Varlıklarda oluşan herhangi bir değişimin tespiti için prosedürler; örneğin, bilgi, yazılım ve donanımda oluşan kayıp veya modifikasyon,

19.2.6. Anlaşma sırasında, sonrasında ya da zaman içinde kabul edilen bir noktada, bilgi ve varlıkların iade veya imha edildiğinin kontrolü,

19.2.7. Varlıklarla ilgili gizlilik, bütünlük, elverişlilik ve başka özellikleri,

19.2.8. Bilgilerin kopyalama ve ifşa kısıtlamaları ve gizlilik anlaşmalarının kullanımı,

19.2.9. Kullanıcı ve yönetici eğitimlerinin metodu, prosedürü ve güvenliği,

19.2.10. Bilgi güvenliği sorumluluğu ve sorunları için kullanıcı bilinci sağlama,

19.2.11. Donanım ve yazılım kurulumu ve bakımı ile ilgili sorumluluklar,

19.2.12. Açık bir raporlama yapısı ve anlaşılan raporlama formatı,

19.2.13. Değişim yönetimi sürecinin açıkça belirlenmesi,

19.2.14. Erişim yapması gereken üçüncü tarafın erişiminin nedenleri, gerekleri ve faydaları,

19.2.15. İzin verilen erişim yöntemleri, kullanıcı kimliği ve şifresi gibi tek ve benzersiz tanımlayıcı kullanımı ve kontrolü,

19.2.16. Kullanıcı erişimi ve ayrıcalıkları için bir yetkilendirme süreci,

19.2.17. Korumanın bir gerekliliği olarak mevcut hizmetleri kullanmaya yetkili kişilerin ve hakları ile ayrıcalıkları gibi kullanımları ile ilgili olan bir bilgilerin bir listesi,

19.2.18. Erişim haklarının iptal edilmesi veya sistemler arası bağlantı kesilmesi için süreç,

19.2.19. Sözleşme de belirtilen şartların ihlali olarak meydana gelen bilgi güvenliği ihlal olaylarının ve güvenlik ihlallerinin raporlanması, bildirimi ve incelenmesi için bir anlaşma,

19.2.20. Sağlanacak ürün veya hizmetin bir açıklaması ve güvenlik sınıflandırması ile kullanılabilir hale getirilmesini tanımlayan bir bilgi,

19.2.21. Hedef hizmet seviyesi ve kabul edilemez hizmet seviyesi,

19.2.22. Doğrulanabilir performans kriterlerinin tanımı, kriterlerin izlenmesi ve raporlanması,

19.2.23. Kuruluşun varlıkları ile ilgili herhangi bir faaliyetin izlenmesi ve geri alınması hakkı,

19.2.24. Üçüncü bir taraf tarafından yürütülen denetimler için sözleşmede belirtilen denetleme sorumlulukları hakkı ve denetçilerin yasal haklarının sıralanması,

19.2.25. Sorun çözümü için bir yükseltme sürecinin kurulması,

19.2.26. Bir kuruluşun iş öncelikleri ile uygun elverişlilik ve güvenilirlik de dahil olmak üzere hizmet sürekliliği gerekleri,

19.2.27. Anlaşmayla ilgili tarafların yükümlülükleri,
19.2.28. Hukuki konularla ilgili sorumlulukları ve yasal gereklerin nasıl karşılanması gerektiğinden emin olunmalıdır, (örneğin, veri koruma mevzuatı, anlaşma diğer ülkelerle ile işbirliği içeriyorsa özellikle farklı ulusal yargı sistemleri dikkate alınarak).
19.2.29. Fikri mülkiyet hakları (IPRs), telif hakkı ve herhangi bir ortak çalışmanın korunması,
19.2.30. Üçüncü tarafların alt yüklenicileri ile birlikte bağlılığı ve altyüklenicilere uygulanması gereken güvenlik kontrolleri,
19.2.31. Anlaşmaların yeniden müzakeresi ya da feshi için şartlar,
19.2.32. Taraflardan birinin anlaşmayı planlanan tarihten önce bitirmesi durumunda bir acil durum planı olmalıdır.
19.2.33. Kuruluş güvenlik gereklerinin değişmesi durumunda anlaşmaların yeniden müzakere edilmesi.
19.2.34. Varlık listeleri, lisanslar, anlaşmalar ve hakların geçerli belgeleri ve onlarla ilişkisi.

19.3. Farklı kuruluşlar ve farklı türdeki üçüncü taraflar arasında yapılan anlaşmalar önemli ölçüde değişebilir. Bu nedenle; anlaşmalar, belirlenen tüm riskleri ve güvenlik gereklerini içerecek şekilde yapılmalıdır. Gerektiğinde güvenlik yönetim planındaki gerekli kontroller ve prosedürler genişletilebilir.

19.4. 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.

19.5. Genellikle anlaşmaların esasları kuruluşlar tarafından geliştirilmiştir. Bazı durumlarda anlaşmaların üçüncü taraflarca geliştirilmesi ve kuruluşa empoze edilmesi durumu olabilir. Kuruluşlar, kendi yapılarına üçüncü taraflarca empoze edilecek anlaşmalarda kendi güvenliklerinin gereksiz yere etkilenmesini engeller.

20. SOSYAL MÜHENDİSLİK ZAAFİYETLERİ VE SOSYAL MEDYA GÜVENLİĞİ POLİTİKASI

20.1. SOSYAL MÜHENDİSLİK ZAFİYETLERİ

20.1.1. Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaaflarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendisler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanların zaaflarından faydalanıp, en çok etkileme ve ikna yöntemlerini kullanırlar.
20.1.2. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.
20.1.3. Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.
20.1.4. Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.
20.1.5. Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.
20.1.6. Şifre kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.
20.1.7. Oluşturulan dosyaya erişecek kişiler ve hakları "bilmesi gereken" prensibine göre belirlenmelidir.
20.1.8. Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
20.1.9. Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
20.1.10. Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.
20.1.11. Kazaa, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.

20.2. SOSYAL MEDYA GÜVENLİĞİ

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