



**T.C**  
**NECMETTİN ERBAKAN ÜNİVERSİTESİ**  
**BİLGİ SİSTEMLERİNİN GENEL KULLANIMI PROSEDÜRÜ**

DOKÜMAN NO: PR-045

YAYIN TARİHİ:01.08.2018

REVİZYON NO: 01

REVİZYON TARİHİ: **01.10.2021**

SAYFA NO 1 / 4

### **1. Amaç – Kapsam**

Kurumumuz bünyesindeki bilişim cihazlarının amaçları doğrultusunda kullanımı hakkında kuralları tanımlamaktır. Kurumumuzun sahip olduğu bütün cihazlar da kapsam dâhilindedir. Bu prosedür kapsamında kurumumuzun bütün çalışanları yer almaktadır.

### **2. Sorumlular**

Bu prosedürün oluşturulmasından ve uygulanmasından BGYS ekibi sorumlu olup bütün çalışanlarımız da söz konusu kurallara uymakla yükümlüdür.

### **3. Uygulama**

Kurumumuz bünyesindeki kullanılan bilişim cihazlarının uygunsuz kullanımı virüs saldırılarına, ağ sistemlerinin çökmesine, hizmetlerin aksamasına sebep olabilir ve bunlar yasal yaptırımlara dönüşebilir. Kurumumuzun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurumumuz, bilerek veya bilmeyerek yapılan yasadışı veya zararlı eylemlere karşı hem çalışanlarını hem de kendi haklarını korumaya adanmıştır. Bilişim ile alakalı sistemler (bilgisayar, yazılım, işletim sistemleri, kayıt cihazları, e-mail, www, ftp vs) kurumumuzun sahip olduğu varlıklardır. Bu sistemler kurumumuzun ve çalışanlarımızın menfaatleri doğrultusunda kullanılmalıdır. Güçlü bir güvenlik ancak bütün çalışanların içerisine dahil olduğu takım çalışmasıyla oluşturulabilir. Bu itibarla, bütün kullanıcılar günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.

### **Genel Kullanım ve Sahip Olma**

- a) Kurumumuzun bünyesinde oluşturulan tüm veriler kurumumuzun mülkiyetinde olduğu düşünülmelidir.
- b) Çalışanlar bilgi sistemlerini kendi kişisel kullanımı için makul seviyede yararlanabilirler. BGYS TEMSİLCİSİ bilgi sistemlerinin kişisel kullanımı için gerekli kuralları koymalıdır. Bgys temsilcisi böyle bir kural koymamış ise kurumumuzun koyduğu genel güvenlik prosedürleri geçerlidir.
- c) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmelidir.
- d) Güvenlik sistemlerinin ve bilgisayar ağının bakımı amacıyla yetkili kişiler cihazları, sistemleri ve ağ trafiğini “Güvenlik Açıkları Tespit Etme Prosedürü” çerçevesinde gözlemleyebilir.
- e) Kurumumuz, bu prosedür çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir. Bütün bilgisayarlarda kişisel parola sistemi olmalıdır.
- f) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
- g) Bilgisayarlar üzerinden iş ile ilgili dosyalar ve uygulamalar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- h) BGYS TEMSİLCİSİNİN bilgisi olmadan Ağ sisteminde sunucu (web hosting servisi, e-posta servisi vb.) nitelikli bilgisayar bulundurulmamalıdır.
- i) Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.



**T.C**  
**NECMETTİN ERBAKAN ÜNİVERSİTESİ**  
**BİLGİ SİSTEMLERİNİN GENEL KULLANIMI PROSEDÜRÜ**

DOKÜMAN NO: PR-045

YAYIN TARİHİ:01.08.2018

REVİZYON NO: 01

REVİZYON TARİHİ: 01.10.2021

SAYFA NO 2 / 4

- j) Gereksizlikçe bilgisayar kaynakları paylaşımına açılmamalıdır, kaynakların paylaşımına açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

### Güvenlik ve Kişiyeye Ait Genel Kurallar

- a) Bilgi sistemlerinde bulunan kritik bilgilere yetkisiz kişilerin erişimini engellemek için gerekli erişim yetkileri tanımlanmalıdır.
- b) Şifreler güvenli bir şekilde tutulmalı ve hesaplar başka kimselerle paylaşılmamalıdır.
- c) Bütün PC ve laptoplar otomatik olarak 10 dakika içerisinde şifreli ekran korumasına geçebilmelidir.
- d) Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri ve gerekirse Bios şifreleri aktif hale getirilmelidir. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır.
- e) KULLANICI Cep telefonlarında Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, vs) özellikleri aktif halde olmamalıdır ve mümkünse anti-virus programları ile yeni nesil viruslere karşı korunmalıdır.
- f) Çalışanlar tarafından haber gruplarına gönderilen maillerde şöyle bir açıklama olmalıdır.

#### Yasal Uyarı:

*Bu e-posta'nin içerdiği bilgiler (ekleri de dahil olmak üzere) gizlidir NECMETTİN ERBAKAN ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI onayı olmaksızın içeriği kopyalanamaz, üçüncü kişilere açıklanamaz veya iletilemez . Bu mesajın gönderilmek istendiği kişi değilseniz (ya da bu e-posta'yı yanlışlıkla aldıysanız), lütfen yollayan kişiyi haberdar ediniz ve mesajı sisteminizden derhal siliniz. NECMETTİN ERBAKAN ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI, bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda bir garanti vermemektedir. Bu nedenle bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından, saklanmasından sorumlu değildir. Bu mesajın içeriği yazarına ait olup, NECMETTİN ERBAKAN ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI'nin görüşlerini içermeyebilir.*

#### Disclaimer:

*This e-mail (including any attachments) may contain confidential and/or privileged information. Copying, disclosure or distribution of the material in this e-mail without NECMETTİN ERBAKAN ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI's authority is strictly forbidden. If you are not the intended recipient (or have received this e-mail in error), please notify the sender and delete it from your system immediately. NECMETTİN ERBAKAN ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI makes no warranty as to the accuracy or completeness of any information contained in this message and hereby excludes any liability of any kind for the information contained therein or for the information transmission, reception, storage or use of such in any way whatsoever. Any opinions expressed in this message are those of the author and may not necessarily reflect the opinions of NECMETTİN ERBAKAN ÜNİVERSİTESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI*

- a) Bilgisayar ağına bağlı bütün bilgisayarlar düzenli olarak güncel anti-virus yazılımı ile taranmalıdır.



**T.C**  
**NECMETTİN ERBAKAN ÜNİVERSİTESİ**  
**BİLGİ SİSTEMLERİNİN GENEL KULLANIMI PROSEDÜRÜ**

DOKÜMAN NO: PR-045

YAYIN TARİHİ:01.08.2018

REVİZYON NO: 01

REVİZYON TARİHİ: 01.10.2021

SAYFA NO 3 / 4

- b) Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar. Çünkü bu mailler virus, e-mail bombaları ve Truva atı gibi zararlı kodları içerebilirler.
- c) Bütün kullanıcılar ağıın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve gerekirse dosyaların sıkıştırılması gerekmektedir. Video streaming izin verilmemektedir.
- d) Bütün kullanıcılar kendi bilgisayarının güvenliğinden sorumludur. Bu bilgisayarlardan kuruma veya kişiye yönelik saldırılardan kaynaklanabilecek zararlardan (örnek, elektronik bankacılık vs.) sistemin sahibi sorumludur.

### Sistem ve Ağ Aktiviteleri

Aşağıdaki aktiviteler kesinlikle yasaklanmış olup sistem yöneticileri bilgisayar ağını denetlemek amacıyla aşağıda belirtilen bazı işlemleri uygulayabilir.

- a) Herhangi bir kişi veya kurumun uygulamalarını izinsiz kopyalamak, ticari sır, patent veya diğer kurum bilgileri, yazılım lisansları vs haklarını çığnemek.
- b) Kitapları izinsiz kopyalamak, magazinlerdeki fotoğrafların dijital formata dönüştürmek, lisan gerektiren yazılımları kopyalamak.
- c) Zararlı programların (örnek, virus, solucan, truva atı, e-mail bombaları vs) ağa veya sunuculara bulaştırılmak.
- d) Kurumumuzun kaynaklarını kullanarak herhangi bir yasadışı bir aktivitede bulunmak,
- e) Kişisel hesap şifrelerini başkalarına vermek veya kişisel hesaplarının kullandırmak. Bu, evden çalışırken aile bireylerini de kapsamaktadır.
- f) Kurumumuzun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karıştırmak.
- g) Ağ güvenliğini etkilemek (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket sniffing, paket spoofing, denial of service vs.).
- h) Port veya ağ taraması yapmak.
- i) Kullanıcı kimlik tanıma yöntemlerinden kaçmaya çalışmak.
- j) Program/script/ komut kullanarak kullanıcının bağlantısını etkilemek.
- k) Kurum bilgilerinin kurum dışından üçüncü şahıslara iletme.
- l) Kişisel bilgisayarlara Teknik Alt Yapı Destek Hizmetleri biriminin bilgisi dışında herhangi bir çevre birimi bağlantısı yapmak.
- m) Cihaz, yazılım veya bilginin izinsiz olarak kurum dışına çıkarmak.
- n) Kurumumuz prosedürleri gereği belirlediği programlar dışında kaynağı belirsiz olan programları (Dergi CD'leri veya internetten indirilen programlar vs) kurmak ve kullanmak yasaktır.

### E-mail ve Haberleşme Aktiviteleri

Aşağıdaki aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.



**T.C**  
**NECMETTİN ERBAKAN ÜNİVERSİTESİ**  
**BİLGİ SİSTEMLERİNİN GENEL KULLANIMI PROSEDÜRÜ**

DOKÜMAN NO: PR-045

YAYIN TARİHİ:01.08.2018

REVİZYON NO: 01

REVİZYON TARİHİ: **01.10.2021**

SAYFA NO 4 / 4

- a) Kurum dışından ve güvenliğinden emin olunmayan bir bilgisayardan web e-posta sistemini kullanmak.
- b) İstenilmeyen e-posta mesajlarının iletmek. Bunlar karşı tarafın özellikle istemediği reklam mesajlarını içeren mailler (spam mail) olabilir.
- c) E-posta veya telefon vasıtası ile taciz etmek.
- d) E-posta başlık bilgilerini yetkisiz kullanmak veya değiştirmek.
- e) Zincir e-postaları oluşturmak veya iletmek.
- f) İş ile alakalı olmayan mesajları birçok haber gruplarına iletmek.

#### **4. BGYS Kayıtları**

-

<b>HAZIRLAYAN</b>	<b>KONTROL EDEN</b>	<b>ONAYLAYAN</b>
BİLGİ İŞLEM DAİRE BAŞKANLIĞI	KURUMSAL KALİTE GELİŞTİRME VE AKREDİTASYON KOORDİNATÖRLÜĞÜ	KURUMSAL YETKİLİ