	T.C. **SAĞLIK BAKANLIĞI** **ARDAHAN İL SAĞLIK MÜDÜRLÜĞÜ** **Varlık Ve Risk Yönetimi Politikası**	

Kodu	Yayın Tarihi	Revizyon No	Revizyon Tarihi	Sayfa Sayısı / Num.
BY.PR.07	29.10.2018	2	03.07.2019	1/5

1. AMAÇ

Bu politikanın amacı, T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesisleri/Birimleri için Standart envanter yönetimi bakış açısıyla, maddi değeri olan tüm varlıkların yürürlükteki Taşınır Mal Yönetmeliği ya da Kamu İdarelerine Ait Taşınmazların Kaydına İlişkin Yönetmelik uyarınca kayıt altına alınmasını ve ilgili yönetmeliklerde belirtilen usuller ile takibinin yapılmasını sağlamaktır.

2. KAPSAM

Bu politika, T.C Sağlık Bakanlığı Ardahan İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesislerinde görev yapan personeli kapsar.

3. TANIMLAR

Varlık: Kuruma ait tüm hassas bilgiler ve bu bilgilerin işlendiği ortamlar

BGYS: Bilgi Güvenliği Yönetim Sistemi

SBYS: Sağlık Bilgi Yönetim Sistemi

4. POLİTİKA METNİ

4.1. BGYS kapsamında varlık envanterine esas olan varlık kategorileri aşağıdaki gibidir.

İş Süreçleri: Kurumsal bilgi varlıklarının kullanıldığı, çeşitli vasıtalarla hassas bilgilerin yoğun olarak işlendiği iş süreçleri (hasta kabul, heyet işlemleri, tıbbi kayıt arşiv vb.)

Kurumsal Bilgi Varlıkları: Elektronik veya kâğıt ortamda tutulan hasta kayıtları, personel kayıt ve dosyaları, kurumsal evraklar, bilgisayarlarda saklanan ve kurum için değeri olan veriler, raporlar, listeler, çizimler, veri tabanları, veri tabanı yedekleri, faturalar, sözleşmeler, teklifler, telifler, lisanslar vb.

Yazılımlar: İşletim sistemleri, ofis uygulamaları, HBYS yazılımları, laboratuvar yazılımları, tıbbi görüntüleme yazılımları, kurumsal yazılımlar (EBYS, ÇKYS, KPS, HİTAP vb.) vb.

Fiziksel varlıklar: Sunucular, masaüstü bilgisayarlar, taşınabilir bilgisayarlar, depolama birimleri, yedekleme birimleri (kasetler, hard diskler vb.), aktif cihazlar (anahtarlama cihazı, güvenlik duvarı, yönlendirici, ağ erişim cihazı, anahtar, modem, erişim noktası vb), fakslar, fotokopiler, yazıcılar, santraller, telefonlar, evrak imha cihazları, ağa bağlı olarak çalışan veya ağa bağlanma arayüzleri olan tıbbi cihazlar vb.

İnsan Kaynakları: Çalışanlar

Altyapı: Yapısal ve elektrik kablolama altyapısı, UPS, jeneratör, iklimlendirme, giriş/çıkış kontrol sistemleri, kamera sistemleri, yangın, duman uyarı sistemleri, yangın söndürme sistemleri, destek teçhizatı vb.

Mekânlar: Yönetim ve hizmet odaları, sunucu odaları, arşiv odaları, tıbbi kayıt saklama odaları vb.

4.2. Varlık Envanterinin Tespiti

4.2.1. Varlık envanterinin belirlenmesi süreci, tek başına bir kişinin üstesinden gelebileceği bir faaliyet değildir. Çalışmanın bilgi güvenliği alt komisyonundan alınan yetki ve destekle, Kurumun üst yönetimi tarafından görevlendirilecek bir ekip vasıtasıyla yapılması gerekir. Ekibe kurumun

sınıflandırılmaya ihtiyaç duyulan diğer bilgi varlıklarının sınıflandırılması için de yukarıda belirtilen gizlilik dereceleri kullanılır. Bu varlıkların korunması ve erişim haklarının düzenlenmesi için alınacak tedbirler, yapılacak olan risk analiz neticesine göre belirlenir ve bu Kılavuz'un 6.1 (Erişim Kontrol Politikası) maddesi gereği hazırlanacak kurum erişim kontrol politika/prosedürü içerisinde ayrıntılı olarak açıklanır.

4.3.3. Gerek elektronik ortamda, gerekse basılı ortamda saklanan bilgilerin;

4.3.3.1. Bilgiye erişimin kayıt ve kontrol altına alınması,
4.3.3.2. İzinsiz kopyalamanın önlenmesi,
4.3.3.3. Elektronik veya basılı olarak depolama süresi ve koşullarının tanımlanması,
4.3.3.4. İletim hassasiyetinin belirlenmesi,
4.3.3.5. Gerektiğinde kanıt olarak kullanılmak üzere bütünlüğünün sağlanması,
4.3.3.6. İhtiyacın sonlanması durumunda imha edilmesi süreçlerinin tanımlanması için uygun şekil ve yöntemlerle etiketlenmesi gerekir.
4.3.3.7. Tasnif dışı bilgiler için etiketleme yapılmasına gerek yoktur.

4.3.4. Resmi yazı şeklinde olan belgelerin etiketlenmesi için yürürlükteki Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te belirtilen esaslar doğrultusunda hareket edilir.
4.3.5. Bu kapsamda;

4.3.5.1. Her sayfaya gizlilik dereceleri yazılır ve damgalanır.
4.3.5.2. Ekler de yazı ile aynı gizlilik derecesini taşır.
4.3.5.3. Gizlilik dereceli bütün yazılar, zaman zaman gizlilik derecelerinin yeniden değerlendirilmesi bakımından gözden geçirilir.
4.3.5.4. Gizlilik derecelerinin indirilip yüksetilmesi yazıyı yazan makamlarca yapıldığı gibi alan makamlarca da bu hususta teklif yapılabilir.
4.3.5.5. Gizlilik dereceli ve bilhassa kontrollü yazılarda kullanılan müsveddeler, karbon kâğıtları ve yanlış yazılar muhakkak imha edilir.
4.3.5.6. Gizlilik dereceli evrak, kâğıt sepetine bütün olarak atılmaz. Kâğıt kırpa makinaları kullanılmak suretiyle imha edilir.
4.3.5.7. Gizli ve özel gizlilik derecesini haiz evrak ve belgeler izinsiz olarak çoğaltılamaz.
4.3.5.8. Gizlilik derecesi taşıyan bilgileri veya belgeleri görevi dışında elde eden veya belgeleri görenler, bu bilgiyi ve belge içeriğini resmi görevlerinin gerektirdiği haller dışında açıklayamaz, çoğaltamaz veya paylaşamazlar. Bu tür bir bilgiyi 48 Bilgi Güvenliği Politikaları Kılavuzu edinenler durumu gecikmeksizin gizlilik derecesini veren makama bildirmek ve elde ettikleri belgeleri gecikmeksizin gizlilik derecesini veren makama teslim etmek zorundadırlar.

4.3.6. İlgili mevzuat tarafından verilen yetkiye dayanılarak Bakanlığımıza bağlı sağlık hizmet

bilgi güvenliği yetkilisinin başkanlık etmesi sağlanır.

4.2.2. Bilgi güvenliği yetkilisince, görevlendirilen ekip ile birlikte kurumun iş süreçleri analiz edilir. Başta taşınır mal sorumluları olmak üzere, teşkilatta yer alan diğer birimlerin birim sorumluları ile birlikte çalışılmak suretiyle, bilgi varlıklarının envanteri belirlenir.

4.2.3. Envanter belirleme işlemi bir kez yapılan ve tamamlanan bir iş değildir. Hazırlanan envanterin, farklı kaynaklardan (Çekirdek Kaynak Yönetim Sistemi/ ÇKYS, Malzeme Kaynak Yönetim Sistemi/SBYS vb.) doğruluğunun kontrol edilmesi ve sürekli olarak güncel tutulması gerekir. Envanter tespit süreci, bir döngü şeklinde, periyodik olarak yapılması gereken bir faaliyettir.

4.2.4. Varlık envanteri, sadece fiziksel varlıklar veya bilgi sistem teçhizatından oluşmaz. Varlıklar belirlenirken, başta hassas bilgilerin işlendiği kritik iş süreçleri olmak üzere, bu süreçlere konu olan tüm kurumsal bilgi varlıklarının ortaya çıkarılması gerekir. (Örneğin İK Birimleri ile yapılacak varlık envanter çalışmasında, kurum çalışanlarının kâğıt ortamda saklanan şahsi dosyaları kurum için korunması gereken önemli bir varlık olarak gündeme getirilmişse, bu kaydın mutlaka varlık envanterinde yer alması gerekir. Eğer bu kayıt, varlık envanterine girmez ise; onunla ilgili riskler ve koruma önlemleri de tespit edilemeyecek, dolayısı ile tesis etmiş olduğumuz BGYS'nin bir bölümü eksik veya hatalı olacaktır.)

4.2.5. Envanterde yer alan her bir varlık için "varlık sahibi" belirlenir. Varlık sahibi gerçek bir kişi olabileceği gibi, bir birim ya da kurum da olabilir.

4.2.6. Varlık sahiplerince Kılavuz'un 4.3 (Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi) maddesinde belirtilen bilgi sınıflandırma kuralları uyarınca, her varlığa bir gizlilik derecesi atanır. Gizlilik derecesi yüksek varlıklar için taşıdığı yüksek risk değeri nedeniyle daha sıkı güvenlik tedbirleri uygulanır.

4.2.7. Kurum bilgi varlıklarının tespitinde örneği KLVZ-EK-05 Kurum Bilgi Varlıkları Envanter Çizelgesi kullanılabilir veya kurumun kendi özelliklerine uygun bir başka çizelge geliştirilebilir.

4.2.8. Varlık sahipleri;

4.2.8.1. Varlıklarını envantere doğru olarak kaydettirmekten,

4.2.8.2. Varlıklarına uygun gizlilik derecesi ve varlık değeri atamaktan, varlıklarının uygun şekilde korunmasından,

4.2.8.3. Varlıklara erişecek kişi veya süreçleri için erişim izinlerini planlamaktan, bunlarla ilgili kararları vermekten,

4.2.8.4. Varlıkların silinmesi ya da imha edilmesinde uygun işlemlerin uygulanmasından sorumludur.

4.2.9. Çalışanlar ve dış tarafların kullanıcıları; iş akitleri, sözleşmeleri veya anlaşmaları sona erdiğinde, ellerinde olan tüm kurumsal varlıkları iade etmekle mükelleftir.

4.3. Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi

4.3.1. Kurum bilgi varlıkları, içerdikleri verilerin hassasiyeti, kurum için taşıdıkları önem ve yasal zorunluluklar dikkate alınarak uygun bir şekilde sınıflandırılır/ gizlilik derecesi verilir.

4.3.2. Bilgi varlıklarına (resmi yazılar dâhil) verilecek gizlilik dereceleri için 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe giren "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar" dikkate alınır. Buna göre;

4.3.2.1. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda kişi güvenliği veya milli güvenlik açısından saygınlık ve çıkarlarımıza hayati derecede zararlar verebilecek, yabancı bir devlet için faydalar temin edebilecek ve güvenlik bakımından olağanüstü sonuçlar doğurabilecek bilgiler "çok gizli",

4.3.2.2. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından, saygınlık ve çıkarlarımıza büyük zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek özellikler taşıyan bilgiler "gizli",

4.3.2.3. İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından saygınlık ve menfaatlere zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek bilgiler "özel",

4.3.2.4. İçerdiği bilgi itibarıyla ÇOK GİZLİ, GİZLİ veya ÖZEL gizlilik dereceleriyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi durumunda gerçek ve tüzel kişilerin itibarını sarsacak bilgiler "hizmete özel" olarak sınıflandırılır.

4.3.2.5. Çok gizli gizlilik dereceli evrak ve dokümanlar, Kurumun en üst düzey yöneticisi tarafından belirlenen ve yazılı olarak görevlendirilen kişi veya kişiler tarafından hazırlanır ve özel usullere göre dağıtımı yapılır. Bu tip evrak ve dokümanlar korumalı odalarda, kasa, çelik masa veya diğer tipte çelik dolaplar içinde muhafaza edilir.

4.3.2.6. Gizli, özel ve hizmete özel evrakların gizlilik derecesi, yazıyı hazırlayan makam tarafından tayin edilir. Gizli ve özel evraklar kilitli çelik dolaplarda, hizmete özel evraklar ise masa gözlerinde kilitli olmak şartıyla muhafaza edilir.

4.3.2.7. Yukarıda sıralanan gizlilik derecelerinden hiçbirisi ile sınıflandırılmayan ve özel bir koruma gerektirmeyen evrak ve dokümanlar, "tasnif dışı" olarak kabul edilir.

4.3.2.8. Tasnif dışı bir gizlilik derecesi olmayıp, evrakın yukarıda sıralanan gizlilik derecelerinden hiç biri ile sınıflandırılmamış olduğunu belirtir. Tasnif dışı belgeler için herhangi bir erişim kısıtlaması yoktur.

4.3.2.9. Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, elektronik ortamda hazırlanması ve dağıtılması ile ilgili hususlar için Sağlık Bakanlığı Elektronik Belge Yönetim Sistemi Yönergesi'nde belirtilen kurallar uygulanır.

4.3.2.10. Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, kâğıt ortamda hazırlanması ve manuel (elektronik olmayan) yöntemlerle dağıtılması için Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te belirtilen kurallar uygulanır.

4.3.2.11. Resmi yazı şeklinde olmayan ancak içerdikleri bilgilerin hassasiyeti açısından

sunucuları tarafından işlenen kişisel sağlık verileri; verinin ait olduğu kişi, ne maksatla istendiği vb. özel durumlar da dikkate alınmak suretiyle yukarıda tanımlanan gizlilik derecelerinden en az "ÖZEL" gizlilik derecesi ile etiketlenir.

4.3.7. Sağlık verilerinin korunmasına yönelik risk analizi yapılırken, kişisel verilerin hassasiyeti ve kanuna aykırı bir şekilde ifşası halinde uygulanacak ağır idari ve cezai yaptırımlar nedeniyle en üst düzeyde özen gösterilir.

5. YAPTIRIM

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla Bilgi Güvenliği Disiplin Prosedürü dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.

Hazırlayan	Kontrol Eden	Onaylayan
Oğuz KARABAĞ Bilgi Güvenliği Yetkilisi	Uz. Dr. Nejat AKIN Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Op. Dr. Erkan ÖZDEMİR İl Sağlık Müdürü