## 1. Amaç

Bu politikanın amacı, MŞÜ bünyesinde yer alan bilgi sistemlerinin genel kullanım esaslarının tanımlanmasıdır.

## 2. Kapsam

MŞÜ bünyesinde çalışan tüm personel bu politika kapsamındadır.

## 3. Sorumlular

Politikanın uygulanmasından tüm MŞÜ personeli sorumludur.

## 4. Kurallar

### 4.1 Genel Kurallar

- Kurum bünyesinde oluşturulan tüm verilerin kurum mülkiyetinde olduğu düşünülmelidir.
- Güvenlik sistemlerinin kontrolü amacıyla yetkili bilgi işlem personeli cihazları, sistemleri ve ağ trafiğini gözlemleyebilir.
- Kurum ağları ve sistemleri periyodik olarak denetlenmelidir.
- Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/kopyalanmamalıdır.
- Bilgisayarlar üzerinden iş ile ilgili dosyalar ve uygulamalar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- Kurum yetkililerinin bilgisi olmadan ağ sisteminde sunucu (web hosting servisi, e-posta servisi vb.) nitelikli bilgisayar bulundurulmamalıdır.
- Bilgi sistemlerindeki değişiklikler prosedürlere uygun yapılmalıdır.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde bu süreç kontrollü olarak uygulanmalıdır.
- Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim yetkileri tanımlanmalıdır.
- Parolalar güvenli bir şekilde tutulmalı ve hesaplar başka kimselerle paylaşılmamalıdır.
- Sistem seviyeli şifreler 6 ayda bir kullanıcı seviyeli şifreler ise 2 ayda bir değiştirilmelidir.
- Bütün bilgisayar ve benzeri araçlar otomatik olarak en fazla 3 dakika içerisinde parolalı ekran korumasına geçebilmelidir.
- Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar. Çünkü bu e-postalar virüs, e-posta bombaları ve truva atı gibi zararlı kodları ve kötücül yazılımları

içerebilirler.

- Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar.
- E- posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve gerekirse dosyaların sıkıştırılması sağlanmalıdır.
- E-posta gönderiminde birbirini görmesi gerekmeyen toplu maillerde TO yerine BCC yapılarak gizli gönderim sağlanmalıdır.

### 4.2 Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler kesinlikle yasaklanmıştır.

- Herhangi bir kişinin veya kurumun uygulamalarını izinsiz kopyalamak, ticari sır, patent veya diğer şirket bilgileri, yazılım lisanları vs. haklarını çiğnemek.
- Kitapları izinsiz kopyalamak, magazinlerdeki fotoğrafları dijital formata dönüştürmek, lisans gerektiren yazılımları kopyalamak.
- Zararlı programları (örnek: virüs, solucan, truva atı, e-posta bombaları vs.) ağa veya sunuculara bulaştırmak.
- Kurum kaynaklarını kullanarak herhangi bir yasadışı aktivitede bulunmak,
- Kişisel hesap şifrelerini başkalarına vermek veya kişisel hesaplarını kullandırmak.
- Kurum bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmak.
- Ağ güvenliğini etkilemek (örnek: bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket spoofing, denial of service vs.).
- Yetkili kişilerin bilgisi dışında port veya ağ taraması yapmak.
- Kullanıcı kimlik tanıma yöntemlerinden kaçmaya çalışmak.
- Program/script/komut kullanarak kullanıcının bağlantısını etkilemek.
- Kurum bilgilerini, Kişisel Verilerin Korunması Kanunu çerçevesinde tanımlanmış kişisel verileri kurum dışından üçüncü şahıslara iletmek.
- Gizlilik, bütünlük veya erişilebilirlik değeri yüksek veya daha üstü olan cihaz, yazılım veya bilgiyi izinsiz olarak kurum dışına çıkarmak.

### 4.3 E-posta ve Haberleşme Aktiviteleri

Aşağıdaki aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.

- Güvenliğinden emin olunmayan bir bilgisayardan web e-posta sistemi kullanmak.

- İstenilmeyen e-posta mesajlarının iletmek (Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren e-postalar, spam e-postalar olabilir).
- E-posta veya telefon vasıtası ile taciz etmek.
- E-posta başlık bilgilerini yetkisiz kullanmak veya değiştirmek.
- Zincir e-postaları oluşturmak veya iletmek.
- İş ile alakalı olmayan mesajları birçok haber gruplarına iletmek.

### 4.4 Diğer Bilgi Sistem Aktiviteleri

- Cep telefonu ve kurum telefonlarıyla iletişimdeyken karşıda konuşulan kişinin o olduğuna dikkat etmek
- Kalabalık ve geniş kitleli ortamlarda telefonla yapılan iletişim esnasında başkaları tarafından duyulmaması gerekli bilgileri konuşmamak
- Mobil cihaz üzerinden kullanılan iletişim uygulamaları (örn: whatsapp, skype, turkcell bip vb) üzerinde paylaşılan bilgiler içinde bilgi güvenliği kriterlerine uyum sağlamak
- Yazıcı, tarayıcı vb. sistemler üzerinden yapılan her türlü kullanımlarda bilgi güvenliği kriterlerine uyum sağlamak

## 5. Yaptırım

Bu politikanın ihlal edilmesi durumunda İdare tarafından gerekli teknik 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 yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Tüm kullanıcılar güvenlik ihlali olaylarını ve bu politikanın ihlallerini en kısa sürede ilgili birimlere bildirme sorumluluğundadır.

| Hazırlayan | Kontrol Eden | Onaylayan |
|---|---|---|
| EFRAİM YILDIZ | CENGİZ ALMAZ | İHSAN TUĞAL |