



Varlıkların Kabul Edilebilir Kullanımı Prosedürü



## Varlıkların Kabul Edilebilir Kullanımı Prosedürü

### DEĞİŞİKLİK TAKİP LİSTESİ

| No | Tarih | Açıklama  |
|----|-------|-----------|
| 00 |       | İlk Yayın |

### İÇİNDEKİLER

|                   |   |
|-------------------|---|
| 1. AMAÇ.....      | 2 |
| 2. KAPSAM.....    | 2 |
| 3. UYGULAMA ..... | 2 |

## 1. AMAÇ

Bu doküman son kullanıcıya verilen bilgi varlıklarının hangi şartlarda kullanılacağını belirlenmesi için oluşturulmuştur.

## 2. KAPSAM

Bilgi İşlem Daire Başkanlığı

## 3. UYGULAMA

- 3.1.1. Sistem Odalarında fotoğraf çekmek, ses kaydı yapmak yasaktır.
- 3.1.2. Kullanıcılar içecek maddelerini bilgisayar ve ofis araçlarından uzak tutmalıdır. Yiyecek, içecek veya gıda malzemelerini bilgisayar ve ofis araçlarının yanında tüketmemelidir.
- 3.1.3. Kullanıcılar hassas özelliği olan sunucu, sistem odaları veya katlarına özel ziyaretçi kabul edemezler.
- 3.1.4. UPS hattı üzerindeki prizlerde klima, ısıtıcı, su ısıtıcıları (kettle) gibi elektrikli cihaz kullanımı yasaktır.
- 3.1.5. Kullanıcılar, hassas özelliği olan oda veya katlarda geçici çalışma gerekleri ile gelmiş yüklenici veya 3. taraf çalışanlarını refakatçisiz bırakamaz.
- 3.1.6. Kullanıcılar masalarını terk ederken hassas bilgi içeren basılı bilgileri açıkta bırakamazlar. Masa başından ayrılacağı zaman hassas bilgi içeren belgeler kilitli ortamlarda saklanacaktır.
- 3.1.7. Kullanıcılar bilgisayarları başından ayrılırken ekranlarını koruma altına alacaklardır.
- 3.1.8. Pamukkale Üniversitesi personeli genel olarak kurumsal etik, nezaket kurallarına uymalı, kurum çalışanlarına müşteri ve diğer tarafları karalayıcı, hakaret içeren ifadeler kullanmamalıdır.
- 3.1.9. Çalışmalarında yasal, anlaşmadan doğan yükümlülüklerle uygun davranmalıdır.

### 3.2. Kullanıcı Bilgi Güvenliği Roller ve Sorumlulukları

- 3.2.1. Bilgi Güvenliği Yönetim Sistemine uygun davranmak.
- 3.2.2. Kendisine emanet edilen donanımlarla birlikte iş ile ilgili olan varlıkların güvenliğini temin etmek.
- 3.2.3. Bilgi güvenliği konusunda, ihlal olaylarını ilgili makamlara raporlamak.

### 3.3. Erişim Hakları

- 3.3.1. Pamukkale Üniversitesi personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş cihazları korumaktan sorumludur. Erişim bilgileri herhangi bir kişi ile paylaşılamaz.
- 3.3.2. Tüm çalışanlar, 3. taraf kullanıcılar ve yüklenici personeli, Pamukkale Üniversitesi içinde çalışırken “Erişim Kontrolü Politikası”na tabidirler.

### 3.4. Taşınır / taşınmaz Bilgisayar Kullanımı

- 3.4.1. Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz.
- 3.4.2. Dizüstü bilgisayarlar ekran ve klavyesi arasında herhangi bir şey yok iken kapatılmalıdır. Dizüstü bilgisayarın ekran kapağı kapatılırken klavye üzerinde bir şey kalmadığına emin olunmalıdır. Aksi durumda oluşacak zararlardan kullanıcı sorumludur.
- 3.4.3. Hiçbir personel, kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.

- 3.4.4. CD, DVD, blueray, flash disk, harici disklerden doküman alınacak veya yazılım kurulacak ise bu ortamlar virüs taramasından geçirilir.
- 3.4.5. Kullanıcılar teknik olarak mümkün olsa bile taşınır/taşınmaz bilgisayarlarındaki güvenlik ayarlarını değiştiremezler veya seviyelerini düşüremezler.
- 3.4.6. Seyahat sırasında kullanılan Pamukkale Üniversitesi'ne ait taşınabilir bilgisayarların kayıp edilmemesine ve açık iken gözetimsiz bırakılmamasına önem gösterilecektir.
- 3.4.7. Taşınabilir bilgisayarın kaybolması durumunda, zaman kaybetmeden Bilgi İşlem Yönetimine haber verilecektir. Sisteme uzaktan erişim hakları iptal edilecektir.
- 3.4.8. Yönetim tarafından belirlenen ortak kullanım bilgisayarlar hariç, kullanacağı zimmetli taşınabilir bilgisayarlar, kullanılmak üzere bir başka personel veya kurum dışı bir kişiye verilemez, verilmesi gereken durumlarda yöneticisinden izin alınması gerekmektedir.
- 3.4.9. Masaüstü ve taşınabilir kasalarının yetkili bilgi işlem elemanları veya yetki verilmiş firma elemanları dışında açılması yasaktır.
- 3.4.10. Masaüstü bilgisayar kasalarının havalandırma mekanizmalarının kapanmayacak şekilde yerleştirilmesine özen gösterilmelidir.
- 3.4.11. İnternet üzerinden veya e-posta ile gelmiş olan zararlı programları (solucan, truva atı gibi) indirmek, kurum bünyesinde oluşturmak ve dağıtmak yasaktır.
- 3.4.12. Bilinmeyen ve güvenilmeyen Flash disk, cd, dvd'ler pc'lere takılmamalıdır.
- 3.4.13. Bilişim ağlarına zarar verecek veya bilgi sızmasına yol açacak yazılımların tamamının son kullanıcı tarafından bilgisayarlarına kurulması yasaktır.

### 3.5. Tarama Kuralları

- 3.5.1. Sistem ve Bilişim Ağları Şube Müdürlüğü personeli dışında hiçbir personel Bilgi İşlem Biriminden izin almadan kendi bilgisayarından veya başka bir kaynak kullanarak, Pamukkale Üniversitesi'nin ağını tarayamaz, izleyemez veya dinleyemez.
- 3.5.2. Sistem ve Bilişim Ağları Şube Müdürlüğü ve Pamukkale Üniversitesi onaylı resmi penetrasyon testleri haricinde, Pamukkale Üniversitesi bilgisayar sunucuları için içeriden veya dışarıdan port taraması yapılması yasaktır.
- 3.5.3. Pamukkale Üniversitesi adına iş yapan yüklenici firma personeli; Pamukkale Üniversitesi'nin izni ve onayı olmadan Pamukkale Üniversitesi bilgilerini başkaları ile paylaşamaz. Pamukkale Üniversitesi'nin izni olmadan iç ağ ve internet üzerinden web servislerini tarayamaz ve sızma testleri gerçekleştiremez.

### 3.6. İnternet Kullanımı

- 3.6.1. Pamukkale Üniversitesi'ne ait olmayan bilgisayarlar sadece kurum kullanıcı hesabını kullanarak internete bağlanabilirler.
- 3.6.2. Kullanıcılar internet üzerindeki sohbet odalarına, tartışma gruplarına ve diğer forumlara yazmaları durumunda kurum ve şahısların mahremiyetini korumalı, kurum iletişim bilgilerini personel isimlerini, unvanlarını özellikle kurumsal e-posta adreslerini paylaşmamalıdır.
- 3.6.3. Kullanıcılar sistem Yöneticisi tarafından özellikle onay verilmemesi dışındaki durumlarda internetten yazılım, veri, ses ve görüntü dosyası indiremez.
- 3.6.4. Kullanıcılar İçerik Filtreleme Kurallarına aykırı olarak engellenmiş yasaklanmış içeriklere erişimi zorlayamaz.

3.6.5. Kurum interneti Sistem ve Bilişim Ağları Şube Müdürlüğü bilgisi dışında herhangi bir donanım veya yazılım vasıtasıyla çoğaltılıp kullanılamaz.

### 3.7. E-posta Kullanımı

- 3.7.1. İlgili taraflarla yapılacak e-posta yazışmaları kullanıcının adı, soyadı, unvan bilgilerini içeren imza satırı yazılmadan yapılamaz.
- 3.7.2. Kurum kullanıcılarının e-posta adreslerine gelen istenmeyen e-posta ve virüs eklentilerini indirmemeli ve açmamalıdır.
- 3.7.3. Kullanıcı e-posta kutularına gelen spam, zincir ve junk e-postaları kullanıcılar tarafından silinmelidir.

### 3.8. Parola Kullanımı

- 3.8.1. Pamukkale Üniversitesi sistemlerinde parola kullanım şekli, “Parola Politikası”nda tanımlanmıştır. Hiçbir çalışan parola politikasında belirtilen kuralların dışına çıkamaz.

### 3.9. Yedekleme Kuralları

- 3.9.1. Kullanıcılar, her türlü olumsuz ihtimale karşı işletim sisteminin çökmesi, donanımsal arıza oluşması vb. durumlarda sorun yaşanmaması için uygun periyotlarda önemli dosyalarının yedeklerini almalıdır.

### 3.10. Bilgi Değişim Kuralları

- 3.10.1. Pamukkale Üniversitesi’nin “Gizli” olarak belirlediği bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Kurumun iş gereksinimleri dışında bu bilgilerin kopya edilmesi ve iletilmesi yasaktır.
- 3.10.2. Kurum içi bilgi paylaşımı sadece görev gereği ilgili veriye erişmesi gereken kullanıcılar arasında olmalıdır.
- 3.10.3. Bilgi paylaşımında “herkese gerektiği kadar” ilkesi çerçevesinde bilgi paylaşılır.
- 3.10.4. Kolluk kuvvetleri ve kamu kurumları ile ilgili bilgi paylaşımı resmi yollarla yapılır.
- 3.10.5. Kullanıcılar kendileri ile ilgili iş verilerinin sahibi olup bu varlıkların korunmasından nihai olarak sorumludur.
- 3.10.6. Pamukkale Üniversitesi çalışanları hassas bilgileri içeren konulara ilişkin görüşmeleri kurum dışında telefon ile yapmamaya özen göstermelidir.
- 3.10.7. Kurumsal web sitesi ve sosyal paylaşım sayfasından yapılan yayınlar da dâhil olmak üzere halka aktarılabilecek bilgiler sadece üst yönetim tarafından onaylanarak, aktarım yapacak birime e-posta ile bildirilir.
- 3.10.8. Verilerin gizli, hizmete özel, tasnif dışı sınıfları üst yönetim tarafından tanımlanır. “Varlık Yönetimi Prosedürü” uygulanır.
- 3.10.9. Pamukkale Üniversitesi’nde çalışan personel kendine zimmetlenmiş bilgi işlem cihazları üzerinden ilgili bilgiyi gerekli haller dışında hiç kimse ile paylaşamaz.

### 3.11. Yazıcı / Fotokopi / Faks Kullanımı ve İmha Kuralları

- 3.11.1. Kullanıcılar bir dokümanı ortak alandaki yazıcı/fotokopi üzerine gönderdikten sonra çıktıları makine üzerinde bırakmamalıdır. Derhal gidip çıktıları almalıdırlar.
- 3.11.2. Telif hakları ile korunan dokümanlar kurum fotokopi makinesi ile çoğaltılamaz ve dağıtılamaz.



## Varlıkların Kabul Edilebilir Kullanımı Prosedürü

3.11.3. Kullanıcılar ve yöneticiler, gereksinimi ortadan kalktığında, tüm basılı belgelerini, CD / DVD gibi ortamları güvenli ve emniyetli bir biçimde imha edeceklerdir.

### **3.12. Kurum personeline ait veya kurum tarafından verilen mobil cihazların kullanımı kuralları**

- 3.12.1. Mobil cihazlara erişimde mutlaka parola kullanılır.
- 3.12.2. Mobil cihaz üzerinde hassas veri tutulmaz.
- 3.12.3. Kurum tarafından verilen mobil cihazların envanteri tutulur.
- 3.12.4. Kurum tarafından verilen mobil cihazlar üzerinden sistemlerin güncellemeleri düzenli olarak kontrol edilmelidir.
- 3.12.5. Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmaz.
- 3.12.6. Kaybolması ve çalınması durumunda sistem yöneticilerine haber verilir ve tüm erişim hakları kaldırılır.
- 3.12.7. Çalışanların kendi mülkiyetinde olan mobil cihazları üzerine kurulan kurumsal uygulamaların güncellenmesi, yamaların yüklenmesi veya uygulamaların değiştirilmesinden kaynaklanan veri kayıplarından / sistem çökmelerinden kurum mesul değildir.

### **3.13. Müşteri / ziyaretçi / tedarikçilerin kendilerine ait mobil cihazlarının kullanım kuralları**

- 3.13.1. Kurum içinde müşteri / tedarikçi ve ziyaretçi mobil cihazları kritik öneme sahip mekanlar hariç (sistem odaları, kamera izleme yerleri, enerji odaları, arşiv vs) kullanımı serbesttir.
- 3.13.2. Kurum içinde ziyaretçilerin, tedarikçilerin, müşterilerin mobil cihazlarının kurum wi-fi ağlarına bağlanmaları yasaktır.

**AD SOYAD**

**İMZA**