BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

İNTERNET VE E-POSTA KULLANIM PROSEDÜRÜ

İçindekiler

1 Amaç

Bu doküman, e-posta ve internet hizmetlerinin yasal yükümlülükler, kapasite kullanımı ve Kurumsal imajını korumak amacına uygun olarak kullanılmasına yönelik dikkat edilmesi gereken hususları belirlemek için oluşturulmuştur.

2 Kapsam

Bu doküman, Bilgi Güvenliği Kapsam Analizi dokümanında belirtilen tüm personeli kapsamaktadır.

3 Sorumluluk

Görev Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
BGYS Birim Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
Peer to Peer (P2P)	İki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür.
Multimedya Streaming	Ses, video ve diğer multimedya dosyalarının İnternet'te veya Kurumsal intranetlerde bilgisayara yüklemeden ve sabit disk içerisinde yer kaplamadan on-line izlenmesini sağlayan, tamamen ses ve görüntü dosyalarından oluşan bir sistemdir.
Spam	İstenmeyen e-posta.

Phishing	Dolandırıcıların rastgele kullanıcı hesaplarına e-mail gönderdikleri bir çevrimiçi saldırı türüdür.
GB	Gigabyte (Bilgisayarlarda kullanılan 1024 megabayt anlamına gelen ölçü birimidir)
MB	Megabyte (Bilgisayarlarda kullanılan 1.000.000 byte anlamına gelen ölçü birimidir)

5 İşlem Detayı

5.1 İnternet Kullanım Esasları

İnternet kullanımında dikkat edilmesi gereken hususlar aşağıda tanımlanmıştır;

1. Kurum bilgisayar ağı erişim ve içerik denetimi yapan bir güvenlik duvarı (firewall) üzerinden geçtikten sonra internete çıkacaktır.
2. Kurum ihtiyacı ve yasal gereklilikler doğrultusunda içerik filtrelemesi yapar, istenilmeyen sitelere (oyun, kumar, şiddet, pornografi vb.) erişim yasaklanır.
3. Kurum ihtiyacı doğrultusunda saldırı tespit ve önleme cihazları kullanır. (IPS, IDS)
4. İnternete giden veya internetten gelen bütün trafik firewall kullanarak virüslere karşı korunmalıdır.
5. Yetkilendirilmiş sistem yöneticileri internete çıkarken ihtiyaçları doğrultusunda bütün servisleri kullanabilir. (ftp, telnet, traceroute vb.)
6. Hiçbir kullanıcı P2P bağlantı yoluyla internetteki servisleri kullanamaz. (Acquisition, Apollon (GUI), BearShare, iMesh, LimeWire, XNap vb.)
7. Multimedya streaming ihtiyaca göre kullanılır.
8. Kişisel internet kullanımı işin üretkenliğini etkilemediği ve işin önceliğinin önüne geçmediği sürece kabul edilebilirdir.
9. İş ile ilgili olmayan yüksek hacimli dosyalar (müzik, video vb.) yüklenmez ve indirilmez.
10. Kurum tarafından onaylanmamış yazılımlar internet üzerinden indirilmez ve Kurum sistemlerine yüklenmez.
11. İnternet kullanımı zorunlu olan kurum dışı (misafir, danışman vb.) kullanıcılar, ilgili Kablosuz Misafir Ağına dâhil olarak interneti kullanabilirler.

12. Kurum içerisinden yapılan Internet erişimlerinde Kurum güvenliğini tehlikeye sokacak veya Türkiye Cumhuriyeti yasalarında yasadışı kabul edilen sitelere girilmemesi kullanıcı sorumluluğundadır.
13. Kurum içerisinden yapılan internet erişimi, 5651 sayılı kanuna uygun olarak yönetilir ve kayıt altına alınır.
14. İnternet erişiminin içeriğinin düzenli olarak izlenmesi kurumun politikasının bir parçası değildir. Ancak yetkili mercilerin yazılı talebi ile haberleşme ve veri akışının içeriğini kayıt etme ve/veya inceleme görevini yerine getirebilir.
15. Kullanıcılar kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bunun için kullanıcılar kimlik bilgilerini uygun şekilde saklamalı ve başkaları ile paylaşmamalıdır.
16. Kurum, kendi altyapısını kullanan tüm kullanıcıların internet kullanımını işlevsel, bakım, teftiş, güvenlik, araştırma faaliyetlerini desteklemek için anonim olarak izleyebilir. Çalışanlar internet kullanımlarını kurumun zaman zaman kontrol edeceği gerçeğini kabul ederek kullanmalıdırlar.

5.2 E-Posta Kullanım Esasları

1. Kullanıcılar kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur.
2. Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.
3. Kurum e-posta kaynakları kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
4. İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez.
5. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
6. Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara zincir e-postası, reklam, karalama SPAM veya Phishing mesajları göndermek için kullanılamaz.
7. Kurumun e-posta sistemi ücretsiz veya ticari yazılımın alınması, gönderilmesi veya saklanması için kullanılamaz.
8. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve/veya kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-posta gönderilemez.

9. E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir.
10. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir.
11. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" vb. uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (ZIP veya RAR formatında) mesaja eklenmelidir.
12. Kurum ile ilgili olan ve sınıflandırması gizli ve üzeri olan bilgi, e-posta ile şifresiz olarak gönderilmemelidir.
13. Kullanıcı, e-posta vasıtasıyla bulaşabilecek virüs gibi zararlı içerikten korunmak amacıyla, tanımadığı kişilerden gelen ve şüpheli eklentiler içerdiği görülen mesajları gerekmediği sürece açmamalıdır. Tüm e-posta içerikleri ve eklentileri açılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmelidir.
14. Zincir mesajlar veya herhangi bir şekilde alıcının haklarına zarar vermeyi amaçlayan (taciz, suistimal vb), çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyecek, Bilgi İşlem'e haber verilecektir. Durum değerlendirildikten sonra gerekli ise bilgi güvenliği ihlal olayı başlatılacaktır.
15. Kullanıcı, e-posta ile uygun olmayan içerikleri (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
16. 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.
17. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Bilgi İşlem'e haber vermelidir. Durum değerlendirildikten sonra gerekli ise bilgi güvenliği ihlal olayı başlatılmalıdır.
18. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Bilgi İşlem Birimi'yle irtibata geçerek parolasını sıfırlamalıdır. Durum değerlendirildikten sonra gerekli ise bilgi güvenliği ihlal olayı başlatılmalıdır.
19. Kuruma ait olmayan e-posta hizmetleri ile (Gmail, Hotmail, Yahoo, vb.) kurumsal bilgiler paylaşılmamalıdır.
20. Çalışanlar düzenli olarak posta kutularını gözden geçirmelidir ve gerekmeyen e-postaları silmelidirler.

21. Kullanıcı, elektronik posta sistemlerini, önemli bilgilerin arşiv deposu için kullanmamalıdır.
22. Kurumsal e-posta hesaplarında kullanılan parolalar "parola politikası" na uygun olmalıdır.
23. Kullanıcılar sadece kurumun yetkili birimlerince onaylanmış e-posta yazılımlarını ve konfigürasyonlarını kullanabilirler.
24. E-posta yazılımının mevcut güvenlik ayarlarını gevşetecek ayarlamalar yapılamaz.
25. Elektronik haberleşmenin içeriğinin düzenli olarak izlenmesi kurumun politikasının bir parçası değildir. Ancak yetkili mercilerin yazılı talebi ile haberleşme ve/veya veri akışının içeriğini kayıt edebilir ve/veya inceleyebilir.
26. Kurum personeli kişisel mesajlaşmaları için kurumsal e-posta hesabını kullanmamalıdır. Bu durumun tespiti için yetkili kişiler önceden haber vermeksizin e-postaları denetleyebilirler.
27. İnternet ve e-posta kullanımı zorunlu olan kurum dışı (misafir, danışman vb.) kullanıcılar, ilgili birim amirinin yazılı teklifiyle, 3. Taraf Bireysel Kullanıcı Taahhütnamesi imzalayarak kullanabilirler.
28. Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından bilgisi dahilde okunmasını engellemelidir.
29. Kullanıcıların, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemek amacıyla e-postalarda gönderilecek postanın altında feragatname (Disclaimer) bulunmalıdır.

    Söz konusu yazı aşağıda belirtilmiştir;

    "Bu elektronik posta ve onunla iletilen bütün dosyalar sadece göndericisi tarafından alması amaçlanan yetkili gerçek ya da tüzel kişinin kullanımı içindir. Eğer söz konusu yetkili alıcı değilseniz bu elektronik postanın içeriğini açıklamanız, kopyalamanız, yönlendirmeniz ve kullanmanız kesinlikle yasaktır ve bu elektronik postayı derhal silmeniz gerekmektedir. …… bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda herhangi bir garanti vermemektedir. Bu nedenle bu bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından ve saklanmasından sorumlu değildir. Bu e-posta bilinen bütün bilgisayar virüslerine karşı taranmıştır. Ancak yollayıcı, bu e-posta mesajının-virüs koruma sistemleri ile kontrol

ediliyor olsa bile virüs içermediğini garanti etmez ve meydana gelebilecek zararlardan doğacak hiçbir sorumluluğu kabul etmez."

" This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient you are hereby notified that any dissemination, forwarding, copying or use of any of the information is strictly prohibited, and the e-mail should immediately be deleted. …….. makes no warranty as to the accuracy or completeness of any information contained in this message and hereby excludes any liability of any kind for the information contained therein or for the information transmission, reception, storage or use of such in any way whatsoever. This e-mail message has been swept by anti-virus systems for the presence of computer viruses. In doing so, however, sender cannot warrant that virus or other forms of data corruption may not be present and do not take any responsibility in any occurrence."

5.1.1 E-posta Saklama Kapasite Sınırları

Kullanıcıya tanımlanan kurumsal e-posta hesabının kapasiteleri 4 kademeli olarak planlanır. Özellikleri aşağıdaki gibi olmalıdır;

- E-Posta Kutusu Boyutu:
  - Üst Yönetim ve Yöneticiler : 10 GB
  - Yetkilendirilmiş kullanıcılar : 5 GB
  - Diğer Kullanıcılar : 1-2 GB
- Tek seferde maksimum E-Posta gönderme ve alma boyutu: 20 MB
- Kullanıcının e-posta kutusunun uyarı seviyeleri: 1 GB için 0,9 GB, 2 GB için 1,9 GB, 5 GB için 4 GB, 10 GB için ise 9 GB.
- E-Posta Sunucusu Üzerinde E-Posta Saklama Süresi: E-Posta kutusu boyutu kadarınca e-posta süresiz olarak saklanır.

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					