|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ** | | | C:\Users\olympos\Desktop\antalya_ism_logo 800x600.jpg |
| **Kodu** | **Yayınlama tarihi** | **Revizyon Tarihi** | **Revizyon No** | **Sayfa** |
| **BG.PR.01** | **20.10.2015** | **20.10.2015** |  | **1/3** |

# Amaç:

Antalya İl Sağlık Müdürlüğü ve Müdürlüğe bağlı sağlık tesislerinde insan kaynakları zafiyetleri yönetimi kapsamında personelin kullandığı bilgi güvenliğini gerektiren unsurları tespit etmek, personelin göreve başlama ve görevden ayrılma süreçlerinde uyması gereken prosedürü belirlemek.

# Kapsam

Bu politika T.C. Sağlık Bakanlığı Antalya İl Sağlık Müdürlüğü ve Müdürlüğe bağlı kurum personeli için yazılmış olup, güvenlik sorumlulukları olan tüm departman ve çalışanlar için geçerlidir.

# Politika Metni:

# İnsan Kaynakları ve Zafiyetleri Yönetimi

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

# Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir.

* ÇKYS üzerinden kişiyle ilgili bir işlem yapıldığında (izin kağıdı 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.) kağıt kesme makinasında imha edilmelidir.
* Tüm çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.
* Görevden ayrılan personel, zimmetinde bulunan malzemeleri teslim etmelidir.
* Personel görevden ayrıldığında veya personelin görev yeri değiştiğinde elindeki bilgi ve belgeleri teslim etmelidir.
* Görevden ayrılan personelin kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ** | | | C:\Users\olympos\Desktop\antalya_ism_logo 800x600.jpg |
| **Kodu** | **Yayınlama tarihi** | **Revizyon Tarihi** | **Revizyon No** | **Sayfa** |
| **BG.PR.02** | **20.10.2015** | **20.10.2015** |  | **2/3** |

# Son Kullanıcı Güvenliği

* 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 yetkileri, içinde bulundukları grup politikasına göre belirlenmelidir.
* Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı loglanarak kayıt altına alınmalıdır.
* 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 bilgisayarlarındaki ve sorumlusu oldukları cihazlardaki bilgilerin düzenli olarak yedeklerini almalıdır. Bilgisayar dosyaları (.xlsx, docx, pptx vb.) isteğe bağlı olarak bilgisayarın hard diskine, flash diske veya CD ortamına alınıp yedeklenip saklanabilir.
* Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir. Bu işlem Windows işletim sisteminde Windows + L tuşları yardımıyla kolaylıkla yapılabilmektedir.
* 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.
* Kullanıcı bilgisayarlarında, güncel anti virüs bulunmalıdır.
* Kurum, son kullanıcı güvenliğine dair oluşturulmuş grup politikalarını, etki alanı üzerinden kullanıcı onayı olmaksızın uygulamalıdır.
* Kurum, son kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişikleri merkezi grup politikalarıyla engellemelidir.
* Kullanıcılarına yeni parolaları bildirilirken sms gibi daha güvenli yöntemler kullanılmalıdır.
* Temiz masa, temiz ekran ilkesi benimsenmeli ve hayata geçirilmelidir.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **İNSAN KAYNAKLARI VE ZAFİYETLERİ YÖNETİMİ** | | | C:\Users\olympos\Desktop\antalya_ism_logo 800x600.jpg |
| **Kodu** | **Yayınlama tarihi** | **Revizyon Tarihi** | **Revizyon No** | **Sayfa** |
| **BG.PR.02** | **20.10.2015** | **20.10.2015** |  | **3/3** |

# Sosyal Mühendislik Zaafiyetleri ve Sosyal Medya Güvenliği

* Taşınan ve işlenen 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 hakları yazma, okuma, değiştirme ve çalıştırma 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, Ares gibi Dosya paylaşım yazılımları kullanılmamalıdır.
* 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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **HAZIRLAYAN**  **(Bilgi Güvenliği Komisyonu)** | | | | | | | |
| *Komisyon Başkanı*  Bülent YURTERİ  Şube Müdürü | *Başkan Yardımcısı*  Ersin HOŞER  V.H.K.İ | *Üye*  Okşan Duru ÖZDAĞ  Doktor | | | *Üye*  Demet KILIÇ  Avukat | *Üye*  Osman ÜNAY  Bilgisayar Mühendisi | *Üye*  K. Erkan AKKUŞ  Bilgisayar Mühendisi |
|  |  |  | | |  |  |  |
| *Üye (Eğitimci)*  Ünal GÖKÇE  Sağlık Memuru | *Bilgi Güvenliği Yetkilisi*  Özgür AYDIN  Programcı | *Üye*  Fethi ÇELİK  Programcı | | | *Üye*  İsmail ÇİFTÇİ  Bilgisayar İşletmeni | *Üye*  Okkan KARADAŞ  Tıbbi Sektreter |  |
|  |  | |  |  |  |  | |

**O N A Y**

…/…/2015

Dr. Ünal HÜLÜR

İl Sağlık Müdürü