1. AMAÇ

Bu politikanın amacı Kocaeli Üniversitesi Bilgi İşlem Daire Başkanlığı ağ ve erişim güvenliği kapsamında e-posta, parola, ağ erişim, sunucu, uzak bağlantı, kablosuz ağ güvenliğine yönelik politikaları ortaya koymaktır.

2. SORUMLULUKLAR VE KAPSAM

Bu politika Kurumda sunulan hizmetlerde e-posta, parola, ağ erişim, sunucu, uzak bağlantı, kablosuz ağ güvenliğinde izlenecek kuralları içermektedir ve bütün çalışanları kapsamaktadır.

3. E-POSTA GÜVENLİĞİ

Kurumda oluşturulan e-postalar resmi bir kimlik taşımaktadırlar. E -posta kurumun en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır.

3.1. Genel Kullanım

a) Kurum çalışanları, kurum ile ilgili çalışmalarında kurumun dışındaki eposta hesaplarını kullanmamalıdır.

b) Kurum çalışanları, mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.

c) Kurum çalışanları, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden parola kullanılmalı ve eposta erişimi için donanım / yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

d) Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen epostaların sahte eposta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

e) Kurum çalışanları, kurumsal epostaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.

f) Kaynağı bilinmeyen eposta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

g) Epostaların sık sık gözden geçirilmesi ve veri kaybını önlemek amacıyla kurum çalışanları epostaların yedeklerini almalı ve kurum arşivinde(varsa) bir yedek tutulmalıdır.

h) Eposta adresine sahip kullanıcı herhangi bir sebepten (emekli olma, işten ayrılma gibi nedenlerle) kurumdaki değişikliğinin yetkililer tarafından ilgili birime bildirilmesi gereklidir.

3.2. Yasaklanmış Kullanım

a) Kurumun eposta sistemi, taciz su istimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine haber verilmesi gerekmektedir.

b) Kurum çalışanları, eposta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

c) Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

d) Spam, zincir eposta, sahte eposta vb. zararlı e-postalara ve mesajlara iliştirilmiş hertürlü çalıştırılabilir dosya içeren epostalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

e) Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen epostaların sahte eposta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.

f) Kişisel kullanım için internet'teki listelere üye olunması durumunda kurum eposta adresleri kullanılmamalıdır.

4. İNTERNET GÜVENLİĞİ

Bütün kullanıcılar ve ağ ve sistem yöneticileri aşağıdaki internet erişim ve kullanım yöntemlerini kullanmalıdır.

4.1. Uygulama

a. Kurumun bilgisayar ağı erişim ve içerik denetimi yapan bir güvenlik duvarı (firewall) üzerinden internete çıkmalıdır.

b. İhtiyaçlar doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. Yasaklı siteler (kumar, şiddet vs.) güvenlik duvarı aracılığıyla engellenebilir.

c. Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme sistemleri kullanılmalıdır (FW, IPS, IDS vb.)

d. Antivirüs geçiş (gateway) sistemleri kullanılmalıdır. İnternete giden veya gelen bütün trafik virüslere karşı taranmalıdır.

e. Kurumda sadece yetkilendirilmiş sistem yöneticileri internete çıkarken ihtiyaç duyulan bütün servisleri kullanma hakkına sahiptir. Çalışılan projeler dahilinde ftp ve telnet yetkisi ilgili personellere verilebilmelidir.

f. Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemelidir. İndirilecek dosyalara virüs taraması yapılacağı için zararlı içerikler antivirüs uygulaması tarafından engellenmelidir.

g. İlgili tarafların kurum internetini kullanmaları kurum sorumlularının izni ve bu konudaki izlenecek politika ve kurallar dahilinde gerçekleştirilmelidir.

5. AĞ ERİŞİM GÜVENLİĞİ

5.1. Uygulama

a) Tüm ağ bileşenlerinin konfigürasyonu tanımlanmalı ve uygun filtreleme programları kullanılmalıdır.

b) İnternet erişimi olan sunucu (server)'lar güvenlik duvarı(firewall) ile korunmalıdır.

c) Sadece kurum tarafından yetkilendirilmiş bilgisayarların, kuruluş içi ağa giriş izni verilmelidir.

d) Kurum çalışanlarına işlerini yapabilmesi için yasaklanmış sitelere girmemek koşuluyla internet erişim hakkı verilmelidir ve erişim yaptıkları internet siteleri 5651 sayılı yasa kapsamında 6 ay boyunca kayıt altında tutulmalıdır.

e) Çalışanlar telif ve fikri mülkiyet hakları kurallarına uymalı ve bir başka organizasyonların uygulamalarını kullanmadan önce ilgili yerlerden izin almalıdır.

f) Ağa(network) bağlı bir iş istasyonu ve sunucular, sadece bilgi güvenliği yöneticilerinin belirlediği gerekliliklerin karşılanması durumunda dış ağlarla iletişim kurabilir.

g) Kurumun ağına bağlı iş istasyonlarına, sunuculara erişim, kullanıcı adı ve parolanın girilmesi ile kontrol altına alınmalıdır.

h) Kurum ağına erişim yetkileri, iş takip sistemi üzerinden her 6 ayda bir periyodik iş oluşturularak güncellenir ve takip edilir. 6 aylık zaman zarfı içerisinde kurumdan / birimden ayrılan ya da katılan personel olması durumunda sürenin dolumu beklenilmeden erişim yetkilerinin kontrolü yapılır.

6. UZAKTAN BAĞLANTI GÜVENLİĞİ

6.1. Uygulama

a) Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

b) Kurum, iş takip sistemi üzerinden her üç ayda bir periyodik iş oluşturularak güncellenir ve takip edilir. Üç aylık zaman zarfı içerisinde kurumdan / birimden ayrılan veya katılan personel olması durumunda sürenin dolumu beklenmeden erişim yetkilerinin kontrolü yapılır.

6.2. Bağlantı Gereklilikleri

a) Kuruluş iç ağında iken kullanıcılara ait hiçbir masaüstü PC ve taşınabilir bilgisayarında, dış servis sağlayıcı bağlantısı (Mobil erişim) gerçekleştirilmemelidir.

b) Bağlantı için herhangi bir nedenle modem kullanılması gerekiyor ise, kullanım öncesi birimdeki ağ ve sistem uzmanına gerekli kontrol ve önlemleri alması için bilgi verilmelidir.

c) Kuruluş dışına yapılan (ağ ve sistem uzmanı karar vereceği) tüm kritik bağlantılar güvenli hatlar üzerinden yapılmalıdır.

d) Kurum ağına uzaktan bağlantı sadece iş amacı için kullanılacaktır.

e) Uzaktan kurum ağına yapılan bağlantıda kuruluşun iç ağına uygulanan güvenlik

politikaları geçerli olacaktır.

f) Uzak bağlantılar, ağ ve sistem uzmanının belirleyeceği güçlü kimlik denetimi ile gerçekleştirilecektir.

Uzak bağlantılarda yapılan tüm dosya yüklemelerinde antivirüs taramasından geçirilecektir.

6.3. Erişim Gereklilikleri

a) İnternet üzerinden kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya Kurumlar VPN teknolojisini kullanacaklardır. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlayacaktır. VPN Teknolojileri IpSec protokolünü içermelidir.

b) Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one time password authentication) veya güçlü bir uzun şifre (passpharase) destekli genel/özel anahtar(public /private key) sistemi kullanılması tavsiye edilmektedir. Sertifika kullanılmalıdır.

c) Kurum çalışanları hiçbir şekilde kendilerinin giriş (login) ve eposta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye vermemelidir.

d) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.

e) Uzaktaki kullanıcı, cihazını VPN bağlantısı esnasında başka bir bağlantı daha yaparak (split -tunnel veya dual homing) konfigure edemezler.

f) Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler birimin özel izni ile geçici olarak izin verilebilirler.

g) Periyodik olarak yapılan kontrollerle kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimlikleri ve hesapları kaldırılmalıdır.

7. SUNUCU GÜVENLİĞİ

Uygulama

a) Sunucular, veri merkezinde tutulacaktır. Veri merkezine erişim yetkilendirilen çalışanlar tarafından sağlanmalıdır.

b) Sunuculara, kullanım amacına yönelik olarak işletim sistemi ve diğer yazılımlar kurulmalıdır. Gereksiz yazılım ya da bileşenleri kaldırılmalıdır.

c) Sunucu üzerinde çalışan işletim sistemlerinin, sistem yazılımlarının ve güvenlik amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Antivirüs ve sunucu güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.

d) Sunucu üzerinde kullanılmayan servisler kapatılmalıdır.

e) Kurum ağ ve sistem uzmanı tarafından belirlendiği üzere, sunucu günlükleri düzenli aralıklarla denetim ve izlemeye tabi tutulmalıdır.

f) Sunucuların uzaktan yönetimi gerekiyor ise; yönetim konsolu ve sunucu arasındaki haberleşme güvenli kanal ve tekniklerle gerçekleştirilmelidir.

8. KABLOSUZ AĞ GÜVENLİĞİ

8.1. Güvenlik Ayarları

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için kurumda kişisel şifreler kullanılmaktadır. Parola politikası da güçlü bir şifreleme için düzenlenmelidir.

b) Erişim cihazlarındaki donanım sürüm (firmware)'leri düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.

c) Güvenlik açığı oluşmaması için erişim cihazlarını kolayca erişilebilir bir yerde olmaması gereklidir.

d) Cihaza erişim için güçlü bir parola kullanılmalıdır. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

e) Varsayılan SSID isimlerini kullanılmamalıdır. SSID bilgisi içerisinde firma ile ilgili bilgi olmamalıdır. (Örneğin: kurum ismi, ilgili bölüm çalışanın ismi vs.)

f) Erişim cihazları üzerinden gelen kullanıcılar güvenlik duvarı üzerinden ağa dahil olmalıdırlar.

g) Kullanıcı bilgisayarlarında kişisel güvenlik duvarı yazılımları yüklü olmalıdır.

h) Kritik yerlerde kullanıcılar VPN teknolojilerini kullanarak firma ağına erişmelidir.

i) Erişim cihazları erişimleri kayıt altına alınmalı ve belirli aralıklarla kontrol edilmelidir.

j) Internet kullanmak isteyen misafirler kurum ağına erişememelidir.

9. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında ilgili maddeler gereği disiplin işlemleri uygulanır.