İNTERNET VE E-POSTA KULLANIM PROSEDÜRÜ

1.AMAÇ: Kurum personelinin internet kullanımı ve e-posta mesajlarında alma, gönderme, yönlendirme ve otomatik gönderme kullanım politikasını tanımlamaktır.

2.KAPSAM: Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumlar bünyesinde kurumun sağladığı resmi internet ve resmi e-posta kullanım işlemlerini kapsar.

3.KISALTMALAR:

BGYS: Bilgi Güvenliği Yönetim Sistemi

4.TANIMLAR:

SBA(Sağlık Bilişim Ağı): Sağlık sektöründe yer alan kurum ve kuruluşların kaynaklarını ve sağlıkla ilgili verileri ortak kullanabilmeleri, veri iletişimini güvenilir ve hızlı bir kanal üzerinden yapabilmeleri amacıyla ülke genelinde oluşturulan özel ağdır.

Spam: İsteğimiz olmadan bize gönderilen reklam içerikli maillerdir.

5.SORUMLULAR:

Hatay İl Sağlık Müdürlüğünde faaliyet gösteren tüm personel sorumludur, bu sürecin işletilmesinden ise BGYS Komisyonu ve Hatay İl Sağlık Müdürlüğü makamı sorumludur.

6.FAALİYET AKIŞI:

6.1.İnternet Güvenliği

6.1.1. Müdürlüğümüz ve bağlı birimlerinde (Aile Sağlığı Merkezleri hariç) internet erişimi Sağlık Bilişim Ağı (SBA) üzerinden yapılır. Sağlık Bilişim Ağı (SBA), Sağlık Bakanlığı ve bağlı kuruluşlarının veri iletişiminin güvenilir ve hızlı bir kanal üzerinden sağlanması amacıyla tesis edilen, KamuNet'e bağlı olarak çalışan, internet erişiminin kontrollü olarak sağlandığı kapalı bir ağdır.

6.1.2. Kurumsal kaynakların etkin olarak kullanılması, 5651 sayılı kanundan kaynaklanan uyum zorunlulukları, veri güvenliğinin sağlanması, zararlı içerik ve yazılımlardan korunma vb. maksatlarla internet erişimi kısıtlamaları yapılabilir.

6.1.3. Basın yayın organlarını takip ederek idareye raporlamakla sorumlu personel haricindeki tüm personelin dizi, film ve TV erişimlerinin kapatılır.

6.1.4. Kurum sosyal medya hesaplarını yönetmekle sorumlu personel dışındaki tüm personelin Facebook, Twitter, İnstagram vb. uygulamalara erişimlerinin engellenir veya bant genişliği sınırlaması yapılır.

6.1.5. Youtube, Vimeo, Dailymotion gibi platformlarda erişimlerle ilgili olarak sadece ihtiyaç duyan personele izin verilir, bu yapılamıyorsa bu platformlara erişimlere bant genişliği sınırlaması uygulanır.

6.1.6.İnternette girdiğimiz sitelerin güvenli olup olmadığına dikkat edilmeli, özellikle varez,serial,crack,adult içerikli sitelerden bilgisayarımıza virüs bulaşma ihtimali çok yüksektir.

6.1.7. Gezdiğimiz sitelerde bir yere tıkladığımızda sürekli yeni sayfalar (popup) açılıyor, şunu yapmak için buraya tıklayın gibi şüpheli ifadeler bulunuyor veya yönlendirme yapılıyor ise o siteyi hemen kapatmamız gerekir.

6.1.8.Girdiğiniz sitelerde veya e-posta adresinize gelen iletilerde ilgili linke tıklamanız halinde para kazanmayı vadeden, ödül vermeyi v.b durumlar var ise bu sitelere girilmemeli, linklere tıklanmamalıdır.

6.1.9.Sosyal medya uygulamalarından (whatsapp,facebook,twitterv.b.) arkadaşlarınızdan beklenmedik zamanlarda gelen dosya gönderileri açılmamalı.Para v.b talepler geldiğinde güvenilmemelidir.

6.1.10.İnternet üzerinden dosya, müzik, video indirirken hangi siteden indirildiğine dikkat edilmeli ve indirdiğimiz dosyayı virüs taramasından geçirmeden açılmamamlıdır.

6.1.11.İnternetten kimlik bilgileriniz (kimlik avı) çalınabilir. Bu nedenle, banka, e-devlet v.b sitelere bilgilerinizi girerken ilgili sitede belirlenmiş kurallara göre bilgiler girilmeli, beni hatırla seçeneği işaretlenmemelidir. Forum siteleri v.b sitelere üye olurken gerçek bilgiler kullanılmamalıdır.
6.1.12.Kablosuz ağlara mutlaka şifre koyulmalı ve şifreler belirli aralıklarla değiştirilmelidir.
6.1.13.Bilgisayarlarda anti-virüs programı bulunmalı ve sürekli güncel tutulmalıdır.
6.1.14.İnternetten on-line alışveriş için güvenilir, herkesçe bilinen siteler tercih edilmelidir.

6.2 Elektronik Posta Güvenliği

6.2.1.Müdürlük ve bağlı birimlerinde görev yapan personel tarafından görevleri gereği yürütülen kurumsal iş ve işlemlerde, *@saglik.gov.tr uzantılı kurumsal veya tüzel e-posta hesabı kullanılır. Kurumsal iş ve işlemler, kişilerin özel işleri için (Gmail, Hotmail gibi) internet hizmet sağlayıcılarından alınan hesaplar üzerinden yürütülmez.
6.2.2.*@saglik.gov.tr uzantılı kurumsal veya tüzel e-posta adreslerinden en fazla 25mb dosya gönderilebilir, aynı anda en fazla 100 kullanıcıya ileti gönderilebilir, adres açıldığında kullanıcıya 1 GB kullanım alanı verilir, 1 yıl boyunca hiç kullanılmayan hesaplar pasife alınır.
6.2.3.*@saglik.gov.tr uzantılı kurumsal veya tüzel e-posta adreslerine giriş ve şifre işlemleri eposta***.saglik.gov.tr*** adresinden yürütülür.
6.2.4.Kullanıcılar, kendilerine ait parolanın güvenliğinden ve söz konusu parola kullanılarak gönderilen e-postalardan doğacak hukuki işlemlerden sorumludur.
6.2.5.Kurumsal e-posta hesabı yalnızca kurumsal süreçlere ilişkin iş ve işlemlerde kullanılabilir. Kurumsal e-posta hesaplarının, idari ve hukuki düzenlemelere aykırı ya da şahsi iş ve işlemlere ilişkin kullanımından kaynaklanan her türlü adli, idari, mali ve cezai sorumluluk ilgili hesap kullanıcısına aittir.
6.2.6. Sosyal medya, alışveriş siteleri, forumlar gibi üyelik isteyen uygulamalarda, Bakanlık tarafından verilen kurumsal e-posta hesapları kullanılamaz. Aksi durumlarda, yapılan tüm işlemlerden ve dile getirilen ifadelerden, ilgili kullanıcı sorumludur.
6.2.7.Konusu suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden ve sahip olduğu görev kapsamı içindeki iş ve işlemler dışındaki e-posta hesabının kullanımından kullanıcı sorumludur.
6.2.8.Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.
6.2.9.İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.
6.2.10.Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz.
6.2.11.Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
6.2.12.Internet 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.
6.2.13.Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.
6.2.14.Personel KONU alanı boş bir e-posta mesajı göndermemelidir.
6.2.15.KONU alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.
6.2.16.E-postaya eklenecek dosya uzantıları ".exe", ".vbs" veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip ve/ya rar formatında) mesaja eklenecektir.

6.2.17.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.

6.2.18.Kullanıcı, Kurumun e-posta sistemi üzerinden taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında Sistem Yönetimine haber verilmelidir.

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

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

6.2.21.Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt verilmemelidir.

6.2.22.Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

6.2.23.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.

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

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

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

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

6.2.28. e-Posta güvenliği ile ilgili şüpheli bir durum oluşması halinde ivedilikle sistem yöneticisine (eposta@saglik.gov.tr)haberverilir. Ayrıca https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir adresinde yer alan ***Bİ.FR.03 Olay Bildirim Formu*** doldurulur.

6.2.29.E-posta gönderimlerinde, mesajın en alt kısmına gönderen kişinin kimlik ve iletişim bilgileri yazılır.

6.2.30.Tüzel e-posta talepleri ilgili form ve resmi yazı ile İstatistik ve Bilgi İşlem Birimine gönderilir. İstatistik ve Bilgi İşlem Biriminden onay alınmadan tüzel e-posta adresi açılamaz.

7.İLGİLİ DOKÜMANLAR:

- ***Bİ.FR.03 Olay Bildirim Formu***