1. AMAÇ

Bu doküman, T.C. Sağlık Bakanlığı ..... Hastanesi bünyesinde işe başlama ve işten ayrılma süreçlerinde uyulması gereken süreçleri ifade eder.

2. KAPSAM

..... Hastanesi Bilgi Güvenliği Prosedürü dokümanının KAPSAM maddesinde yer alan fiziki tanımlı alanlarda faaliyet gösteren tüm birimler ve tüm insan kaynaklarıdır.

3. SORUMLULAR

..... Hastanesi bünyesinde faaliyet gösteren tüm personel sorumludur, bu sürecin işletilmesinden ise Bilgi Güvenliği Ekibi ve ..... Hastanesi makamı sorumludur.

4. UYGULAMA

4.1. İNSAN KAYNAKLARI VE SON KULLANICI GÜVENLİĞİ

4.1.1. İşe alma görevi ..... Hastanesi tarafından yürütülmüyorsa, bu prosedürden sorumlu değildir ve tüm iş ve işleyişler İl sağlık Müdürlüğü tarafından yapılır.

4.1.2. İşe alma görevi hastane tarafından yapılacaksa;

4.1.2.1. İşe Alma Öncesinde Yapılacak Kontroller

a) 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 (tarama yapılır) edilir, bilgi güvenliği ve sosyal mühendislik zafiyetleri konularında eğitim verilmelidir. Tüm bu eğitimler uyum eğitimlerine dâhil edilmelidir.

b) 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.

c) 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.

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

e) İşe başlamadan önce tüm personel ile Personel Gizlilik Sözleşmesi imzalanacağı ilgili taraflara bildirilir. İmzalatılacak sözleşmelerin içeriği ve ilgililerin yükümlülükleri detaylı olarak açıklanır. Sözleşmelerde kişilerin ve idarenin bilgi güvenliği sorumlulukları açıkça belirtilir. Bu işlem için PERSONEL GİZLİLİK SÖZLEŞMESİ imzalanır.

f) 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.

4.1.2.2. Çalışma Esnasında Uygulanacak Kontroller

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

b) İşe yeni başlayan personelin başlayış işlemlerinin eksiksiz olarak yapılmasını sağlamak için "işe başlama formu" hazırlanır ve uygulanır.

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

d) İşe başlama formunda bilgi güvenliği ile ilgili olarak personel giriş kartı çıkarılması ve bina/tesislere erişim için verilecek yetkiler, bilgi sistemlerine erişim için hesap açılması ve verilecek yetkiler (ePosta, elektronik belge yönetim sistemi, hastane bilgi yönetim sistemi, insan kaynakları sistemi gibi), bilgi güvenliği farkındalık eğitimi, oryantasyon eğitimi, gizlilik sözleşmesi imzalatılması gibi hususlar mutlaka yer alır. Örnek olarak İşe Başlama Formu kullanılabilir.

e) Bilgi güvenliği ile ilgili beklentiler ve sorumluluklar, çalışanların görev tanımlarına eklenmelidir.

f) Çalışanların kuruluşun bilgi güvenliği politikasına uyumu sürekli izlenmelidir

g) Tüm çalışanların bilgi güvenliği farkındalık eğitimi programlarına katılmaları sağlanmalıdır.

h) Bilgi güvenliği ihlaline neden olan kişilere yapılacak işlemler (disiplin prosedürü) önceden belirlenir ve kişilere duyurulur. İhlal oluştuğunda, disiplin prosedüründe yazan hususlar uygulanır.

i) Bilgi güvenliği ihlali yapan personele uygulanan yaptırımlar (kişi kimlik bilgisi verilmeden) diğer çalışanlara duyurulur ve onlar için de örnek teşkil etmesi sağlanır.

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

a) 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.

b) 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.

c) İşten ayrılan veya görev değişikliği yapan personelin ayrılma işlemlerinin eksiksiz olarak yapılmasını sağlamak için "işten ayrılma formu" hazırlanır ve uygulanır. Örnek olarak İşten Ayrılma Formu kullanılabilir.

d) Formda yazan işlemlerin tam olarak uygulanmasını sağlamaktan, kişinin bağlı bulunduğu birim yöneticisi ile insan kaynakları birimi müştereken sorumludur.

e) 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.

f) 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.

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

h) Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.

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

j) Mümkünse ayrılan personel ile yeni katılan personelin geçici bir süre birlikte görev yapması sağlanır.

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

l) İlgili form doldurulmadan personelin kurum ile ilişiği kesilmez.