1. AMAÇ

Nevşehir İl Sağlık Müdürlüğü'nde bilgi güvenliğinin amacı; dışarıdan ve/veya içeriden gelebilecek, kasıtlı veya kasıtsız olabilecek tüm tehditlerden korunması, kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve bilginin geniş çaplı tehditlerden korunmasını sağlamaktır.

Nevşehir İl Sağlık Müdürlüğü ve bağlı olduğu birimlerin sahip olduğu tüm bilgi varlıklarının gizliliğinin sağlanması, bütünlüğünün korunması ve sürekli erişilebilir bir bilgi yönetimi nihai amaçtır.

2. HEDEF

T.C. Sağlık Bakanlığı tarafından yayımlanan Bilgi Güvenliği Politikaları Yönergesi ve kılavuzu çerçevesinde, kurumda çalışan tüm personellerin bilgi güvenliği farkındalığını artırmak, iş sürekliliğini sağlamak, kurumsal riskleri en aza indirmek, kurumun güvenliği ile güvenilirliğini, çizdiği imajını korumaktır.

3. KAPSAM

Nevşehir İl Sağlık Müdürlüğü, tüm bağlı birimleri, sağlık çalışanları ile aşağıdaki varlık ve teknoloji kategorilerini kapsamaktadır.

- Bilgi,
- Donanım (kişisel bilgisayarlar, yazıcılar, sunucular),
- Yazılım (işletim sistemleri, geliştirilen uygulamalar, ofis programları),
- Haberleşme cihazları (telefonlar, hatlar, kablolar, modemler, anahtarlama cihazları),
- Dokümanlar (stratejik toplantıların tutanakları, sözleşmeler vb.),
- kurumun prestiji / imajı
- Kurum tarafından üretilen, kullanılan ve geliştirilen tüm verileri kapsar.
-

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

4. TANIMLAR

Nevşehir Sağlık Müdürlüğü: Nevşehir İl Sağlık Müdürlüğü, şubelerini ve tüm bağlı birimlerini ifade etmektedir.
Bağlı Birimler: İlçe Sağlık Müdürlükleri ile 112 Komuta Kontrol Merkezlerini ifade etmektedir.
Bilgi Güvenliği: Nevşehir İl Sağlık Müdürlüğü bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunmasıdır.
Varlık: Nevşehir İl Sağlık Müdürlüğü iş süreçleri için değeri olan, kaybı halinde işlerin aksayacağı, insan, yazılını, donanım, itibar, bilgi gibi unsurların tümüdür.
Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olmasıdır.
Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılmasıdır.
Erişilebilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an erişilebilir olmasıdır.

5. BİLGİ GÜVENLİĞİ ORGANİZASYONU

Nevşehir İl Sağlık Müdürlüğü tarafından, bilgi güvenliğinin iç organizasyonunun sağlanması için bilgi güvenliği konusunda uzmanlaşmış, bilgi sistemlerinin kapsamı göz önüne alınarak yeterli sayıda personelden oluşan, teknik, idari ve hukuki süreçlerde çalışmalarda bulunmak üzere ***"Bilgi Güvenliği Yönetim Komisyonu"*** oluşturulur.

Nevşehir İl Sağlık Müdürlüğü Bilgi Güvenliği Komisyonun görevleri;

- Bilgi güvenliği politika ve stratejilerini belirler, gerektiğinde Bilgi Güvenliği Politikaları Yönergesine bağlı olarak çalışma grupları tarafından hazırlanacak olan kılavuzlarla ilgili revizyon kararlarını verir,

- Bilgi güvenliği politikalarının uygulamasının etkinliğini gözden geçirir,
- Bilgi güvenliği faaliyetlerinin yürütülmesini yönlendirir,
- Bilgi güvenliği eğitimi ve farkındalığını sağlamak için plan ve programları hazırlar,
- Bilgi güvenliği faaliyetleri ve kontrollerinin tüm kurum ve kuruluşlarda koordine edilmesini sağlar.

5.1 Bilgi Güvenliği Komisyon Üyeleri

- Sağlık Bilgi Sistemlerinden Sorumlu Başkan
- Destek ve Personel Hizmetlerinden Sorumlu Başkan
- Bilgi Güvenliği Yetkilisi (İlgili Birim)
- Hukuk İşleri Sorumlusu
- Sağlık Bilgi Sistemleri Biriminden (2 kişi)
- İl Ambulans KKM Başhekimliği (1 kişi) olmak üzere 7 kişiden oluşur
-

6. BİLGİ GÜVENLİĞİ EĞİTİMLERİ

Kurum içi Bilgi Güvenliği farkındalığını artırmak ve gerekli güvenlik kurallarına uymak için eğitim planlaması yapılır ve gerekli eğitimler Müdürlük çalışanlarına verilir.

7. BİLGİ VARLIKLARIMIZ

Müdürlüğümüz ve bağlı birimleri bünyesinde yer alan tüm fiziki alanlarda bulunan birimlerin yapmış oldukları işlerde 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, yazılım ve programlar kurumumuz için bilgi varlığı olarak tanımlanmıştır.

BİLGİ SINIFLANDIRMA KILAVUZU		**SAKLANMA YERİ**
Gizli Bilgi	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 bilgisayarlarda
Iç Kullanım	Sadece birimlere özel bilgilerdir. Departman çalışanları dışında hiçbir 3. taraf kurumun veya kişinin görmemesi gereken bilgilerdir. Gizlilik ön plandadır.	Birimlerin kilitli dolapları, kişisel bilgisayarlarda
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 çekmecelerinde
Kuruma Açık	Bu bilgiler kurum çalışanlarının kullanımı içindir. Erişilebilirlik ve bütünlük ön plandadır. Departmanların kendi aralarında paylaştıkları bilgiler bu sınıfa girer.	Departmanın kilitli ortak dolaplarında
Halka Açık	Bu bilgiler T.C. Sağlık Bakanlığına bağlı tüm teşkilatına, tedarikçilere ve halka açık bilgilerdir. Bu bilgilerin erişilebilirliği önemlidir.	Dolaplar ve dolap dışlarında

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.

8. İNSAN KAYNAKLARI VE ZAAFİYETLERİ YÖNETİMİ

Nevşehir İl Sağlık Müdürlüğü ve bağlı birimlerinin uyması gereken prosedürler;

- Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır.
- ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında(izin kâğıdı gibi) ekranda bulunan kişisel bilgilerin diğer kişi veya kişilerce görülmesi engellenmelidir.
- Diğer kişi, birim veya kuruluşlardan telefonla ya da sözlü olarak çalışanlarla ilgili bilgi istenilmesi halinde hiçbir suretle bilgi verilmemelidir.
- İmha edilmesi gereken (müsvedde halini almış ya da iptal edilmiş yazılar vb.) kâğıt kesme makinesinde imha edilmelidir.
- Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
- Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
- Personel görevden ayrıldığında veya personelin görevi değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
- Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.
- Kurum son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar verir ve bu İşletim sistemine uygun yazılım donanım sistemlerinin kurulumunu temin eder.
- Kurum, bilgisayar başındaki kullanıcının doğru kullanıcı olup olmadığını tespit etmek için her bilgisayarda etki alanı kimlik doğrulamasını sağlamalıdır.
- Kurum, mevcut envanteri haricindeki donanımların kurum bilgisayarlarında kullanımını engellemelidir.
- Son kullanıcılar sistemlere, etki alanları dâhilinde kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanmalıdır.
- Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir.
- Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı loglanarak kayıt altına alınmalıdır.

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

- 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.
- Son kullanıcılar bilgisayarlarında ki ve sorumlusu oldukları cihazlarda ki bilgilerin yedeklerini kaybetmemek için verilerini bilgi sistemleri biriminin belirlemiş olduğu alana kaydetmelidir.
- Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir.
- Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde USB flash bellek ve/veya harici hard disk gibi Removable Media (taşınabilir medya) bırakmamalıdır.
- Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır.

9. PAROLA GÜVENLİĞİ

Nevşehir İl Sağlık Müdürlüğü olarak parola güvenliğini sağlamak için parola standardı belirlendi. Bu parola sistemi aşağıdaki unsurları içerecek standarda göre uygulanacaktır.

- En az 8 karakterden oluşmalıdır.
- Harflerin yanı sıra, rakam ve "?, !, #, %, +, *, %" gibi özel karakterler içermelidir.
- Büyük ve küçük harfler bir arada kullanılmalıdır.

Parola güvenliği ihlalinin önüne geçmek için aşağıdaki unsurlara dikkat edilmelidir.

- Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır.
- Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.
- Güçlü Parola Yöntemleri kullanılmalıdır.

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

- Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile 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 ‘E’ yerine 3	‘g’ yerine 9	

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

T, ’t’ yerine	'Ş', 'ş' yerine $	
‘kar’ , "yıldız" yerine	dolar ", "para" yerine '$'	Örneğin "Dün Kar Yağmış” “Dün*Yağml$” "Şeker gibi bir soru sordu- $eker~l?Sordu
‘Soru’ yerine ‘ ? ‘	"gibi" yerine ‘~’	
‘gül’ yerine’ ;)'	‘eksi ’ yerine ‘_’	
		“Tek eksiğim bir güldü” 1-ğim1:) dü “yüzeysel bir soru eşittir eksi puan”: %eyse1?=puan
‘bir', 'tek" yerine 1	‘yüz’, “yüzde" yerine ‘ %’	

10. İHLAL BİLDİRİM YÖNETİMİ

Bilgi Güvenliği Politikası kapsamında oluşturulmuş kural ve süreçleri ihlal eden personel, paydaş ve üçüncü taraflar hakkında adli ve idari yasal takibat başlatılarak ***Bilgi Güvenliği Disiplin Prosedürüne*** göre işlemler yapılacaktır.

Bilgi güvenliği ile ilgili olaylar derhal rapor edilmelidir. Olası bir tehdide meydan verecek bir zayıflığı tespit eden çalışanlar ***Bilgi Güvenliği İhlal Bildirim Formu*** ile bilgi işlem birimine başvuruda bulunurlar.

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

11. BİLGİ KAYNAKLARI ATIK VE İMHA YÖNETİMİ

Nevşehir İl Sağlık Müdürlüğü olarak kendi bünyemizde arşiv mevcuttur. Evraklar idari ve hukuki hükümlere göre belirlenmiş, Evrak Saklama Planı'na uygun olarak muhafaza edilmektedir.

Kurum olarak dikkat edilecek hususlar;

- 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.
- 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.
- İmha işlemi gerçekleşecek materyalin özellik ve cinsine göre imha edilecek lokasyon belirlenmelidir.
- İmha işlemi gerçekleşek materyalin uygun şekilde kırılması ve kırılma sürecinden önce veri ünitelerinin adet bilgisi alınmalıdır
- Yetkilendirilmiş personel tarafından imhası gerçekleşen atıklara data imha tutanağı düzenlenmesi ve bertaraf edilen ürünlerin seri numaraları ve adet bilgisinin data-imha tutanağı düzenlenmelidir.
- Tamamen tahrip edilememiş disk parçalarının delme, kesme makinaları ile kullanılamaz hale getirilmelidir. Hacimsel küçültme işlemi için parçalanmalıdır. Kırılan parçaların fiziksel muayene ile tamamen tahrip edilip edilmediğinin kontrolü yapılmalıdır.
- Son ürünlerin gruplar halinde fotoğraflanarak ilgili kişi ve/veya kuruma iletilmesi gereklidir.
- Çıkan metallerin sınıflarına göre ayrılarak, biriktirildikten sonra eritme tesislerine iletilmesi gerekmelidir.

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

12. İNTERNET VE ELEKTRONİK POSTA GÜVENLİĞİ

12.1 E-Posta Güvenlik Politikaları

Bu politikanın hazırlanmasındaki amaç; e-posta mesajlarını alma, gönderme, yönlendirme ve otomatik gönderme kullanımına ait Nevşehir İl Sağlık Müdürlüğü politikasını tanımlamaktadır. E-Posta politikası **BG.PO 3** kodlu dökümanda ayrıntılı olarak belirlenmiştir.

12.2.Sunucu Güvenlik Politikaları

Nevşehir İl Sağlık Müdürlüğüne hizmet veren tüm uygulama ve veri tabanı sunucuları kurumun veri merkezlerinde veya idarece uygun görülen güvenli fiziksel alanlarda konumlanmaktadır.

- Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları, anti virüs vb. koruma amaçlı yazılımlar sürekli güncellenmektedir.
- Sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmayıp sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklıdır.
- Kurumda bulunan sunucuların yönetiminden, ilgili sunucu yönetimi için yetkilendirilmiş personel sorumluğundadır. Görevinden ayrılan personelin tüm erişim yetkileri anında iptal edilmektedir.
- Sunucu kurulundan, konfigürasyonları, işletim sistemi yedeklemeleri, yamalan, güncellemeleri Sistem Yönetimi tarafından yapılmaktadır.
- Sunuculara ait bilgilerin yer aldığı envanter veri tabam oluşturulmalıdır. Bu veri tabanında, sunucuların isimleri, IP adresleri, yeri, ana görevi, üzerinde çalışan uygulamalar, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personelin isimleri ve telefon numaraları yer almalıdır. Bu tablo bir portal üzerinde bulundurulmalıdır.
- Sunucuların yazılım ve donanım bakımları, yetkili personel tarafından yapılmaktadır.
- Kuruma ait sistemler ve sunucular dışarıdan gelebilecek saldırılara karşı güncel teknolojilere sahip donanımsal FİREWALL (güvenlik duvarı) cihazları ile korunmalıdır.
- Kurum'da bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel sorumluluğundadır.
- Sunucu kurulundan, konfigürasyonları, işletim sistemi yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel tarafından yapılmaktadır.
- Sunucular üzerinde lisanslı yazılımlar kurulmaktadır.
- Sunucular fiziksel olarak korunmuş sistem odalarında bulunmaktadır.

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

•1 Kritik sistemlerde, uygulamalar kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.

> Kayıtlara çevrimiçi olarak en az 90(doksan) gün süreyle erişilmelidir.

> Günlük tape backuplar en az l(bir) ay saklanmalıdır.

> Haftalık tape backuplar en az l(bir) ay saklanmalıdır.

> Aylık fiili backuplar en az 6(altı) ay saklanmalıdır.

> Kayıtlar sunucu üzerinde tutulmalarının yanı sıra ayrı bir sunucuda da saklanmalıdır.

> Sunucu üzerinde zararlı yazılım (malware, spyvvare, hack programları, warez programları, vb.) çalıştırılmamalıdır.

> Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.

> Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.

> Denetimler, Bilgi İşlem grubu tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.

> Sunucuların bilgileri yetkilendirilmiş kişi tarafından tutulmalı ve güncellenmelidir.

• Sistem odalarına giriş ve çıkışlar kontrol edilmelidir.

13. MAL VE HİZMET ALIM GÜVENLİĞİ

• Kurum olarak mal ve hizmet altınlarında İlgili kanun, genelge, tebliğ ve yönetmeliklere aykırı olmayacak ve rekabete engel teşkil etmeyecek şekilde gerekli güvenlik düzenlemeleri Teknik Şartnameler de belirtilmektedir.

• Belirlenen güvenlik gereklerinin karşılanması için anlaşmaya eklenmesi gereken maddelerin hususunda dikkat edilmektedir.

• 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.

• Bilgi güvenliği yönetimi dış kaynaklı ise anlaşmalarda üçüncü tarafın güvenlik garantisinin yeterliliğini nasıl ele alındığı anlaşmada belirtilmelidir. Risk değerlendirmede tanımlandığı gibi, risklerdeki değişiklikleri belirlemek ve başa çıkmak için güvenliğin nasıl adapte edileceği ve sürdürüleceği ele alınmalıdır.

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

• 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 fesh edilmesi hakkına sahip olduğu için kuruluşun planlaması ve yönetimi önemlidir.
• 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.
• 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

13.1 Gizlilik Sözleşmeleri

Gizlilik veya ifşa etmeme anlaşmaları yasal olarak uygulanabilir terimleri kullanarak gizli bilgileri korumanın gerekliliğini ele almalıdır. Bu kapsamda Müdürlüğümüz tarafından çalışanlar için ***Personel Gizlilik Taahhütnamesi*** ve yüklenici kurumlarla ***Kurumsal Gizlilik Sözleşmesi*** yapılmalıdır.

• Bir kuruluşun güvenlik gereksinimlerine dayalı olarak, diğer unsurlarla bir gizlilik veya ifşa etmeme anlaşması gereklidir.
• Gizlilik ve ifşa etmeme anlaşmaları uygulandığı yerin geçerli tüm yasa ve yönetmeliklerine uygun olmalıdır.
• Gizlilik ve ifşa etmeme anlaşmaları için gerekler periyodik olarak veya gerekleri etkileyecek bir değişiklik olduğunda gözden geçirilmelidir.
• Gizlilik ve ifşa etmeme anlaşmaları kurumsal bilgileri korumalı ve imzalayanın, bilginin korunmasından, kullanılmasından ve ifşa edilmesinden yetkili ve sorumlu olduğunu belirtmelidir.
• Farklı koşullarda gizlilik ve ifşa etmeme anlaşmaları kuruluşun ihtiyaçları doğrultusunda farklı şekillerde kullanılmalıdır.

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

14. SOSYAL MÜHENDİSLİK ZAAFİYETLERİ VE SOSYAL MEDYA GÜVENLİĞİ

Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanmaktadır. Başka bir tanım ise; İnsanoğlunun zaaflarım 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.

Dikkat edilmesi gereken hususlar;

• Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunmalıdır.

• Kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edilmelidir.

• Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edilmelidir.

• Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde şifre gibi özel bilgileriniz paylaşılmamalıdır.

• Şifre kişiye özel bilgidir. Sistem yöneticiniz dahil telefonda veya e-posta ile şifrenizi paylaşmamalısınız. Sistem yöneticisi gerekli işlemi şifrenize ihtiyaç duymadan da yapabilmelidir.

• Oluşturulan dosyaya erişecek kişiler ve hakları "bilmesi gereken" prensibine göre belirlenmelidir.

• Erişecek kişilerin haklan yazma, okuma, değiştirme ve çalıştınna yetkileri göz önüne alınarak oluşturulmalıdır.

• Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.

• Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.

• Kazaa, emule gibi dosya paylaşım yazılımları kullanılmamalıdır.

14.1.Sosyal Medya Güvenliği

Kurumsal olarak personellerin veri güvenliği kapsamında dikkat etmesi gereken hususlar;

• Sosyal medya hesaplarına giriş için kullanılan şifreler ile kurum içinde kullanılan şifreler farklı olmalıdır.

• Kurum içi bilgiler sosyal medyada paylaşılmamalıdır.

• Kuruma ait hiçbir gizli bilgi, yazı sosyal medyada paylaşılmamalıdır.

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü

EKLER:

1. E-Posta Kullanım Politikası
2. Temiz Masa Temiz Ekran Politikası
3. Bilgi Güvenliği İhlal Olayları Prosedürü
4. Bilgi Güvenliği Disiplin Prosedürü
5. İşe Başlama ve İşten Ayrılma Prosedürü
6. Personel Gizlilik Taahhütnamesi
7. Kurumsal Gizlilik Sözleşmesi
8. İhlal Bildirim Formu
9. İşe başlama Formu
10. İşten ayrılma Formu
11. Toplantı Tutanak Formu

Hazırlayan	Onaylayan
Tayfun İMİR Bilişim Uzmanı Bilgi Güvenliği Yetkilisi	Dr. Rahim ÜNLÜBAY Nevşehir İl Sağlık Müdürü