	E-POSTA POLİTİKASI	Doküman No	PL.08
		Yayın Tarihi	16.07.2018
		Revizyon No	09
		Revizyon Tarihi	19.08.2025
		Sayfa No	1/6

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

1. Amaç

ESOGÜ'de @ogu.edu.tr e-postalarının kullanımına yönelik kuralları Bilgi Güvenliği Yönetim Sistemine uygun olarak tanımlamaktır.

2. Kapsam

Bu politika kapsamında ESOGÜ bünyesinde e-posta adreslerinin kullanımına yönelik esaslar ele alınmaktadır.

3. Dayanak

Bu talimatta yer alan uygulama kuralları; ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi Standardı Kontrol Maddelerine ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı'nın 10.07.2020 tarih ve 2020/1.0 sürüm no.lu Bilgi ve İletişim Güvenliği Rehberi'nde yer alan "E-Posta Sunucusu ve İstemcisi Güvenliği" başlığı altındaki tedbir maddelerine dayanılarak hazırlanmıştır.

4. Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

CBDDO: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

5. Sorumlular

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

6. Uygulama

E-posta bir kurumun en önemli iletişim kanallarından biri olup bu kanalın kullanılması kaçınılmazdır. E-Posta hizmeti ESOGÜ BİDB tarafından sağlanmaktadır. Personel Bilgi Sistemi ve e-posta sistemi birbiri ile entegre olduğundan, Personel Bilgi Sistemine kayıt edilen kişinin, Netyetki kullanıcısını aktif etmesi esnasında; kişinin seçimine bağlı olarak e-posta adresi otomatik olarak verilir.

Kurumdan ilişiği kesilen personelin e-posta hesabı otomatik olarak kapalı konuma gelir. Öğrencilerin eposta hesapları ise üniversiteden mezun olduklarında veya ilişiği kesildiğinde BİDB tarafından kapalı duruma getirilir ve kullanıma kapatılır.

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

E-posta sisteminin güvenli kullanımına ilişkin kural ve kısıtlamalar aşağıdaki maddelerle belirtilmiştir:

a) Kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.
b) Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz.
c) Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM(Gereksiz Posta), phishing (oltalama) gibi mesajlar göndermek için kullanılamaz.
ç) Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
d) İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta adresi bu mesajlarda kullanılamaz.

e) E-posta kullanıcıları KONU alanı boş bir e-posta mesajı göndermemelidir.

f) E-postaya eklenecek dosya uzantıları ".exe", ".vbs" vb. uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip ve/ya rar formatında) mesaja eklenecektir.

g) Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.

ğ) 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.

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

ı) Bilgi güvenliği kapsamında hiçbir gizli bilgi e-postada yer alamaz. Bunun kapsamına içerisine iliştirilen öğeler de dâhildir.

i) Zincir mesajlar (spam); bu mesajlara iliştirilmiş her türlü çalıştırılabilir dosya veya her türlü zararlı bağlantı içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

j) Zincir mesajlara (spam), sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır, bu mesaj ve e-postalar paylaşılmamalıdır.

k) E-posta içerisinde uygun olmayan içerikler (ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderilmemelidir.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

l) 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.

m) Personel iş ile ilgili yazışmalarında kişisel e-posta hesaplarını (örnek: Gmail, hotmail, yahoo, mynet, vs.) kullanmamalı, aynı zamanda e-postalarının bir kopyasını yönlendirmemelidir.

n) 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.

o) 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.

ö) Gelen e-postada; kullanıcılardan, kullanıcı kodu/parola girmesini isteyen e-postanın sahte e-posta olabileceği dikkate alınarak, gelen bu e-posta herhangi bir işlem yapılmaksızın derhal silinmelidir.

p) 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 yönlendirmemelidir.

r) Kullanıcı, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt vermelidir.

s) Kullanıcı **@ogu.edu.tr** kurumsal e-posta hesabı üzerinden dakikada 50 adetten fazla gönderim yapmamalıdır. Dakikada 50 adedi aşan gönderimler alıcılara iletilmeyecektir.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

ş) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar ESOGÜ BİDB Sistem Yönetimine haber verilmelidir.

t) 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.

u) Kurum tarafından onaylanmış, üretici tarafından desteği devam eden kararlı ve güncel sürüme sahip internet tarayıcıları ile e-posta istemcileri kullanılmalıdır.

ü) E-POSTA KULLANIM TALİMATI gereği toplu e-posta gönderimi yetkisi, yetkiyi talep eden birimlere aittir.

8. Yaptırım

Bu politikanın ihlal edilmesi durumunda Bilgi Güvenliği Birimi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel Bilgi Güvenliği Birimi tarafından e-posta üzerinden yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa 657 sayılı devlet memurları kanunu gereğince personel hakkında işlem yapılır.

9. İlgili Dokümanlar

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

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI