1. **AMAÇ**

Bu talimatın amacı Bilgi İşlem Daire Başkanlığı tarafından sunulan hizmetlerin veri güvenliğini ve sürdürülebilirliğini en üst düzeyde tutmak ve olası bilgi kayıplarını en aza indirgemek için parola güvenliği ile ilgili yöntemleri belirlemektir.

1. **KAPSAM**

Bilgi Güvenliği kapsamında faaliyet yürütülen tüm birimleri ve kurumsal iletişim ağlarını kullanan tüm çalışanları ve misafir kullanıcıları kapsamaktadır.

1. **TANIMLAR**
* YTÜ – Yıldız Teknik Üniversitesi
* BİDB – Bilgi İşlem Daire Başkanlığı
* AD – aktive Directory
* KULLANICI – Kurum çalışanları
* ŞİFRE – Bir anlamlı veriyi anlayabileceğiniz (unutmayacak) şekilde anlamsız hale getirme işlemidir.
* PAROLA – Bir sisteme girmemiz için belirlediğimiz harf, rakam ve sembollerden oluşan şifrelerdir.
* SUNUCU – Uygulama yayınlanan sistemler.
1. **SORUMLULUK**

Yıldız Teknik Üniversitesi BİDB Ağ ve Sistem Şube Müdürlüğü

1. **UYGULAMA**
	1. **KULLANICI ŞİFRELERİ**
* YTU kullanıcıların herbirine bağımsız bir hesap açılır. Ve açılan hesaplara giriş için BİDB veya Uygulama sistemleri tarafından geçici parola atanmaktadır.
* Şifreler alındıktan sonra 5.3 maddesine göre kullanıcı tarafından yeni parola atanır.
	1. **SİSTEM ŞİFRELERİ**
	2. **GÜVENLİ PAROLALAR İÇİN ŞİFRE OLUŞTURMAK**

Güvenli parola

* Şifreleriniz için ingilizce karakter kullanmalısınız. *“ş,ç,ü veya başka alfabe karakterleri kullanamazsınız.”*
* Şahsınızla ilgili kolay tahmin edilecek ad, doğum tarihi, yaşam alanınızla ve yakınlarınızla ilgili kısaltmalar kullanmamaya veya farklı varyasyonlar kullanmak. “*Örnek Levent adını Lvnt olarak kullanmak gibi.”*
* Şifrenizi 8 karakterden az kullanamazsınız. Sistemin size izin verdiği uzunluk en güvenilir şifre konbinasyonlarını oluşturmaktadır.
* Sistem sadece rakamlardan veya harflerden oluşmasın. En az bir tane noktalama işareti ve sembol kullanmaya özen gösteriniz. *“! % & + .....”*
* Şifreniz sadece küçük harf ve sadece büyük harf kullanmayın.
* Şifrenizi bir kâğıda yazmayın veya cihazlara kaydetmeyin.
* Bütün hesaplarınız için ***“AYNI”*** şifreyi kullanmayınız.

*Bilgilendirme amacıyla Örnek olarak verilmiştir, hesaplarınızda kullanmayınız* ***!***

 *“MailSifRem!34” – “MeeMeeD19!” – “GuVenliSifreM(21)”*

1. **PAROLA YÜKÜMLÜLÜKLERİ**
	1. Kullanıcı parolaların gizliliğinden şahsen sorumludur
	2. Kullandığı tarayıcılarda parola hatırlatma kullanılmamalı veya üçüncü kişilerin erişebileceği şekilde kayıt altına almamalı ve paylaşmamalıdır.
	3. Parola ile yaşadığı sorunları [www.teknikdestek.yildiz.edu.tr](http://www.teknikdestek.yildiz.edu.tr) adresinden ivedi destek talebi açılmalıdır.
	4. Kurum bilgisayarı ise kurum teknik desteğinden destek almalıdır. Kişisel cihazları için, kişisel sorumluluğunda antivirüs yazılımları ile güvence altına almalıdır.
2. **YAPTIRIM**

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli 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 BGYS Temsilcisi tarafından e-posta üzerinden yazılı olarak uyarılır. Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3’ten fazla tekrar ederse “PR-033-Bilgi Güvenliği İhlal Olayları ve Disiplin Soruşturması Prosedürü” gereğince kişiler hakkında işlem yapılır. Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, birim amirinin bilgisi dahilinde BGYS Ekibi’ne en kısa sürede bildirme sorumluluğundadır.