



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	1 / 14

## 1. Amaç

Bu prosedürün amacı T.C. Sağlık Bakanlığı Yozgat İl Sağlık Müdürlüğü'nün; kurum bilişim ağında bulunan Sistem, Bilgi ve Varlıkların Gizlilik, Bütünlük ve Erişilebilirlik özelliğini garantilemek ve kurumun itibar ve güvenilirliğini zedelememek için yapması ve uyması gereken iş kurallarını tarif etmektir.

## 2. Kapsam

T.C. Sağlık Bakanlığı Yozgat İl Sağlık Müdürlüğü'nün tüm çalışanlarının; kurum bilişim ağına bağlı donanımlar, bu donanımlar üzerindeki yazılım ve bilgilerin kullanım ve erişim faaliyetlerini kapsar.

## 3. Sorumluluklar

Tüm çalışanlar bu kurallara uymaktan yöneticiler ise çalışanlarının bu kurallara uyumunu sağlamaktan sorumludur.

## 4. Prosedür Akışı

### 4.1. Genel Kullanım Politikası

- 4.1.1. Çalışanlar günlük işlerinin ifasında istisnai durumlar hariç sadece kurum tarafından kendilerine tahsis edilmiş olan bilişim kaynaklarını (yazılım, donanım, erişim vb.) kullanacaktır.
- 4.1.2. İstisnai durumlarda, çalışanın bağlı bulunduğu en üst düzey yönetici ve Bilgi Sistemleri Departmanının ortak kararı ile kurumsal işlerde şahsi cihaz ve bilişim kaynakları kullanılabilir.
- 4.1.3. Bilgisayarlara ek bir donanım kurulumu sadece Bilgi Sistemleri Departmanının sorumluluğundadır. Bilgi Sistemleri Departmanının onayı olmaksızın ek donanım kurulumları hiçbir şekilde ve sebeple çalışanlar tarafından yapılamaz.
- 4.1.4. Kurumun iş gereği tahsis etmiş olduğu masaüstü bilgisayarlar, dizüstü bilgisayarlar, tabletler, masa telefonları ve dect telefonlar iş gereği kullanılır, özel işlerde kullanılmaz, kurum bilişim kaynakları üzerinde kişisel veriler bulundurulmaz.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	2 / 14

- 4.1.5. Bütün masaüstü ve dizüstü bilgisayarlar mesai bitiminde kapatılır. Bu işlem “Bilgisayarı Kapat” düğmesine basılarak yapılmalı, “Uyku” seçeneği seçilmemelidir.
- 4.1.6. Bütün masaüstü ve dizüstü bilgisayarlar kullanılmadıkları durumlarda otomatik olarak en fazla 5 dakika içerisinde şifreli ekran korumasına geçmelidir.
- 4.1.7. Çalışanlar; açık olarak korumasız şekilde bırakılan ve kendisinin kullanım ve erişim yetkisi olmayan bilgisayarları ve/veya diğer donanım ve erişimleri kullanamaz.
- 4.1.8. Çalışanlar, kurumda başka bir çalışanın kişisel bilgisayarının korumasız olarak bırakıldığını gördüğünde, derhal kişisel bilgisayarın sahibine ve/veya bu çalışanın

bağlı olduğu bölümdeki yetkili kişiye durumu bildirerek gerekli önlemin alınması konusunda uyarıda bulunmalıdır.

- 4.1.9. Bütün Cep Telefonu ve PDA (Personal Digital Assistant) cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, vs.) özellikleri aktif halde olmamalıdır ve mümkünse antivirüs programları ile yeni nesil virüslere karşı korunmalıdır.
- 4.1.10. Çalışanlar, kurum bilişim kaynaklarını kullanarak herhangi bir suç unsuru içeren olaylara karışmaya azami özen gösterir.
- 4.1.11. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (DoS saldırısı, port-network taraması, packet sniffing, packet spoofing vb.) eylemlere girişilmez.
- 4.1.12. Kurumsal verilerin, çalışan gizliliğine ve mahremiyetine özel önem gösterilmelidir. Kurum bilgileri, çalışanlar ile ilgili bilgiler hiçbir şekilde ve sebeple kurum dışından üçüncü kişilerle paylaşılmaz.
- 4.1.13. Çalışanlar kendilerine verilmiş yetkiler çerçevesinde hareket eder; kurumdaki gizli ve hassas bilgileri görmeye, elde etmeye ve üçüncü şahıslar ile paylaşmaya teşebbüs kesinlikle yasaktır.
- 4.1.14. Kurumun güvenilirliğini ve üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak amacıyla her çalışan, görevi gereğince

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	3 / 14

kendisinde bulunan ve yaptığı işlerle ilgili sahip olduğu her türlü belgeyi, veriyi ve bilgiyi korur ve kurum tarafından bu bilgilerin her zaman kendisinden istenebileceği ve alınabileceğini bilerek hareket eder.

- 4.1.15. Kurumda Bilgi Sistemleri Yönetiminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb) sunucu niteliğinde bilgisayar ve cihaz bulundurulamaz.
- 4.1.16. Tüm faks-modem üniteleri ile haberleşme ve internet erişim donanım yazılımlarının kurulması ve ayarları sadece T.C. Sağlık Bakanlığı Yozgat İl Sağlık Müdürlüğü Bilgi İşlem Daire Başkanlığı yetkisindedir.
- 4.1.17. Bilgi Sistemleri Departmanı personeli ve Bilgi Sistemleri Departmanı tarafından diğer birimlerde yetkili kılınan teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilemez.
- 4.1.18. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilemez, ivedilikle Bilgi İşlem birimine haber verilir.
- 4.1.19. Bilgisayarlar arası dosya alışverişinde mutlaka gerekmediği sürece CD/DVD ve/veya USB donanımlar yerine network özelliklerinden yararlanılır (mail, ortak alanlar).
- 4.1.20. Kurum bilişim sistemlerinde kullanılan yazılımların; yüklenmesi, silinmesi ve değiştirilmesi Bilgi Sistemleri Departmanının sorumluluğunda olup bahsi geçen eylemler hiçbir şekilde ve sebeple çalışanlar tarafından gerçekleştirilemez.
- 4.1.21. Kurum bilgisayarlarına hiçbir şekilde ve sebeple Bilgi Sistemleri Departmanı tarafından belirlenmiş lisanslı ve uluslararası patent kurallarına uyan yazılımlar dışında farklı bir yazılım yüklenemez.
- 4.1.22. Kurum bilgisayarlarına hiçbir şekilde ve sebeple oyun veya eğlence amaçlı yazılımlar yüklenemez.
- 4.1.23. Bilgi Sistemleri Departmanının bilgisi ve onayı olmadan herhangi bir yazılım, bir lisanslama yükümlülüğü olmasa bile (Freeware, Shareware, General Public License vb.), Internet, e-mail veya dışarıdaki bir network sisteminden kopyalanarak kurum bilişim sistemlerinde kullanılamaz.
- 4.1.24. Kurumda kullanılan yazılımlar çalışanlar tarafından hiçbir şekilde ve sebeple kopyalanamaz, çoğaltılamaz ve üçüncü şahıslarla paylaşılamaz.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	4 / 14

- 4.1.25. Bütün bilgisayarda kurumun lisanslı anti virüs yazılımı ve modülleri yüklenmiş olmalıdır.
- 4.1.26. Anti virüs yazılımı yüklü olmayan bilgisayar ağa bağlanmaz ve hemen Bilgi Sistemleri Departmanına haber verilir.
- 4.1.27. Hiçbir çalışan herhangi bir sebepten dolayı anti virüs programını sistemden kaldıramaz ve başka bir anti virüs yazılımını sisteme kuramaz.
- 4.1.28. Virüs bulaştığında, sistemin cevap verme zamanında yavaşlama, geri döndürülemeyen dosya kayıpları, değişiklik tarihlerindeki farklılıklar, dosya büyüklüklerinde artmalar, bilgisayarlarda donanım ve yazılım olarak tümünden arızalar vb. şekilde belirtiler karşımıza çıkar. Bu durumlardan bir veya birden fazlasıyla karşılaşıldığında hemen Bilgi Sistemleri Departmanına haber verilir.
- 4.1.29. Kurum bünyesinde zararlı programlar (örneğin, virüsler, solucanlar, truva atı, e-mail bombaları vb.) oluşturulamaz ve dağıtılamaz.
- 4.1.30. Bilgi Sistemleri Departmanı tarafından atanan yetkili kişiler çalışana haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel bilgisayardaki verileri, çalışanın onayı olmaksızın görüntüleyemez, kopyalayamaz ve değiştiremez.
- 4.1.31. Gereksinimle bilgisayar kaynakları paylaşımına açılmaz, kaynakların paylaşımına açılması gerekliliği halinde gerekli güvenlik tedbirleri alınır.

## 4.2. Fiziksel ve Çevresel Güvenlik

- 4.2.1. Kurum üst yönetimi tarafından yetkilendirilmediği sürece hiçbir çalışan kurum binaları içinde ve dışında fotoğraflama, görüntüleme, ses kaydetme gibi kayıt araçlarını kullanamaz.
- 4.2.2. Çalışanlar, kurumun iş gereği kendilerine tahsis etmiş olduğu tüm kurumsal cihazı bozulmaması ve kaybolmaması amacıyla azami dikkat ve özen ile kullanmak zorundadır.
- 4.2.3. Kurum tarafından çalışanlarına günlük işlerinde kullanmak üzere tahsis edilmiş olan taşınabilir cihazların (dizüstü, tablet vb.) fiziksel güvenliğinden kullanıcıları sorumludur. Bu cihazların çalınması/kaybolması durumunda en kısa sürede Bilgi Sistemleri Departmanına haber verilir.

Hazırlayan	Kontrol Eden	Onaylayan
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	5 / 14

- 4.2.4. Kurumda kullanılan hassas ve önemli iş bilgilerini içeren her türlü bilgi varlıkları (basılı belgeler, USB Bellekler, CD/DVD vb.) kullanılmadığında, özellikle de mesai saatlerinin dışında, çekmecelerde ve/veya diğer güvenli yerlerde kilitli olarak tutulur.
- 4.2.5. Gelen ve giden gizli bilgiler, gelişigüzel ya da güvenli olmayan bir şekilde, faks/yazıcı/fotokopi/tarayıcı cihazlar üzerinde bırakılamaz.
- 4.2.6. Bilgi işlem araç gereçlerinin yakınlarında ve sistem odalarında; yiyecek, içecek veya sigara kullanılamaz.
- 4.2.7. Bilgisayarlar, iletişim cihazları ve veri depolama cihazları, kullanım veya depolama amacıyla yerleştirilirken; cihaz üreticisinin belirttiği teknik standartlara uygun ortamlar sağlanır. Gerekirse, çevresel kontrollerle bu ortam gözlenir ve uygun aksiyonlar alınır.
- 4.2.8. Cihaz yerinde bakıma tabi tutulamayacaksa; bakıma gönderilmeden önce, içindeki bilgiler kontrol edilir, kritik bilgiler güvenceye alınır.
- 4.2.9. Hassas bilgileri içeren kayıt araçları, güvenli bir şekilde depolanır ve kullanımdan kaldırılacağı zaman imha edilir.
- 4.2.10. Medyalarda ve donanımlarda bulunan, kullanımına ihtiyaç kalmamış (yasal yükümlülükler veya iş gerekleri için saklanması gereken bilgiler dışında) kurumsal veriler ve yazılımlar silinir, gerekli görülüyorsa medya yok edilir.
- 4.2.11. Depolama ortamı içeren cihazların tüm öğeleri, örneğin takılmış sabit diskler, elden çıkartılmadan önce, tüm hassas verilerin ve lisanslı yazılımların kaldırılmış olduğunun veya üstüne yazılmış olduğunun temin edilmesi için, kontrol edilir.
- 4.2.11.1. Eğer taşınabilir depolama ortamı içerisinde saklanan bilgi artık ihtiyaç duyulmayacak bir veri ise, geri dönülemeyecek şekilde imha edilir.
- 4.2.11.2. Ortamın ya da ortam içerisindeki verinin kaldırılmasında onay gereksinimi var ise, imha öncesinde ve sonrasında denetim kaydı tutulur.
- 4.2.11.3. Taşınabilir ortamda veriler sadece iş gereksinimi mevcut ise tutulur.
- 4.2.12. Saklama ortamları, kullanımına ihtiyaç olmadığında güvenli ve tehlikesiz şekilde imha edilir. Saklama ortamları yeterli özen gösterilmeden imha edildiğinde, hassas bilgi başka kişilerin eline geçebilir. Riski en aza indirmek amacıyla veri depolama ortamlarının güvenli imhası için resmi prosedürler

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	6 / 14

hazırlanır. Aşağıdaki esaslar değerlendirilir: Hassas bilgi ve lisanslı yazılım içeren saklama ortamları güvenli ve tehlike içermeyecek şekilde saklanır ve imha edilir (yakarak, parçalara ayırarak, kuruluş içerisinde başka bir uygulama tarafından kullanılmadan önce bilgi işlem müdürlüğü çalışanları tarafından format atılarak, anlaşmalı şirketler aracılığı ile vb.).

Aşağıdaki liste güvenli imhası gereken malzemeleri listelemektedir:

- Kağıt dokümanlar
- Çıktı raporları
- Çıkarılabilir disk ve kasetler
- Optik depolama ortamları (tüm formlar ve yazılım dağıtıcı ortamlar da dahil)
- Test verisi
- Sistem dokümantasyonu

Hassas malzemelerin imhasına yönelik denetim kaydı tutulur. İmha için malzeme toplanması sırasında, gizli olarak nitelendirilmeyen bilginin miktarı artarak bir grup gizli bilgiden daha hassas ve daha kritik bir hale dönüşebilir. Bu yığın etkisine özel olarak dikkat edilmelidir.

4.2.13. Kuruma ait cihaz, yazılım ve veriler hiçbir şekilde ve sebeple izinsiz ve yetkisiz olarak kurum dışına çıkarılamaz.

Bina içerisine ya da dışarısına her tür malzeme taşınması güvenlik tarafından kontrol edilir. Dışarı çıkartılan tüm malzemeler için Bilgi İşlem yönetimi tarafından onay temin edilir. Dışarı çıkarılacak bu malzemeler Bilgi İşlem yönetimi tarafından gizlilik derecesine göre ve gerek gördüğü durumlarda kayıt defterinde tutulur ve takip edilir. Güvenlik sorumluları gerekli gördükleri durumlarda, dışarıya çıkartılan malzeme için Bilgi İşlem yönetiminin onayını kontrol etmekle mükelleftir. Eğer bir Bilgi İşlem varlığı tamir için dışarıya çıkartılıyorsa, muhtemel dönüş tarihi de tutulan kayıtlara eklenir. Çıkışı yapılan varlığın bir hafta içerisinde geri getirilmemesi halinde, bu gecikmeden Bilgi İşlem yönetimi haberdar edilir ve hizmeti sağlayan

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	7 / 14

tarafından açıklama temin edilir (Envanter Kayıtları envanter listesinden kontrol edilebilir).

Güvenlik personeli binaya girişi yapılan malzeme ile ilgili bilgi toplar ve malzemenin binada ilgili birime iletilmesini sağlar. İlgili çalışan, malzemenin teslim alındığına

dair bilgilendirilir.Malzemeyi teslim alan çalışan ilk incelemeyi yapar ve bir problem olmaması durumunda malzemenin girişini onaylar. İlgili çalışan da ayrıca, malzemenin alındığına dair bilgileri envanter listesine girer.

4.2.14. Çalışanlar, yönetilen bilgi sistemleri üzerindeki hassas bilgiler ya da cihazlarla kurum dışında çalışmak zorunda kaldıkları durumlarda (yöneticileri tarafından yetkilendirildiklerinde), bütün sorumluluğun kendilerine ait olduğu konusunda bilgilendirilir.

4.2.15. Kurum cihazını kurum dışında kullanmasına izin verilen çalışan, aşağıdaki kontrollerin uygulanmasından sorumludur:

- 4.2.15.1. Cihazın fiziksel güvenliği sağlanır, var ise üreticinin koruma ve kullanım ile ilgili talimatları her zaman uygulanır;
- 4.2.15.2. Kurumsal varlık ve verilerin güvenliği sağlanır. Kurum alanı dışına çıkarılmış kurumsal varlık ve veriler özellikle de umumi alanlarda hiçbir zaman gözetimsiz ve korumasız bırakılmaz.
- 4.2.15.3. Cihazın güvenlik kontrolleri varsa, kullanılır; (fiziksel kilit, dosya şifreleme sistemi vb.)

İçlerinde çok gizli/gizli/hizmete özel/kuruma özel gibi bilgiler bulunduran laptop, notebook, tablet, akıllı telefon vb. sahipleri, bu cihazları hiçbir zaman, diğer çalışanların ve/veya üçüncü şahısların kolayca erişebileceği yerlerde, korumasız bırakmaz.

4.2.16. Çalışanlara pozisyonları gereği tahsis edilmiş olan ve oturdukları yerleşim planına uygun kurulmuş olan tüm bilgisayar ve donanımlar Bilgi Sistemleri gözetimi ve bilgisi dışında hiçbir şekilde ve sebeple başka bir yere taşınmaz veya başka bir donanımla yeri değiştirilmez.

4.2.17. Çalışanların bina içindeki çalışma yerlerinin ya da çalıştıkları binanın değişimi söz konusu olduğunda, bir hafta öncesinden haber vermek kaydı ile

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	8 / 14

değişimler sadece Bilgi Sistemleri Departmanı tarafından gerçekleştirilir.

- 4.2.18. Çalışanların yer değişikliği pozisyon değişikliğini de içeriyorsa, eski bilgisayarı eski pozisyona yeni çalışan alınana kadar Bilgi Sistemleri Departmanı tarafından alıkonulur, kendilerine ise ilgili pozisyona tahsis edilmiş bilgisayar verilir.
- 4.2.19. Kurumda kullanılan bilgisayarlar ve bunlara bağlı donanımlarının yer değişikimi sadece Bilgi Sistemleri Departmanının yetkisindedir.

### 4.3. Parolalar

- 4.3.1. Kullanıcı hesabı veya uygulama erişim yetkisi olan tüm T.C. Sağlık Bakanlığı Yozgat İl Sağlık Müdürlüğü çalışanları parola kurallarına uymak zorundadır.
- 4.3.2. T.C. Sağlık Bakanlığı Yozgat İl Sağlık Müdürlüğü bünyesinde çalışan tüm personellerin kullanıcı hesabı ve uygulama parolaları, minimum 8 karakterden oluşmalı ve "B"üyük/"k"üçük harf (Ör. a-z, A-Z), karakterler (Ör. @!#\$\*\_ \_{}&[]%()+\ vb. ) ve rakamlara (Ör. 0-9) sahiptir. (Parolanız K@rM4\$!k olsun)
- 4.3.3. Parolalar başkaları tarafından tahmin edilmesi kolay olan aile/arkadaş/sevilen yer/yemek/hayvan/sanatçı isimleri, klavye sıralı harfler, sıralı sayılar, doğum tarihi/yeri, adres veya telefon bilgisi içermemelidir. Kişi özelinde hatırlaması kolay kısaltmalar vb. kullanılabilir.
- 4.3.4. Kullanıcı parolaları her doksan (90) günde bir sistem tarafından değiştirilmeye zorlanır.
- 4.3.5. Sistem geriye doğru yirmidört (24) parolayı hatırlar, dolayısıyla parola değişikliği sırasında son yirmidört (24) parola kullanılmaz.
- 4.3.6. Değiştirilen parola 24 saat boyunca yeniden değiştirilemez.
- 4.3.7. Kullanıcı parolaları kişiye özel bilgilerdir ve gizli bilgi olarak değerlendirilir. Buna göre işin sürdürülmesi amacıyla bile olsa kimseyle paylaşılamaz.
- 4.3.8. Parolalar herhangi bir yere (form vb.) yazılmaz veya elektronik ortamda (e-posta mesaj içeriği vb.) tutulamaz.
- 4.3.9. Kullanıcı parolaları bilgisayarların yakınında kolaylıkla erişilebilecek şekilde yazılı bırakılmaz.
- 4.3.10. Kurum bünyesinde kullanılan şifreler kurum dışında (Ör. İnternet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde) herhangi bir şekilde kullanılmaz.

Hazırlayan	Kontrol Eden	Onaylayan
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü





T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	9 / 14

- 4.3.11. Kullanıcı şifresinin herhangi bir kişi tarafından istenmesi halinde (telefon, e-posta, sözlü olarak) Bilgi Sistemleri Departmanı yetkilisi bilgilendirilir ve/veya yardım masası üzerinden Bilgi Güvenliği İhlal Olayı kaydı açılır.
- 4.3.12. Uygulamalardaki "şifre hatırlama" özellikleri seçilmez (Ör. Outlook, Uygulama, Internet Explorer vb.).
- 4.3.13. Herhangi bir şüpheli durumda kullanıcı parolaları mutlaka değiştirilir.

## 4.4. E-Posta Kullanımı

- 4.4.1. Çalışanların kurum adına yaptığı tüm elektronik posta (e-mail) haberleşmeleri, kurumsal elektronik posta adresi yoluyla yapılır, şahsi e-posta adresleri kurumla ilgili haberleşmelerde kullanılmaz.
- 4.4.2. Çalışanlar kurumun e-posta sistemini özel işlerinde kullanamaz.
- 4.4.3. Çalışanlar herhangi bir sebepten ötürü başka çalışanların e-posta hesaplarını kesinlikle kullanamaz.
- 4.4.4. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz.
- 4.4.5. Hiçbir kullanıcı "Konu:" alanı boş bir e-posta gönderemez.
- 4.4.6. "Konu:" alanına konunun önüne gönderilen mailin sınıfına göre alıcıyı da uyarmak açısından gerektiğinde "GİZLİ:" ve "KURUMA ÖZEL" ibareleri yazılır.
- 4.4.7. Kuruma ait çok gizli bilgiler gönderilen mesajlarda ve/veya eklerinde yer almamalıdır.
- 4.4.8. Kurumun e-posta sistemi; yasa dışı, taciz, suiistimal, hakaret veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için hiçbir şekilde ve sebeple kullanılamaz.
- 4.4.9. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinir ve kesinlikle başkalarına iletilmez.
- 4.4.10. Kişisel kullanım için İnternetteki listelere üye olunması durumunda kurum e-posta adresleri kullanılmaz.
- 4.4.11. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmaz.
- 4.4.12. İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	10 / 14

posta adresi bu mesajlarda kullanılamaz. Ancak iş gereği üye olunması gereken internet haber grupları için yönetici onayı alınarak kurumun sağladığı resmi e-posta adresi kullanılır.

- 4.4.13. Çalışanların kullanıcı parolası girmesini isteyen e-postalar; sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinir.
- 4.4.14. Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemez.
- 4.4.15. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engeller.
- 4.4.16. Çalışanlar, gizli ve kuruma özel e-postaları kurum dışındaki üçüncü şahıslar ile hiçbir şekilde ve sebeple paylaşamaz.
- 4.4.17. Kaynağı bilinmeyen e-posta ekinde gelen ve virüs, e-mail bombaları ve Truva atı gibi zararlı kodlar içerebilecek dosyalar kesinlikle açılmaz ve derhal silinir.
- 4.4.18. Kurumsal e-posta adresleri doğrudan ya da dolaylı olarak ticari ve kar amaçlı olarak kullanılmamalı, diğer kullanıcılara bu amaçla e-posta gönderilmemelidir.
- 4.4.19. Çalışanlar kendilerine ait kurumsal e-posta adresinden gönderilen e-postalardan doğacak hukuki işlemlerden kendileri sorumludur.
- 4.4.20. Kurumdan ayrılan çalışanın kurumsal e-posta hesabı kapatılır ve/veya yöneticisinden gelen talep doğrultusunda ilgili talepte belirtilen süre için pasif hale getirilir.

## 4.5. İnternet Erişimi ve Kullanımı

- 4.5.1. İnternet kullanımındaki esas, çalışanların kurumsal internet kaynaklarını kurum içi görev ve sorumluluklarını yerine getirirken kullanmaları, kişisel işler ve kişisel kazanç için kullanmamalarıdır.
- 4.5.2. Kurumsal internet kaynakları, hizmet verilen sektörlerdeki iş süreçlerinin geliştirilmesi ve iyileştirilmesi amacıyla kullanılabilir, fakat bu süreçlerin aksamasına etki edebilecek şekilde yoğun iş saatleri içinde kullanılmaz.
- 4.5.3. Ayrıca kurum, çalışanlarının kişisel gelişimine katkıda bulunmak amacıyla, İnternet kullanımını kabul eder. Ancak, kişisel gelişimi artırıcı araştırma ve geliştirme faaliyetleri iş zamanında değil, kişisel zamanlarda, maliyetler ve iş süreçleri de göz önüne alınarak yapılır, çalışma saatleri içerisinde iş ile ilgili

Hazırlayan	Kontrol Eden	Onaylayan
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	11 / 14

olmayan sitelerde gezinilmez.

- 4.5.4. Çalışanlar, işleri için gereken ancak kurum politikalarına göre engellenmiş İnternet sayfaları ya da erişimin engellenmesini gerekli gördükleri İnternet sayfaları için yönetici onayı eşliğinde Yardım Masası kanalı ile Bilgi Sistemleri Departmanına başvurabilirler. Bu talepler değerlendirilerek uygun görülürse işleme alınacaktır.
- 4.5.5. Hiçbir çalışan peer-to peer bağlantı yoluyla internetteki servisleri kullanamaz. (Örneğin; KaZaA, iMesh, eDonkey, Torrent vb.)
- 4.5.6. ICQ, MIRC, Messenger vb. gibi mesajlaşma ve sohbet programları kullanılamaz.
- 4.5.7. Kurumsal İnternet erişimi üzerinden "Tor" ağına bağlantı yapılamaz.
- 4.5.8. Kurumsal İnternet erişimi üzerinden Multimedia Streaming (Video, mp3 yayını ve iletişimi) yapılamaz.
- 4.5.9. Kurumsal İnternet erişimi üzerinden iş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar gönderilemez ve/veya indirilemez.
- 4.5.10. Kurumsal İnternet erişimi üzerinden kurum tarafından onaylanmamış yazılımlar indirilemez.
- 4.5.11. Kurumsal İnternet erişimi üzerinden genel ahlak anlayışına aykırı internet sitelerine erişilemez ve/veya dosya indirimi yapılamaz.
- 4.5.12. Kurumsal İnternet erişimi üzerinden ekran koruyucu, yamalar, masaüstü resimleri, yardımcı, tamir edici program olduğu belirtilen araçlar gibi dosya ve programlar indirilemez ve/veya kurulamaz.
- 4.5.13. Üçüncü şahısların kurumsal interneti kullanmaları Bilgi Sistemleri Departmanının izni doğrultusunda gerçekleştirilir.
- 4.5.14. İş sürekliliğinin devamlılığını tehdit edecek herhangi bir bilgi (sistem kullanım şifreleri, güvenlik parametreleri vb.), İnternet üzerinden şifrelemeden, okunabilecek bir şekilde gönderilmez. Hassas bilgilerin İnternet üzerinden taşınması gerektiğinde, bu bilgiler kesinlikle ek şifreleme mekanizmaları ile korunur.
- 4.5.15. Bilgi Sistemleri Departmanı, iş kaybının önlenmesi amacı ile çalışanların internet kullanımı hakkında gözlemlene ve istatistik yapma yetkisine sahiptir.

## 4.6. Sosyal Medya Kullanımı

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	12 / 14

- 4.6.1. Sosyal Medya kişisel bloglar, web siteleri, Facebook, Twitter, Instagram, LinkedIn, YouTube ve buna benzer tüm sosyal paylaşım alanlarını kapsar.
- 4.6.2. Sosyal medya, paylaşımların hızlı ve kontrolsüz yapılabildiği bir alandır. Özellikle kurumdan hizmet almış tüm özel kişilikleri tüzel kişilikleri ve kurum çalışanlarını ilgilendiren sosyal medya paylaşımları, ilgili kişi ve kurumların bilgisi ve izni olmaksızın yapılamaz.
- 4.6.3. Çalışanlar kurum adını içeren ya da kurumla ilişkilendirilebilecek sosyal medya kullanımlarında; kuruma ait hiçbir gizli/özel bilgiyi, onaylanmamış gelişmeyi, müziği, videoyu, yazıları ve fotoğrafları kurumun yazılı izin olmadan üçüncü kişilerle paylaşamaz.
- 4.6.4. Kurum bünyesindeki kişi, departman toplantı içerik, detay ve mekânları sosyal medyada işaretlenmez; örneğin Instagram, FourSquare, Twitter ve Facebook'ta "Biz VVV otelde, XXXX takımıyla, ZZZ amaçlı toplantı için bulunuyoruz" gibi paylaşımlarda bulunulmaz.
- 4.6.5. Sosyal medyada kurumla ilgili gizlilik, güvenlik ve rekabet açısından risk oluşturabilecek uygulamalar kullanılamaz.
- 4.6.6. Çalışanlar sosyal medyayı kullanarak öğrencileri, tedarikçileri, çalışanları veya diğer paydaşları aşağılayamaz, rakipler hakkında yanlış veya kanıtlanmamış beyanlarda bulunamaz.
- 4.6.7. Çalışanın kurum içindeki görevi özellikle bu tür görüşleri beyan etmek değilse, çevrim içinde ifade edilen görüş ve fikirlerin aynı zamanda kurumun görüşlerini temsil ettiği izlenimini vermediğinden emin olunur.
- 4.6.8. Kurum bilişim kaynakları kullanılarak yazılan elektronik yazılar dahi kuruma atfedilebilir. Bu nedenle, kurum tarafından sağlanan bilişim sistemlerini kullanarak iletişim yazıları yazarken özellikle dikkat edilir.
- 4.6.9. Sosyal medyada fikirlerin özgürce ifade edilme sürecinde sergilenecek her türlü davranış, temsil edilen kurumun imajını zedeleyebilir. Bu durumdan özellikle kaçınılır.
- 4.6.10. Sosyal medyada kullanılan kelimelere ve dile dikkat edilir; ayrımcı, rahatsız edici, ırkçı, cinsel, etnik, dini ya da fiziksel saldırı ve aşağılama niteliğinde ifadeler kullanılmaz, paylaşılmaz ve bu tür durumlara aracı olunmaz.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	13 / 14

## 5. Yaptırımlar:

- 5.1.** Kurumda bulunan donanımlar kurumun malı olup, bunlara zarar verilmesi halinde kurum, zarar veren çalışan aleyhine Takdir ve Disiplin Yönetmeliği uyarınca işlemleri başlatır. Kurum yetkililerinin onayı ve talimatı bulunmaksızın donanımın dış görünüşünü değiştirmek, bağlı parçaların bağlantı şeklini değiştirmek, parçaları çalmak veya çalmaya teşebbüs etmek gibi durumlar gerçekleştiğinde Bilgi Sistemleri Departmanı tarafından çalışanın hesabı süresiz kapatılır, tutanak tutulur, söz konusu davranışlarda bulunan kişiler hakkında Takdir ve Disiplin Yönetmeliği uyarınca gerekli işlemler başlatılır.
- 5.2.** Bilgi güvenliğini tehlikeye atacak durumların saptanması durumunda, bu durum sebebiyle zarar görmesi muhtemel servislerin erişimleri kesilebilir, kullanıcı hesapları geçici olarak kapatılabilir. Bu durumda ilgili bölümler veya tüm çalışanlar bilgilendirilir.
- 5.3.** Tüm üniversite tarafından kullanılan veya belirli bir birime atanmış ve hizmet kesintisi veya güvenlik ihlali durumunda, iş/imaj/para kaybına neden olabilecek servislerin yetkilerin kötüye kullanılması ile çalışmasını aksatacak olaylara neden olunması durumunda, çalışanın kurum servislerine erişimi kapatılır. İlgili çalışan ve yöneticisi durumdan haberdar edilir ve gerekli görülür ise Takdir ve Disiplin Yönetmeliği uyarınca gerekli işlemler başlatılır.
- 5.4.** Kurum tarafından sağlanan elektronik iletişim sistemleri (kurumsal e-posta, internet erişimi, USB erişimi vb.) kullanılarak kurum ve/veya kurumun iş ilişkisinde bulunduğu 3. Kişilere ait ticari sır niteliğindeki her türlü bilgi, evrak ve Know-how'ın yetkilendirilmemiş üçüncü şahıslarla paylaşılması durumunda çalışanın hesabı süresiz kapatılır ve Takdir ve Disiplin Yönetmeliği uyarınca gerekli işlemler başlatılır.
- 5.5.** Çalışan, yukarıdaki maddelerde belirlenen kurallara uygun kullanımının, çalışanın kişilik hakları saklı kalmak üzere, kurum tarafından kontrol edilebileceğinden haberdardır. Çalışan, kurumun bu belgede yer alan bilgi güvenliği ihlallerinden bir veya birkaçını tespit etmesi halinde, önlemler alabileceğini kabul eder. Ancak bu önlemler, ihlalin genel ağ işleyişini ve güvenliğini etkilememesi durumunda, ilgili çalışan ile iletişim kurulduktan ve

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü



T.C. SAĞLIK BAKANLIĞI

# VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI PROSEDÜRÜ



YOZGAT  
İL SAĞLIK MÜDÜRLÜĞÜ

Kodu	Yayınlama Tarihi	Revizyon Tarihi	Revizyon No	Sayfa
BG.PO.01	01.06.2016	01.08.2019	V.3.0	14 / 14

belli bir süre tanıdıktan sonra alınabilir.

- 5.6. Kurum, herhangi bir bilgi güvenliği ihlali veya ifşası halinde daha önce sözü edilen şartlarla kısıtlayıcı önlemler alabilir.

<u>Hazırlayan</u>	<u>Kontrol Eden</u>	<u>Onaylayan</u>
Ömer YILDIZ Bilgi Güvenliği Yetkilisi Uzman	Özer ŞİŞMAN Personel ve Destek Hizmetleri Başkanı	Dr. Fatih ŞAHİN İl Sağlık Müdürü