	BİLGİ SİSTEMLERİ GENEL KULLANIM POLİTİKASI		
Doküman No: PLT.01	**Yayın Tarihi:** 25.04.2022	**Revizyon Tarihi:** -	**Revizyon No:** -

1. AMAÇ

Muğla Sıtkı Koçman Üniversitesi bünyesindeki bilişim cihazlarının ve yazılımlarının uygun kullanımı hakkında standart oluşturmayı amaçlamaktadır.

2. KAPSAM

Bu politika kurum adı altında çalışan bütün kişileri ve kurumun sahip olduğu ve kiraladığı bütün cihazları kapsamaktadır.

3. KISALTMALAR

Bu prosedürde geçen;

3.1. MSKÜ: Muğla Sıtkı Koçman Üniversitesi'ni ifade eder.

4. TANIMLAR

5. SORUMLULUKLAR

MSKÜ'nün bilgi sistemlerini kullanan tüm kullanıcıları kapsamaktadır.

6. UYGULAMA

Genel kullanım ve sahip olma ile güvenlik ve kişiye ait bilgiler aşağıdaki gibi açıklanmıştır.

6.1. Genel Kullanım ve Sahip Olma

a) Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da kurumun bünyesinde oluşturulan tüm veriler kurumun mülkiyetindedir.
b) Kullanıcılar bilgi sistemlerinden kendi kişisel kullanımları için makul seviyede yararlanabilirler.
c) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmelidir.
d) Güvenlik ve ağın bakımı amacı ile yetkili kişiler cihazları, sistemleri ve ağ trafiğini burada tanımlanan politikalar çerçevesinde gözlemleyebilir. Kurum, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
e) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalıdır ve kopyalanmamalıdır.
f) Bilgisayarlar üzerinden işle ilgili belgeler, resmî belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
g) Kurumda sorumlu bilgi işlem personeli ve ilgili teknik personel dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeler hiçbir surette değiştirilmemelidir.
h) Bilgisayarlara hiçbir surette lisanssız program yüklenmemelidir.

Hazırlayan	Kontrol Eden	Onaylayan
Bilgi Güvenliği Ekibi	Bilgi İşlem Daire Başkanlığı	Rektör Yardımcısı

i) Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Kaynakların paylaşıma açılması halinde de mutlaka şifre politikasına göre hareket edilmelidir.

6.2. Güvenlik ve Kişiye Ait Bilgiler

a) Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim hakları tanımlanmalıdır.
b) Şifreleri güvenli bir şekilde saklamalı ve hesap bilgileri başka kimselerle paylaşılmamalıdır. Sistem seviyeli şifreler ve kullanıcı seviyeli şifreler yılda en az bir kez değiştirilmelidir.
c) Bütün PC ve Laptoplar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.
d) Bilgisayarlar güvenlik açıklarına karşı korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.
e) Bilgisayarın çalınması / kaybolması durumunda, durum fark edildiğinde en kısa zamanda yetkili kişiye haber verilmelidir.
f) Kuruma ait cep telefonu, tablet ve el terminali cihazlarının gerekli güvenlik tedbirlerini almaktan cihaz kullanıcısı sorumludur.
g) Kullanıcılar bilinmeyen kimselerden gelen dosyaları açmamalıdır. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilir.
h) Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve gerekirse dosyalar sıkıştırılmalıdır.

6.3. Uygunsuz Kullanım

Genel olarak aşağıdaki eylemler yasaklanmıştır. Sistem yöneticileri bu kapsamın dışında olabilir. Herhangi bir kullanıcı kurumun kaynaklarını kullanarak hiçbir şart altında herhangi bir yasadışı aktivitede bulunamaz.

6.3.1. Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler hiçbir istisna olmadan standartlaştırılmıştır.

a) Herhangi bir kişi veya kuruma ait verilerin izinsiz kopyalanması,
b) Kitapların izinsiz kopyalanması, magazinlerdeki fotoğrafların dijital formata dönüştürülmesi, lisans gerektiren yazılımların kopyalanması,
c) Zararlı programların ağa veya sunuculara bulaştırılması,
d) Kullanıcıların kendi hesabının şifresini başkalarına vermesi veya kendi hesabını kullandırması,
e) Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılması,
f) Ağ güvenliğinin etkilenmesi, ağ haberleşmesinin bozulması,

g) Kullanıcı kimlik tanıma yöntemlerinden kaçılması,
h) Program/script/komut kullanarak kullanıcının bağlantısını etkilemesi,
i) Kurum bilgilerinin kurum dışından üçüncü şahıslara iletilmesi,
j) Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programların kurulması ve kullanması yasaktır.

6.3.2. E-mail ve Haberleşme Aktiviteleri

a) Kurum dışından web posta sisteminin güvenliğinden emin olunmayan bir bilgisayardan kullanılması,
b) İstenilmeyen e-posta mesajlarının iletilmesi (Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren mailler olabilir),
c) E-posta veya telefon vasıtası ile taciz edilmesi,
d) E-posta başlık bilgilerinin yetkisiz kullanılması veya değiştirilmesi,
e) Zincir e-postaların oluşturulması veya iletilmesi,
f) Yetkili kişilerin izni olmadan haber gruplarına iletilmesi yasaktır.

6.4. Yaptırım

Kurumsal Bilgi Güvenlik Politikalarının ihlali durumunda çalışan personel ise personel yönetmeliğince belirlenmiş disiplin süreçleri, tedarikçi kurum ise sözleşmelerle ve yasalarla belirtilen kanunlar ve ilgili maddeleri esas alınarak işlem yapılır.

7. İLGİLİ DOKÜMANLAR

-