1. **AMAÇ:**

Bu talimatın amacı Yıldız Teknik Üniversitesi personellerinin Bilgi varlıklarının kullanımı ile kurallarını belirlemektir.

1. **KAPSAM:**

Bilgi Güvenliği kapsamında yürütülen tüm birimleri kapsamaktadır.

1. **UYGULAMA**
	1. Personelin kullanımına verilen Flash disk gibi taşınabilir hafıza cihazları dışında kişisel veri kayıt cihazlarının (taşınabilir harddisk, cd-dvd writer, usb memory) kullanımı yasaktır.
	2. Kurum içerisinde kullanım için verilen taşınabilir hafıza cihazları dışarıda başkasına ait pc-laptop, internet kafeterya, ev veya başka halka açık bilgisayarlarda kullanılamaz. Kurumun temin ettiği bilgisayarlar dışında bu cihazların kullanımı yasaktır.
	3. Bilgisayarlarda Kurulu olan yazılımların çalışmasını engelleyecek davranışlarda bulunulamaz. Kullanıcılar bilgisayarlarının BIOS ayarlarını değiştirmek, bilgisayarları harici bir araç ile açmak (boot etmek), İşletim sisteminin açılmasını engellemek, İşletim sistemine ait özel dosyalara erişmek veya bu dosyaları değiştirmek, bilgisayarlarda kurulu olan programların çalışmasını engellemek, bilgisayarlara program yüklemek işlemlerini yapamazlar.
	4. İşletim sistemi ve ofis programları sadece yetkililer tarafından yüklenebilir.
	5. Her kullanıcı bilgisayarının dış temizliğinde olduğu kadar iç temizliğinde de duyarlı olmalıdır. Sistem kaynaklarını sömüren gereksiz hiç bir program kurulmamalıdır. (Oyun, P2P download, programlar (emule, limewire, kazaa gibi), haber vericiler, ilave güvenlik duvarı (firewall), Explorer arama tool barları (google toolbar, yahoo toolbar vb.)
	6. Kullanıcının tanımadığı kişilerden gelen ve özellikle eki (attachment) olan elektronik postaları (e-mail) açmadan silinmelidir. Postalarınız merkezi olarak anti virüs yazılımı ile kontrolden geçmekle birlikte, tam güvenlik için bu uygulama gereklidir.
	7. Kullanıcılar bilgisayarlarında çökertme ve sistem kırma (hacking&cracking), ağ dinleme (sniffing), saldırı (attacking), dinleme amaçlı program ve araçlarını bulunduramazlar.
	8. Kullanıcılar bilgisayarlarda yetkisiz program yazarak veya dışarıdan program temin ederek bunları başkalarına zarar verecek şekilde veya başkalarına ait alanlara izinsiz erişim için kullanamazlar.
	9. Kullanıcılar bilgisayarlara kurulu olan programları başkalarına zarar verecek şekilde veya başkalarına ait alanlara izinsiz erişim için kullanamazlar.
	10. Kullanıcılar başka bir kullanıcının hesabı ile bilgisayara giriş yapma, başka bir kullanıcı hesabı ile ileti göndermek, başka bir kullanıcı hesabından çıktı almak, başka bir kullanıcıya şifresini vermek işlemlerini yapamazlar.
	11. Kurum tarafından sağlanan e-posta hizmeti başkalarına zarar verecek şekilde veya saldırı amaçlı kullanılamaz.
	12. Kurum içinde kullanılan bilgisayarlar kurum içinde farklı personelin kullanımına verilmeden önce formatlanır. Elden çıkartılacak bilgisayarların kuruluş dışına çıkmaması gereken diskleri ayrılır. Diskler parçalanarak imha edilir. Elden çıkartılan teçhizat envanterden düşülür. Ardından ağ cihazı üzerindeki yazılım ve yapılandırma sıfırlanır. Elden çıkartılan ağ cihazı sistem envanterinden düşülür.
2. **Bilgisayar Kullanımı**

Kurum personeline işlerin yerine getirilmesi için tesis edilen masaüstü veya mobil bilgisayarların kullanımında aşağıdaki kurallar dikkate alınmalıdır:

* 1. Personel, Kurum tarafından kendilerine tahsis edilen bilgisayarda sadece kendilerine verilen kullanıcı adı ve şifre ile oturum açmalıdır.
	2. Personele verilen kullanıcı adı ve şifre kişiye özeldir. Bilgisayar, e-posta ve internet kullanımlarından kaynaklanan olumsuz durumlarda sorumlu kullanıcı adı ile tespit edilebildiğinden ve kullanıcı ile ilgili hukuki işlem yapılması söz konusu olabildiğinden, kullanıcı adı ve şifreler kimse ile paylaşılmamalıdır.
	3. Personel, kullandığı sistemler ile ilgili erişim yetkisi değişiklikleri ile ilgili taleplerini, resmi yazı ile bildirmektedir.
	4. Personele sağlanan bilgisayar kaynakları, kişisel veya yasal olmayan amaçlar için kullanılamaz.
	5. İş veya çalışma konuları ile ilgili olmayan yazılımlar bilgisayarlarda saklanmamalı, yükleme yapılmamalı veya çalıştırılmamalıdır.
	6. Personelin yazılı izin verilmedikçe, içeriden veya dışarıdan ağı izlemesi, portları taraması veya açıklık taraması yapması veya bu tür taramalar için ortam sağlaması yasaktır.
	7. Üçüncü taraf personeli, Bilgi İşlem Daire Başkanlığının izni ve onayı olmadan zafiyet/ip taraması yapamaz, yapması halinde elde ettiği bilgileri İletişim ve Daire Başkanlığı haricinde her ne şekilde olursa olsun paylaşamaz. Paylaştığı tespit edildiğinde 5237 sayılı Türk Ceza Kanunun bilişim suçları maddelerine göre işlem başlatılır.
	8. Personelin kullanıcı bilgilerini, parolalarını tespit etmekte kullanılan program ve uygulamaları kendi bilgisayarlarına kurmaları, kullanmaları ve paylaşmaları yasaktır.
	9. Personelin kullanıcı bilgilerini, parolalarını tespit etmekte kullanılan ve internet üzerinden paylaşılan programları kullanmaları yasaktır.
	10. Personelin dâhili veya harici ne olursa olsun servis durdurma atakları yapan programları kullanmaları ve paylaşmaları yasaktır.
	11. İş amaçlı olmayan veriler, fotoğraflar, videolar, müzik dosyaları, dokümanlar bilgisayar kaynaklarında saklanmamalı, işlenmemeli ve yazdırılmamalıdır.
	12. Kişisel bilgisayarlar üzerindeki disklerde bulunan sayısal bilgilerin güvenliğinden ve yedeklenmesinden kullanıcı sorumludur.
	13. Bilgisayarlar açık ve şifre koruması olmadan gözetimsiz bırakılmamalıdır. Bırakılması durumunda “Windows ve L” tuşlarına aynı anda basarak kilitlenmeli.
	14. Kullanıcılar kendi kullanıcı adı ve parolalarının yetkisiz erişime karşı korunmasından sorumludurlar.
	15. Kullanıcılar belirtilen parola koruma ile ilgili önlem ve açıklamalara uymalıdırlar.
	16. Kullanıcılar kullanıcı adı ve parolalarını açıkta, yazılı veya gözetimsiz bir şekilde saklamamalıdırlar.
	17. Kullanıcılar erişim ile ilgili bilgileri izinsiz bir şekilde 3. taraflar ve yabancılar ile paylaşmamalıdırlar.
	18. Bilgisayar gizli bilgiler içeriyor ise çalışma durumunda monitör başkaları tarafından kolayca görülemeyecek bir açı ile yerleştirilmeli ve kullanılmalıdır.
	19. Mesai bitiminden sonra sunucular ve çalışması zaruri olan bilgisayarlar hariç diğer bilgisayarlar kapatılmalıdır.
	20. Kurum dışına çıkarılan mobil bilgisayarlar çalınma veya yetkisiz erişime karşı uygun şekilde yerleştirilmeli, saklanmalı ve korunmalıdır.
	21. Seyahat sırasında mobil cihazlar çantalarında saklanmalı araçlar içerisinde açıkta ve başıboş bırakılmamalıdır. Toplu taşım araçlarında mobil cihazlar çantalarında kullanıcının gözetiminde tutulmalıdır.
	22. Satın alınan bilgisayarlar varlık envanterine eklenmeli ve zimmet takibi yapılmalıdır.
1. **Telefon Kullanımı**

Kurum personeline sabit telefon imkânı sağlamaktadır. Bu imkândan aşağıdaki kurallar dikkate alınarak faydalanılabilir:

* 1. Telefonlar sadece iş amaçlı kullanılmalıdır; öncelikle diğer iletişim yöntemleri (e-posta, faks vb.) tercih edilmelidir.
	2. Telefonda gizli bilgiler (proje bütçe bilgileri, finansal bilgiler, yaklaşık maliyet, kredi bilgisi, kişisel bilgi, kullanıcı adı, şifre vb.) kesinlikle paylaşılmamalıdır.
	3. Çalışma ortamlarında telefon ile, başkalarının dikkatini dağıtacak şekilde ve yüksek sesle konuşmalardan kaçınılmalıdır.
	4. Telefon görüşmeleri 5089 Nolu Elektronik Haberleşme Kanununa uygun olarak gerçekleştirilmelidir. Personel, paydaş, vatandaş veya üçüncü taraflar ile görüşmelerde Kurumun prestijine zarar verecek kaba ve uygun olmayan ifadeler kullanmamalıdır.
	5. Kurum, personele verdiği telefon kullanma hakkını istediği bir anda herhangi bir gerekçe ile veya gerekçesiz iptal edebilir.