VARLIKLARIN KABUL EDİLEBİLİR KULLANIM PROSEDÜRÜ

Kod	BGYS/BP/06
Yayın Tarihi	1.12.2024
Revizyon	00
Revizyon Tarihi	-
Oluşturan	
İmza	

Dağıtım Listesi

Kopya No:	Dağıtılan Kişi	Tarih	İmza	İade	
				Tarih	İmza
1					
1					
1					
1					
1					
1					
1					
1					
1					
1					
1					

Değişiklik Geçmişi

Tarih	Revizyon	Oluşturan	Değişiklik Açıklaması

Hazırlayan **Kontrol** **Onaylayan**

İçindekiler

1. AMAÇ

Bu doküman Üniversitemiz uyulması gereken internet, e-posta, varlık ve sistemlerin genel kullanım kurallarını açıklamak için hazırlanmıştır.

2. KAPSAM

Bu prosedür tüm çalışanlarımızı kapsar.

3. TANIMLAR

Kurum (Üniversite) : İstanbul Gedik Üniversitesi

BGYS : ISO IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi

4. UYGULAMA

4.1 E-Posta Kullanım Kuralları

- ✓ E-posta sistemi sadece iş amaçlı olarak kullanılacaktır.
- ✓ Kullanıcılar kendi e-posta hesaplarından gönderilen e-posta içeriklerinden sorumludur.
- ✓ Özellikle hassas bilgi içeren e-postalar şirket içi ve şirket dışına gönderimlerinden önce bir kaç kez gözden geçirilmelidir.
- ✓ E-posta sistemi kullanılarak kurum itibarını küçük düşürücü, dil, din, ırk, cinsiyet, siyasi görüş ayrımı yapan veya ahlak kurallarına aykırı e-posta içeriği göndermek yasaktır.
- ✓ E-posta sisteminden SPAM (reklam içerikli yada bir mesajın yüksek sayıda kopyasının) içerikli e-posta gönderimi yasaktır.
- ✓ Elektronik posta kutuları için kota uygulaması devrededir. Kullanıcılar kendileri için tanımlanan kota limitine yaklaştıklarında sistem tarafından otomatik olarak uyarılacaktır. Kullanıcılar eski olan tüm e-postalarını arşive taşımakla ve/veya silmekle yükümlüdür.
- ✓ Tüm kullanıcıların üniversitemiz E-posta sunucu altyapısı kullanarak gerçekleştirdiği üniversite içi ve üniversite dışı e-posta yazışmaları şirket politikaları gereği arşivlenmektedir. Üst yönetim herhangi bir bilgilendirmeye ihtiyaç duymadan gerek gördüğü durumda tüm yazışmaları inceleyebilir.
- ✓ Tüm e-postalar SPAM ve zararlı yazılım kontrolünden geçirilmektedir, alınan tüm önlemlere rağmen kullanıcı şüpheli gördüğü Kaynağı bilinmeyen e- posta ekinde gelen dosyalar kesinlikle açmamalı ve derhal silmelidir. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler. Tanınmayan adreslerden gelen epostaları mutlaka açmadan siliniz. (Örnek Türkcell Fatura, PTT Fatura gibi veri şifreleme linkleri olan epostalar.) e-postayı açmadan silerek, Bilgi İşlem Bölümü' nü bilgilendirmelidir.

- ✓ SPAM veya zararlı içerik kontrolü sırasında önemli bilgi içeren e-postalar filtrelemeye takılabilir, kullanıcılar kendilerine gelecek e-postaların takibini gerçekleştirmek ve e-posta sorgulaması için Bilgi İşlem Bölümü' ne talepte bulunmakla yükümlüdür.
- ✓ SPAM veya zararlı yazılım kontrolü en güncel yöntemler ile gerçekleştirilmektedir. Gönderen firma kaynaklı sorunlar sebebi ile Bilgi İşlem Bölümü sorumlu tutulamaz.
- ✓ Çalışanlar şirketin e-posta adresini iş amaçlı web siteleri dışındaki web sitelerine (alışveriş vb.) üye olmak için kullanmayacaktır.
- ✓ Görevden ayrılma vb. sebepler dolayısı ile personelin e-posta hesabının başka bir kullanıcıya yönlendirilmesi sadece ilgili bölüm yöneticisinin yazılı veya e-posta ile onayı sonrasında Bilgi İşlem Bölümü tarafından gerçekleştirilebilir.
- ✓ Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- ✓ E-posta gönderimlerinde konu kısmı boş bırakılmayacaktır.
- ✓ Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar Tarafından görülmesi ve okunmasını engellemekten sorumludurlar,
- ✓ E-posta gönderimlerinde e-posta içeriğinin gizlilik derecesine göre gerekli önlemlerin alınması çalışan sorumluluğundadır.
- ✓ Kullanıcılar kendilerine ait e-posta adresinin şifresinin güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumludurlar. Şifrelerinin kırıldığını fark ettikleri andan itibaren yetkililerle (Bilgi işlem ve/veya ilgili birim yöneticisi) temasa geçip durumu haber vermekle yükümlüdürler.
- ✓ Altı ay süre ile kullanılmayan e-posta kutuları Bilgi İşlem Birimi tarafından kaldırılır. Kurumdan ayrılan personel kurumsal e-posta sistemini kullanamaz.

4.2 İnternet Kullanım Kuralları

- ✓ İnternet altyapısı sadece görev gereği gerekli içeriğe erişmek için kullanılacaktır.
- ✓ Üniversitemiz tarafından sağlanan internet içeriği 5651 sayılı kanun gereklilikleri, üniversitemiz etik değerleri, teknik altyapı göz önüne alınarak belirlenmektedir.
- ✓ Internet erişimi ile ilgili gerekli güvenlik tedbirleri Bilgi İşlem tarafından alınacaktır, fakat internet erişimi olan sistemlerde %100 güvenlik kesinlikle garanti edilememektedir.
- ✓ Kullanıcıların Internet üzerinden program indirmesi yasaktır. Bu konuda bölümlerden gelecek talepler Bilgi işlem bölümü tarafından değerlendirilerek uygun bulunması halinde gözetimli olarak gerçekleştirilecektir.
- ✓ İnternet erişimlerinde alınan güvenlik tedbirlerini atlatmaya yönelik girişimlerin gerçekleştirilmesi yasaktır.

- ✓ Taşınabilir bilgisayar kullanıcıları üniversitemiz dışındaki internet erişimlerinde de bu maddeler içerisinde belirtilen kurallara uymakla yükümlüdür.
- ✓ Servis Sağlayıcılar tarafından sağlanan internet erişimi kullanılarak internet üzerindeki diğer sistemlere servis durdurma vb. saldırılarda bulunulması yasaktır.
- ✓ Hassas (gizli) bilgilerin internet üzerindeki dosya paylaşım sunucuları, e-posta servisleri vb. altyapılar üzerinde saklanması ve transfer edilmesi yasaktır.
- ✓ Kullanıcıların internet üzerindeki tüm aktiviteleri yasa ve iş gereklilikleri gereği kayıt altına alınmaktadır.
- ✓ Şirketin internet alt yapısı kullanılarak şirket itibarını küçük düşürücü, dil, din, ırk, cinsiyet, siyasi görüş ayrımı yapan veya ahlak kurallarına aykırı e-posta içeriği göndermek yasaktır.
- ✓ Bilgi işlem bölümü her hangi bir tehdit tespit ettiği durumlarda kullanıcı bazında veya genel olarak internet erişimini kısıtlayabilir ve/veya engelleyebilir.

4.3 Varlıkların ve Sistemlerin Genel Kullanım Kuralları

- ✓ Taşınabilen bilgi işleyen cihazlar halka açık ortamlarda, araç içinde, toplantı odaları, konferans salonları gibi yerlerde kontrolsüz olarak bırakılmayacaktır.
- ✓ Taşınabilir cihazların fiziksel güvenliğinden varlık/risk sahibi sorumludur.
- ✓ Taşınabilir bilgi işleyen cihazların (üniversite bilgilerini içeren kişisel cihazlar dâhil (Akıllı telefon üzerinden kullanılan uygulamalar (E-posta vb.) çalınması kaybolması durumunda varlık/risk sahibi en kısa süre içerisinde Bilgi İşlem Bölümü' ne bilgi vermekle yükümlüdür.
- ✓ Taşınabilir bilge işleme cihaz sahipleri verilerini düzenli olarak dosya sunucusundaki kendi bölümüne ait kişisel alanlara yedeklemek ile yükümlüdür.
- ✓ Taşınabilir bilgisayarlar diskler üzerindeki arızaları ve veri kayıplarını önlemek için işletim sistemi "Kapalı veya Hazırda Beklet" modunda iken taşıma yapılacaktır.
- ✓ Taşınabilir bilgisayarlar işyerinde bırakılacak ise yangın tehdidine karşı şarjda bırakılmamalıdır.
- ✓ Bilgisayarlar (ofiste bırakıldığı sürece) mesai saatleri dışında mutlaka kapalı konumda muhafaza edilmelidir.
- ✓ Şirket tarafından çalışanlara tahsis edilen bilgisayarlar, diğer bilgi işleme ve saklama cihazları (Telefon, USB Bellek vb.) aile fertleri, arkadaş, dış firma vb. kişilerin kullanımına verilemez.
- ✓ Taşınabilir bilgi işleme aygıtları kullanılarak halka açık ve güvenliğinden emin olunmayan yerlerde kablolu veya kablosuz bağlantılar üzerinden hassas (gizli) şirket bilgileri ile ilgili işlem yapılamaz.

- ✓ Bütün Cep telefonu, PDA (Personel Dijital Asistan), tablet, taşınabilir bilgisayarlar kurumun ğı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, wifi vs.) özellikleri aktif halde olmamalıdır.
- ✓ Ağ güvenliğini (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi)
  veya ağ haberleşmesini bozacak (paket sniffing, paket spoofing, denial of service vs.) ortadan kaldıracak eylemlere girişmemelidir. Port veya ağ taraması yapılmamalıdır.
- ✓ Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır, Şirket bilgilerini kurum dışından üçüncü şahıslara iletilmemelidir.
- ✓ Bilgisayarlarda Telif Hakkı yasası ile korunan (Film – Müzik – Mp3 – Mpg ve diğerleri) Bilgisayara yüklenmesi paylaşılması ve bilgisayarda barındırılması yasaktır. Yükleyenler kanuni yaptırımlar durumunda kendilerinin sorumlu olacaklarını kabul ve beyan ederler.
- ✓ Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Yükleyenler kanuni yaptırımlar durumunda kendilerinin sorumlu olacaklarını kabul ve beyan ederler.

4.4 Temiz Masa Temiz Ekran Politikası

Temiz Masa

- ✓ Tüm çalışanlar kendi masalarının temizliği ve düzeninden sorumludur.
- ✓ Bilgi seviyesi gizli ve üstü olan varlıklar gözetimsiz olarak çalışma ortamlarında bırakılamaz.
- ✓ Masa üzerlerinde sözleşme, müşteri bilgisi, personel bilgisi, muhasebe evrakları gibi evraklar bırakılamaz.
- ✓ Kullanımı biten not kağıtları, fotokopiler, personel özlük bilgileri gibi basılı evraklar müsvedde amaçlı kullanılamaz.
- ✓ Kullanımı biten basılı evraklar kağıt imha makinesi ile imha edilir. İmha işlemi gerçekleşmeden çöpe atılmaz.
- ✓ Her çalışanımız masasının başından ayrılmadan önce masasını kontrol etmelidir.
- ✓ Gizli bilgi içeren basılı veya elektronik dokümanlar kontrolsüz olarak ekranda veya ofis masalarında kontrolsüz olarak bırakılmayacaktır.
- ✓ Gizlilik seviyesi olan tüm bilgi varlıkları kilitli dolaplarda muhafaza edilmelidir.
- ✓ Terk edilmiş masaların üzerlerinde not kâğıtları, kişisel ajandalar ve işle ilgili dokümanlar bırakılmamalıdır.

- ✓ Masa üzerlerinde taşınabilir belek, CD, DVD, mobil telefon gibi veri taşıma ve depolama araçları gözetimsiz bırakılmamalıdır. Bu tarz teçhizatlar kilitli dolaplarda muhafaza edilmelidir.
- ✓ Yazıcılar üzerinde gizli ve üstü bilgi seviyesindeki dokümanlar bırakılmaz.

Temiz Ekran

- ✓ Çalışanlar ekranlarını sadece geçerli olan kullanıcı adı ve şifrelerini kullanarak açabilir,
- ✓ Kullanıcılar bilgisayarlarının başından ayrılmaları gerektiğinde “Ctrl + Alt + Del” veya “Windows + L” tuş birleşimlerini kullanarak oturumlarını kilitleyeceklerdir.
- ✓ Çalışanlar arasında birbirinin kullanıcı bilgilerini paylaşmaları ve kullanmaları yasaktır,
- ✓ Tüm bilgisayarın ekranlarının arka planları ve masa üstü yönetimi BT Ekibi tarafından kontrol edilir.
- ✓ Çalışanlar bilgisayarlarını gözetimsiz ve ekranı açık şekilde bırakamaz
- ✓ Ekran koruyucular otomatik olarak devreye girer ve kapatıldığında kullanıcı ve şifre bilgisi girilmeden bilgisayarlar açılamaz
- ✓ Kuruluşun idari kadrosu kendilerine teslim edilen masaüstü ya da taşınabilir bilgisayarların amaca uygun kullanımı ve güvenliğinden sorumludur.
- ✓ Bilgisayar ekranlarında kuruluşa ait çalışma dosyaları klasörler, herhangi bir formatta bilgi içeren dosyalar ve bunlara ait kısa yollar bulundurulmamalıdır.
- ✓ Yapılan çalışmalar ile ilgili bilgiler ortak ağda ya da ilgili bilgisayarda belirlenen adrese kaydedilmelidir.
- ✓ Bilgisayar ekranlarında zararlı yazılımlara ait kısa yollar, siyasi içerik, ırkçılık, pornografi, erotizm içeren resim, yazı, dosya veya bu içeriklere ait internet sitelerine bağlanan kısa yollar bulundurulmamalıdır.
- ✓ Toplantı sonrasında toplantı odalarındaki tüm evraklar toplanacak, tahta içeriği temizlenecek ve projeksiyon cihazı kapatılacaktır.
- ✓ Ofislerde ve toplantı odalarında bilgisayarlar kontrolsüz şekilde bırakılmayacaktır.

Taşınabilir Ortam Yönetimi

- ✓ Taşınabilir ortam sürücülerinin kullanımı üniversitemiz içinde sınırlandırılmış ve yetkilendirilmiştir. Sadece bir iş nedeni olduğunda BGYS/BF/006 Yetkilendirme ve Talep Formu üzerinden ve ilgili bölüm yöneticisinin onayı sonrasında Bilgi teknolojileri tarafından etkinleştirilmektedir.
- ✓ Sökülüp takılabilen medya güvenli ortamda barındırılmakta ve bilgi zarar görmeyecek şekilde saklanmaktadır.

- ✓ Taşınabilir ortam içinde hassas bilgi (Gizli) saklanırken Tablo-2 de tanımlandığı gibi şifreleme metotları kullanılmaktadır.
- ✓ Kullanılmayan taşınabilir medya (sökülüp takılabilen medya) güvenli bir şekilde tamamen imha/yok edilir. Varlık sahibi imhanın gerçekleştirilmesinden sorumludur.

Ortamın Yok Edilmesi

- ✓ Kullanılmayan hassas bilgi içeren dokümanların, sökülüp taşınabilen medyanın, ortamların (DVD, Usb, Disk ya da Bellek v.b) imhası; kâğıt /DVD kırpma makinası ya da ilgili ortamın yakılması, parçalanması ile yapılır. İmha işlemi tutanak ile kayıt altına alınır.
- ✓ Ortam başka bir uygulama için kullanılacak ise içindeki bilgiler tekrar geriye dönülemeyecek şekilde yöntemler uygulanarak silinir.

Fiziksel Ortam Aktarımı

- ✓ Hassas önemli bilgi içeren ortam aktarım sırasında yetkisiz erişime, bozulmaya ve yetkisiz kullanıma karşı varlık sahibi veya varlık sahibinin yetkilendirileceği kişi tarafından korunarak transfer edilir.
- ✓ Elektronik ve fiziksel çoğaltma ve dağıtım işlemleri bilgi varlıklarının gizlilik derecelerine göre Tablo 2 deki gibi gerçekleştirilecektir.
- ✓ Elektronik dokümanların şifreli gönderiminde ve şifreli olarak saklanmasında Microsoft Office şifreleme özellikleri ve 7zip, zip, rar dosya türü şifreleme yöntemleri kullanılabilir. Şifreler şifre politikalarına uygun olarak karmaşık yapıda olmalı, kolay tahmin edilebilir olmayacaktır.
- ✓ Bilgi Teknoloji altyapısı üzerindeki tüm kullanıcı aktiviteleri kayıt altına alınmaktadır. Kullanıcılar kendileri ile ilgili olmayan elektronik dokümanları şifresiz olarak bulsa dahi erişme, çoğaltma ve transfer etme girişimlerinde bulunmayacaklardır.

Varlıkların Teslimi

Tüm çalışanlar ve dış tarafların kullanıcılarının istihdamlarının, sözleşme veya anlaşmalarının başlamasının ardından tüm kurumsal varlıklar ilgili hususlar aşağıdaki gibi tanımlanmış ve uygulanmaktadır.

- ✓ İşten başlayan personele tüm varlıklar İnsan Kaynakları Bölümü tarafından zimmet formu ile imza karşılığı verilir.
- ✓ Kullanıcıya ERP ve Mail adresi açılması mail ya da form ile ilgili birimden bölüm yöneticisi veya IK birini tarafından talep edilerek açılması sağlanır.

Varlıkların İadesi

Tüm çalışanlar ve dış tarafların kullanıcılarının istihdamlarının, sözleşme veya anlaşmalarının sonlandırılmasının ardından ellerinde olan tüm kurumsal varlıkların iadesi ile ilgili hususlar aşağıdaki gibi tanımlanmış ve uygulanmaktadır.

- ✓ İşten ayrılan personelin sorumlu olduğu varlıklar ilgili birim tarafından zimmet formu veya tutanak ile imza karşılığı geri alınır.
- ✓ Halen devam etmekte olan bir proje ile ilgili bilgi mevcut ise bu bilgi dokümante edilerek gerekli durumlarda ayrıca sözlü olarak ilgili bölüm yöneticisine teslim edilir.
- ✓ Personel Daire Başkanlığı tarafından öncesinde Bilgi İşlem Daire Başkanlığına bildirimi yapılan çalışan ayrılma-ayırma işlemleri esnasında bilgilerin yetkisiz kopyalanmasını engelleyici tedbirler alınır.

5. YÜRÜRLÜLÜK

Bu prosedür yayımlandığı tarihten itibaren yürürlüğe girer, Üniversitemiz bu prosedürü gerektiği zaman kısmen ve/veya tamamen değiştirebilir veya yürürlükten kaldırabilir. Prosedürü tamamen veya kısmen yürürlükten kaldırma yetkisi Üst Yönetime aittir. Bu kapsamda değiştirilen ve/veya kaldırılan hükümler, kazanılmış hak oluşturmaz.

6. EK