İNTERNET, E-POSTA VE PAROLA(ŞİFRE) KULLANIM PROSEDÜRÜ

T.C. SAĞLIK BAKANLIĞI
ÇORUM
İL SAĞLIK MÜDÜRLÜĞÜ

E-POSTA KULLANIMI:

1. Kurumsal iş ve işlemlerini yapabilmek için her kullanıcının Sağlık Bakanlığı eposta hesabı olmalıdır.
2. Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.
3. Kurum 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.
4. Kullanıcı, Kurumun e-posta sistemini taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Kullanıcılar bu tür özelliklere sahip bir mesaj alındığında kurum bilgi güvenliği sorumlusuna haber verilmelidir. Ayrıca kurumların web sitelerinde yer alan Olay Bildirim Formunu kullanarak veya "https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir" adresinden ihlal bildirimi yapılmalıdır.
5. Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçlar ile e-posta gönderilmemelidir.
6. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, bilgi güvenliği birim sorumlusuna haber verilmelidir.
7. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
8. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
9. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.
10. Kurumsal E-posta kişisel amaçlar için kullanılmamalıdır.
11. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e- postalara herhangi bir işlem yapmaksızın bilgi güvenliği sorumlusuna haber vermelidir.
12. Kullanıcı, kurumsal mesajlarını, kurum iş akışının aksamaması için zamanında cevaplandırmalıdır.
13. Kullanıcı, kurumsal e-postalarının, kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.
14. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar bilgi güvenliği sorumlusuna haber verilmelidir.
15. Kullanıcı parolaları, en az 8 karakterden oluşmalı ve parolalarda; en az 1 tane harf, en az 1tane rakam ve en az 1 tane özel karakter (@,+,$,#,&./,(,*,- ,}.=...) bulunmalı; parola içeriğinde kullanıcı adını soyadını açık bir şekilde yazmamalıdır.
16. Kullanıcı, kendilerine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren Bilgi İşlem Birimine haber vermelidir.
17. Bakanlığımız tarafından talep edilen birimlere özel olarak verilen tüzel e-posta hesapları Tüzel Kişiler E-posta Talep Formu kullanılarak yapılmalıdır.
18. Bakanlığımız tarafından talep edilen birimlere özel olarak verilen tüzel eposta hesapları direkt kullanıcı hesaplarına yetkilendirilmiştir. Yetkilendirilen kişilerin birim değişikliği veya kurumda ayrılması durumunda ilgili birim tarafından Bilgi İşlem Birimine haber verilmelidir. Haber verilmemesi durumunda doğacak her türlü zarardan ilgili birim sorumlu olacaktır.

PAROLA(ŞİFRE) KULLANIMI:

1. Sistem sunucuları, uygulamalar ve ağ cihazlarında kullanıcı tanımı yapılırken, şifreler boş bırakılmamalıdır. Şifrelerin en az sekiz (8) karakter olması, en az bir harf, iki rakam ve en az 1 kompleks karakter içerecek şekilde ayarlamaları yapılmalıdır.
2. Oluşturulan bu parolalar en az aşağıdaki özelliklere sahip olmalıdır.
    - İçerisinde en az 1 (bir) tane büyük (Örn: ABCDEF...) ve en az 1(bir) tane küçük harf(Örn: abcdef ...) bulunur.
    - İçerisinde en az 1 (bir) tane rakam bulunur (örn: 1234567890)
    - İçerisinde en az 1 (bir) tane özel karakter bulunur. (@, !,?,A,+,$,#,&,/,{,*,- ,],=,...)
    - Aynı karakterlerin peş peşe kullanılması engellenir. (aaa, 111, XXX, ababab...)
    - Sıralı karakterlerin kullanılması engellenir. (abcd, qwert, asdf,1234,zxcvb...)
3. Tüm uygulamalar ve sunucu sistemleri üzerinde yapılacak ayarlarla, kullanıcı şifrelerinin en geç 6 (altı) ayda bir değiştirilmesi zorunlu kılınacaktır.
4. Kullanıcı şifreleri oluşturulduktan sonra kullanıcılara gönderimi yapılacak ve ilk girişte kullanıcının parolasını değiştirmesi zorunlu hale getirilecektir.
5. Uygulamalara ve sistemlere ilk girişte belirlenmesini istediği yeni şifrenin tanımlanması ve korunması ilgili personel sorumluluğundadır. Şifreler hatırlanmak maksadı ile başka birinin göreceği şekilde herhangi bir kayıt ve kağıt ortamına yazılamaz, başkası ile paylaşılamaz.
6. Uygulamalarda aynı işi yapan kullanıcılara her bir kullanıcı için ayrı yetkilendirme yapılmalıdır. Ortak şifre ile birden fazla kişi işlem yapmamalıdır. Yapılan işlemden kaynaklanan hata/zararlardan şifresini paylaşan personel sorumlu olacaktır.
7. Şifrelerin unutulması durumunda, kullanıcı şifresi yenilenmesi için personel ilgili Sistem Yöneticisine şahsen başvurmalıdır. Daha sonra değiştirilmek üzere kullanıcı için yeni bir geçici şifre oluşturulur.
8. Kullanıcı ilk verilen geçici şifreyle sisteme giriş yaptığında, yeni bir şifre belirlenmesi sistem tarafından otomatik olarak istenmelidir.
9. Her kullanıcı hesabına ait ayrı bir parola olmalıdır.(E-posta hesabı ile bilgisayar şifresinin aynı olmaması gibi)
10. Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilmelidir.
11. Şifrelerin klavyeden girilmesi sırasında dikkatli olunmalı ve çevredeki kişilerin görmesine izin vermeyecek şekilde girilmelidir.
12. Şifreler ilave bir şifreleme metodu kullanılmadan hatırlamak amacıyla kayıt edilmemelidir. (kağıt, bilgisayardaki bir dosya, cep telefonu gibi ortamlarda saklanmamalıdır).

İNTERNET KULLANIMI:

1. Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır. Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
2. Kurum içinde free vpn, Proxy server, Tor, torrent, hotspot vb. uygulamaların kullanılması yasaktır.
3. Kurumun politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır.
4. Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.
5. Kurumun ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır.
6. Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.
7. İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.
8. Mesai saatleri içerisinde iş ile ilgili olmayan video, müzik vb. aşırı veri çeken streming media kullanılmamalıdır.
9. Mesai saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.

10. Kurumsal alanlarda verilen internet hizmetinin şahsi iş ve işlemlerde kullanılamaz.
11. Kurum network güvenliği açısından yönetilemeyen switch (Hub çoklayıcı) kullanılmamalıdır.
12. Kurum network güvenliği açısından Hub, acces point vb. Cihazların Bilgi İşlem Birimi izni dışında kurum networküne kesinlikle bağlanmamalıdır.
13. İnternet üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez ve kurum sistemleri üzerine bu yazılımlar kurulamaz.
14. Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumum bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir
15. Kurum network güvenliği acısından mümkün olduğunca VLAN yapısı kullanılmalıdır.
16. Merkezi olarak kullanılan HBYS hizmetleri ve bakanlığımız uygulamalarına erişimin aksamaması, bant genişliği trafiğini sağlıklı yönetilmesi, siber saldırı tehditlerine karşın gerekli önlemleri almak için internet erişim düzenlemeleri gerekli hallerde İl Sağlık Müdürlüğü tarafından değiştirilir.
17. Kamusal hizmetlerin yürütülmesinde erişim engeli yaşayan personeller için Ayrıcalıklı Erişim Talep Formuyla ıslak imzalı olarak İl Sağlık Müdürlüğüne resmi yazı ile bildirilerek gerekli değerlendirme yapılacaktır.
18. Yasaklanması gereken siteler bilgi güvenliği yönetim komisyonu tarafından belirlenip onaylandıktan sonra uygulamaya konulacaktır. Ancak kurum bilgi güvenliğini tehlikeye düşürecek bir durumda (siber saldırı, veri kaybı vb.) onay alınması beklenmeden uygulamaya geçilebilecektir.

Hazırlayan	Kontrol Eden	Onaylayan
Samet ŞENSOY Bilgi Güvenliği Yetkilisi	Ahmet Bahadır ÜNLÜ Destek Hizmetleri Başkanı Bilgi Sistemleri Koordinatörü	Uzm. Dr. Ömer SOBACI İl Sağlık Müdürü