	E-POSTA POLİTİKASI	Doküman No	PL.08
		Yayın Tarihi	16.07.2018
		Revizyon No	08
		Revizyon Tarihi	04.07.2025
		Sayfa No	1/6

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

1. Amaç

ESOGÜ'de @ogu.edu.tr e-postalarının kişisel ve iş amaçlı kullanımına yönelik kuralları tanımlamaktır.

2. Kapsam

Bu politika kapsamında ESOGÜ bünyesinde mail adreslerinin kullanımına yönelik esaslar ele alınmaktadır.

3. Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Sorumlular

Bu politikanın oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Politikanın uygulanmasından @ogu.edu.tr uzantılı eposta kullanan tüm personel ve öğrenciler sorumludur.

5. Uygulama

E-posta bir kurumun en önemli iletişim kanallarından biri olup bu kanalın kullanılması kaçınılmazdır. E-Posta hizmeti ESOGÜ BİDB mail sunucuları tarafından sağlanmaktadır. Tüm üniversite personeline ve öğrencilerine @ogu.edu.tr eposta adresi BİDB tarafından tanımlanır. @ogu.edu.tr e-posta adresine sahip personelin emekli olma, işten ayrılma gibi durumlarda e-posta adresi BİDB tarafından kapatılır. Öğrencilerin eposta hesapları ise üniversiteden mezun olduklarında veya ilişiği kesildiğinde BİDB tarafından silinir.

6. E-Posta Sisteminin Güvenli Kullanımına İlişkin Kural ve Kısıtlamalar

- Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.
- Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM(Gereksiz Posta), phishing (oltalama) gibi mesajlar göndermek için kullanılamaz.
- Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
- İnternet 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.
- Personel KONU alanı boş bir e-posta mesajı göndermemelidir.
- KONU alanı boş ve kimliği belirsiz e-posta açılmadan silinmelidir.
- 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.
- Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.
- Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde kanunen suç sayılmış, alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ESOGÜ BİDB'ye bildirilmesi gerekmektedir.

- Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
- Bilgi güvenliği kapsamında hiçbir gizli bilgi mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dahildir.
- Zincir mesajlar (spam), mesajlara iliştirilmiş her türlü çalıştırılabilir dosya, mesajlara iliştirilmiş her türlü zararlı link içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır, paylaşılmamalıdır.
- E-posta içerisinde uygun olmayan içerikler (ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb.) gönderilmemelidir.
- 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.
- Yukarıdaki maddeye binaen, giden E-postalarda kuruma ait sorumluluk reddi bulunmalıdır.
- Personel iş ile ilgili yazışmalarında kişisel e-posta hesaplarını (örnek: Gmail, hotmail, yahoo, mynet, vs.) kullanmamalı, aynı zamanda e-postalarının bir kopyasını yönlendirmemelidir.
- Personel, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden güvenliği yüksek bir parola kullanmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri ile yetkisiz erişimlere karşı koruma sağlamalıdır. Bilgisayarda veya mobil cihazlarda ekran koruma parolası olmalıdır.
- Sahada çalışan personel, kurumsal e-postalarına, mobil cihazlardan erişmesi durumunda, bilginin gizliliğini sağlamak zorundadır ve aynı zamanda bu gizliliği sağlamak için mobil cihazlarında parola kullanmak zorundadır.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

- Kullanıcılardan, kullanıcı kodu/parola girmesini isteyen e-postanın sahte e-posta olabileceği dikkate alınarak, gelen bu e-posta herhangi bir işlem yapılmaksızın derhal silinmelidir.
- E-posta kullanıcıları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekle sorumludurlar. Aynı zamanda kurum çalışanları, kurumsal e-postalarını, içerikleriyle beraber, kurum dışındaki şahıslar veya yetkisiz şahısların e-posta hesaplarına yönlendiremezler.
- Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.
- Kullanıcı **@ogu.edu.tr** kurumsal e-posta hesabı üzerinden dakikada 50 adetten fazla gönderim yapmamalıdır. Dakikada 50 adedi aşan gönderimler alıcılara iletilmeyecektir.
- Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar ESOGÜ BİDB Sistem Yönetimine haber verilmelidir.
- Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının çalındığını/kırıldığını fark ettiği anda parolasını derhal değiştirmelidir.
- Kurum tarafından onaylanmış, üretici tarafından desteği devam eden kararlı ve güncel sürüme sahip internet tarayıcıları ile e-posta istemcileri kullanılmalıdır.
- E-POSTA KULLANIM TALİMATI gereği toplu e-posta gönderimi yetkisi, yetkiyi talep eden birimlere aittir.

7. Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK

kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

8. İlgili Dokümanlar

PR.12 - OLAY İHLAL YÖNETİM PROSEDÜRÜ

PL.08 -TL.01- E-POSTA KULLANIM TALİMATI

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	SEVİNÇ ÇOLAK	DİLEK ÇELİK