T.C.
İSTANBUL
KÜLTÜR
ÜNİVERSİTESİ

İKÜ BST

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

ELEKTRONİK POSTA KULLANIM POLİTİKASI (EKP)

HAZIRLAYANLAR	KONTROL EDEN	ONAYLAYAN
Ufuk Dikme	İsmail Koç	
Bilgi Güvenliği Yönetim Müdürü	Bilgi Sistemleri ve Teknolojileri Daire Başkanı	Rektörlük Temsilcisi

İÇİNDEKİLER

1. AMAÇ

Bu politikanın amacı, T.C. İstanbul Kültür Üniversitesi "@iku.edu.tr" uzantılı elektronik posta mesajlarında alma, gönderme, yönlendirme ve otomatik gönderme kurallarına ilişkin genel kuralları tanımlamaktır.

2. KAPSAM

Bu politika, T.C. İstanbul Kültür Üniversitesi bünyesinde kurumun sağladığı resmi elektronik posta hesabı olan personeli kapsamaktadır.

3. DAYANAK

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Ek.A.13.2.3 maddesi.
- 5651 numaralı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.
- 6698 numaralı Kişisel Verilerin Korunumu Kanunu
- 15.03.2018 tarihli ve 19924119-719-E.21240 sayılı "2016-2019 Ulusal Siber Güvenlik Eylem Planı" konulu YÖK yazısında, üniversitelerin ISO27001 Bilgi Güvenliği Yönetim Sertifikası alması ve iş süreçlerini bu şekilde yapılandırması gerektiği ifade edilmiştir.

4. TANIMLAR VE KISALTMALAR

KISALTMALAR	TANIMLAR
BSTDB	Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı
E-POSTA	Elektronik Posta
ITSM	Bilgi Sistemleri ve Teknolojileri Servis Yönetim Yazılımı
İKÜ, KURUM	T.C. İstanbul Kültür Üniversitesi
KULLANICILAR	İKÜ'nün altyapı ve kaynaklarını kullanan öğrencileri, öğretim üyeleri, idari personeli, araştırmacıları ve/veya diğer mensuplarıdır. Kullanıcı, İKÜ personeli olmadığı halde, kurum ağ kaynaklarına girişte ve ağa bağlı kaldığı süre içinde, kimlik doğrulaması ve yetkilendirmesi yapılabilen geçici/misafir kullanıcılar da bu grup içindedir.
KVKK	6698 Numaralı Kişisel Verilerin Korunumu Kanunu
PHISHING	Kimlik Avı
SPAM/ZARARLI E-POSTA	Çoğu zaman istenmeyen mesajlar olarak adlandırılan bu elektronik postalar, içeriğinde zararlı yazılımlar taşıyabildiği gibi, zararlı yazılım yayan sitelere de yönlendirme yapabilmektedirler.

ZİNCİR E-POSTA	İletinin gövdesinde veya konusunda, alıcıdan e-postayı birden çok kişiye iletmesini isteyen iletilerdir.

5. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
1	İKÜ BSTDB İşten Ayrılma Prosedürü
2	BGYS Disiplin Prosedürü
3	6698 Numaralı Kişisel Verilerin Korunumu Kanunu

6. ELEKTRONİK POSTA KULLANIM POLİTİKASININ HEDEFLERİ VE PRENSİPLERİ

6.1. İKÜ bünyesinde çalışan tüm personel için kurumsal e-posta (@iku.edu.tr) hesabı tahsis edilir ve tüm iş amaçlı e-postaların kurumsal e-posta hesabı ile gerçekleştirilmesi zorunludur.

6.2. Kullanıcıya resmi olarak tahsis edilen e-posta adresi kişisel çıkar amaçlı kullanılamaz.

6.3. İş dışı konulardaki haber grupları kurumsal e-posta adres defterine eklenemez.

6.4. Kurumun kaynakları üzerinden, kurum içi kullanıcılara veya kurum dışı diğer adreslere Spam ve Phishing mesajlar gönderilemez, bu amaçla kullanılamaz.

6.5. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.

6.6. İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta hesabı kullanılamaz. Ancak iş gereği üye olunması yararlı Internet haber grupları için yöneticisinin onayı alınarak kurumun sağladığı resmi e-posta adresi kullanılabilir.

6.7. Hiçbir kullanıcı, gönderdiği e-posta adresinin Kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.

6.8. Konu alanı boş veya kimliği belirsiz adreslerden gelen, konusunda kullanıcıların bilgilerini talep eden şüpheli hiçbir e-posta açılmaz ve BSTDB'ye bilgi verilir.

6.9. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" veya yasaklanan diğer uzantılar olamaz.

6.10. Farklı kişi veya kurumlara gönderilen e-postaların ekinde şifreli doküman bulunmamalıdır. Dokümanlar ".rar" formatında sıkıştırılarak gönderilebilir. ".exe" uzantılı dosyalar ".rar" formatında sıkıştırılsalar bile gönderilemez.

6.11. İKÜ'ye şifreli olarak gönderilen e-postalar sistem tarafından otomatik olarak karantinaya alınır. Karantinadaki şifreli e-postalar BSTDB Ağ, Güvenlik ve İletişim Müdürlüğü tarafından incelenir. Uygun bulunması durumunda e-postanın iletilmesine izin verilir. Şifreli mesajlaşma zaruri ise izin verilmesi için gönderen ve alan e-posta adresleri BSTDB'ye ITSM üzerinden sebebiyle birlikte bildirilir.

6.12. İKÜ ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamına içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

6.13. Kişisel veriler, gönderilen e-postalarda yer almamalıdır. "IKU KVKK Politikası" na uygun olarak hareket edilmelidir.

6.14. Kurumun e-posta sistemi üzerinden taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajlar gönderilemez. Bu tür özelliklere sahip bir mesaj alındığında BSTDB Ağ, Güvenlik ve İletişim Müdürlüğüne haber verilmelidir.

6.15. Kullanıcı hesapları, doğrudan ya da dolaylı, ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-posta gönderilmesi yasaktır.

6.16. Kullanıcılar, zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-posta aldığında, e-posta başka kullanıcılara iletilmeden BSTDB'ye haber verilir.

6.17. Kullanıcılar, zararlı e-posta, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt vermez.

6.18. Kullanıcı hiçbir suretle kurumsal e-posta ile uygun olmayan içerikler (taraftarlık ve üyelikler, siyasi propaganda, din, dil, ırk, pornografik içerik, fikri mülkiyet içeren malzeme, vb.) gönderemez.

6.19. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Kanunlara göre suç teşkil edebilecek her türlü mesajın içeriğinden kullanıcı sorumludur.

6.20. Kullanıcılar, hesabını/parolasını doğrudan veya web sayfası yönlendirmeleriyle talep eden bir e-posta aldığında, herhangi bir işlem yapmaksızın BSTDB'ye haber verir.

6.21. Kullanıcılar, kurumsal mesajlarına, kurum iş akışının aksamaması için zamanında yanıt verir.

6.22. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmaz ve tehdit unsuru olduğu düşünülen e-postalar BSTDB'ye haber verilir.

6.23. Kullanıcılar, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının çalındığını fark ettiği anda BSTDB'ye haber verir.

6.24. İşten ayrılan personelin e-posta adresi ile ilgili "İKÜ BSTDB İşten Ayrılma Prosedürü" belgesindeki ilgili maddeler esas alınır.

6.25. Kullanıcılar, e-posta işlemleri için kendilerine verilen kotanın dolması durumunda eski e-postalarını arşivler. Eğer arşivleme yapmasına rağmen kotada bir artış olmazsa BSTDB'den kotasının artırılmasını ITSM vasıtasıyla talep eder.

6.26. Kullanıcının arşivlenen elektronik postaları bilgisayarı dışında farklı bir yerde tutulur.

7. ELEKTRONİK POSTA KULLANIM POLİTİKASININ YAPTIRIMLARI

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla "IKU BSTDB Bilgi Güvenliği Disiplin Politikası" ve "IKU BSTDB Bilgi Güvenliği İhlal Olayları Prosedürü" belgelerinde belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır. Bu belgenin yetersiz kaldığı durumlar üniversite makamlarınca değerlendirilir.

8. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar
EKP-001-2.0		6.9. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" veya yasaklanan diğer uzantılar olamaz. ~~Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak yalnızca ".rar" formatında mesaja eklenecektir.~~	Ufuk Dikme
EKP-001-2.0		6.11. (İKÜ'ye) şifreli olarak gönderilen e-postalar sistem tarafından otomatik olarak ~~silinecektir~~ (karantinaya alınır. Karantinadaki şifreli e-postalar BSTDB Ağ, Güvenlik ve İletişim Müdürlüğü tarafından incelenir. Uygun bulunması durumunda e-postanın iletilmesine izin verilir.) Şifreli mesajlaşma zaruri ise izin verilmesi için gönderen ve alan e-posta adresleri BSTDB'ye ITSM üzerinden sebebiyle birlikte bildirilir.	Ufuk Dikme
EKP-001-2.0		6.13. ~~Başkalarına ait olan~~ Kişisel veriler, gönderilen e-postalarda yer almamalıdır. "IKU KVKK Politikası" na uygun olarak hareket edilmelidir.	Ufuk Dikme