İnternet, Mesajlaşma, Sosyal Medya ve E-Posta Kullanım Politikası

DEĞİŞİKLİK TAKİP LİSTESİ

No	Tarih	Açıklama
00	07.12.2022	İlk Yayın

İÇİNDEKİLER

1. AMAÇ

Bu doküman, Kuruluşta internet, mesajlaşma, sosyal medya ve e-posta hizmetlerinin uygun olmayan kullanımını engelleyerek; Kuruluş yasal yükümlülüklerini, kapasite kullanımını ve kurumsal imajını korumak amacı ile dikkat edilmesi gereken hususları ve belirlemek için oluşturulmuştur.

2. KAPSAM

İlgili prosedür Üniversite'nin tüm idari ve akademik personelini kapsamaktadır.

3. UYGULAMA

3.1. İnternet ve Anlık Mesajlaşma Kullanım Esasları

Her türlü bilgiye erişilebilen ve her türlü bilginin paylaşılabileceği internet kullanımında dikkat edilmesi gereken hususlar aşağıda tanımlanmıştır.

1.Kurum bilgisayar ağı erişim ve içerik denetimi yapan bir güvenlik duvarı (firewall) üzerinden geçtikten sonra internete çıkar.

2.Kurumun ihtiyacı ve yasal gereklilikler doğrultusunda kurum içerik filtrelemesi yapabilir, istenilmeyen sitelere (oyun, kumar, şiddet, pornografi vb.) erişim yasaklanmıştır.

3.Yetkilendirilmiş sistem yöneticileri internete çıkarken ihtiyaçları doğrultusunda bütün servisleri kullanabilmelidir. (ftp, telnet, traceroute vb.)

4.Hiçbir kullanıcı P2P bağlantı yoluyla internetteki servisleri kullanamaz. (Acquisition, Apollon (GUI), BearShare, iMesh, LimeWire, XNap vb.)

5.Kurumun izin verdiği anlık mesajlaşma hizmeti/hizmetleri dışında diğer anlık mesajlaşma hizmetleri kullanılmamalıdır.

6.Anlık mesajlaşma hizmeti yalnızca kurumsal görüşmeler için kullanılmalıdır.

7.Kişisel internet kullanımı işin üretkenliğini etkilemediği ve işin önceliğinin önüne geçmediği sürece kabul edilebilirdir.

8.Kurum tarafından onaylanmamış yazılımlar internet üzerinden indirilmemelidir ve kurum sistemlerine yüklenmemelidir.

9.3.tarafların interneti kullanımı Sistem Uzmanı izni ile sağlanmalıdır ve 3.tarafların kullandıkları ağ ile kurum sistemlerinin bulunduğu ağ birbirinden farklı olmalı ve birbirileri ile haberleşmeleri engellenmelidir.

10.Kurum içerisinden yapılan Internet erişimlerinde kurum güvenliğini tehlikeye sokacak veya Türkiye Cumhuriyeti yasalarında yasadışı kabul edilen sitelere girilmemesi kullanıcı sorumluluğundadır.

11.Kurum içerisinden yapılan internet erişimi, kurum tarafından denetlenmeli ve kayıt altına alınır.

12.5651 sayılı kanun gereği kurum ilgili erişim bilgilerini tutmak ve devletin ilgili mercileri tarafından istenmesi durumunda bu bilgiyi sağlamakla yükümlüdür. Bu kanun doğrultusunda kullanıcılar yasadışı kabul edilen sitelere girmesi durumunda kurum yetkilileri tarafından gerekli cezai işlem uygulanabileceği ya da Savcılık tarafından haklarında suç duyurusunda bulunulabileceğini bilmekle yükümlüdür.

13.Kurum, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü taraflarla, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.

14.İnternet kullanımından kaynaklanacak ihlal ve suçlarla ilgili olarak kurum içerisinde disiplin süreçleri işletilir.

3.2. 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-postalar, reklam, karalama SPAM veya oltalama 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 kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-posta gönderilemez.
9. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.
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 eklenecektir.

12. Kurum ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Gönderilmesi zorunlu durumlarda ise içerik şifrelenmelidir ve mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.
13. Zincir mesajlar, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip Sistem Uzmanına haber verilmelidir. Durum değerlendirildikten sonra gerekli ise bilgi güvenliği ihlal olayı başlatılmalıdır.
14. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
15. 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.
16. Kullanıcı, gelen ve/veya giden mesajlarının kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.
17. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Sistem Uzmanına haber verilmelidir. 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 Sistem Uzmanına haber verilmelidir. Durum değerlendirildikten sonra gerekli ise bilgi güvenliği ihlal olayı başlatılmalıdır.
19. 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.
20. Kuruma ait olmayan e-posta hizmetleri ile (Gmail, Hotmail, Yahoo, vb.) kurumsal bilgiler paylaşılmamalıdır.
21. Çalışanlar düzenli olarak posta kutularını gözden geçirmelidir ve gerekmeyen e-postaları silmelidirler.
22. Kullanıcı, elektronik posta sistemlerini, önemli bilgilerin arşiv deposu için kullanamaz.
23. Kurumsal e-posta hesaplarında kullanılan parolalar parola politikasına uygun olmalıdır.
24. Kullanıcılar sadece kurumun yetkili birimlerince onaylanmış e-posta yazılımlarını ve konfigürasyonlarını kullanabilirler.
25. E-posta yazılımının mevcut güvenlik ayarlarını gevşetecek ayarlamalar yapılamaz.
26. Kullanıcılar e-posta yazılımının gönderenin kimliğini gizleyecek özelliklerini kullanamaz.

27. Elektronik haberleşmenin içeriğinin düzenli olarak izlenmesi kurumun politikasının bir parçası değildir. Ancak kurum şüphelenilen mesajların inceleme hakkına ve yetkisine sahiptir.

    Kurum dışına gönderilen e-postalarda gönderilecek postanın altında feragatname (Disclaimer) bulunmalıdır.

3.3. Sosyal Medya Kullanım Esasları

1.Kurum ve kuruma bağlı birimlerin sosyal medya hesaplarında kişisel bilgiler verilmemelidir. Bu hesaplarda pau.edu.tr uzantılı e-posta adresleri kullanılmalıdır.

2.Yayınlanan içerikler Pamukkale Üniversitesi kimliğine uygun olmalıdır.

3.Sosyal medya platformlarında özel hayata dair ve kişisel bilgiler paylaşılmamalıdır.

4.Yayınlanan içeriklerde (fotoğraf, video, makale, müzik, söz, sanat eseri vb.) alıntı yapılmış ise referans gösterilmesi gereklidir.

5.Pamukkale Üniversitesi ve bağlı birimlerinin resmi hesapları dışında kişisel hesaplardan yapılan içeriklerden Pamukkale Üniversitesi sorumlu değildir.

6.Sosyal medya hesaplarında kar ve ticari amaç güden reklamlara yer verilmemelidir.

7.Politik görüş, dini inanç, etnik köken, cinsel yönelim gibi toplum nezdinde hassas olarak karşılanan konularda paylaşım yapılırken hassasiyetlere dikkat edilmeli ve ilgili üst yönetim biriminden onay alınarak yorum, cevap ve açıklamalarda bulunulmalıdır.

8.Sosyal medya üzerinden yayınlanan içeriklere yapılan yorumlara/verilen cevaplara kurumun kimliğine zarar getirecek ifadelerden kaçınılmalı, nezaket kuralları çerçevesinde cevap verilmeli ya da kullanıcıya bilgi verilmesi için ilgili birim ya da kişilerle iletişime geçmesi yönünde yönlendirmelerde bulunulmalıdır.

4. İLGİLİ DOKÜMANLAR