1. **AMAÇ:**

Bu politikanın amacı, Yıldız Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı personellerine ait bilgi içeren mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.

1. **KAPSAM:**

Bilgi Güvenliği kapsamında çalışmalar yürütülen tüm birimleri kapsamaktadır. Dizüstü bilgisayar, gibi taşınabilir cihazlar, kurum bilgilerini kurum dışına taşıma imkanı sağladıklarından, bilgi sistemleri için önemli açıklar içerebilmektedir. Bu nedenle dizüstü bilgisayar, akıllı cep telefonları, tablet bilgisayar (ör: iPad) gibi taşınabilir cihazların kullanımının getirdiği risklere karşı dikkatli olunması esastır.

1. **UYGULAMA**
   1. Kuruma ait bilgi içeren taşınabilir ortam ve cihazlar ilgili kişiye zimmetlenerek teslim edilir.
   2. Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
   3. Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur. Taşınabilir cihaza erişim için mutlaka tahmin edilmesi zor bir PIN ya da parola oluşturulmalı ve cihazın kullanılmadığı zamanlarda otomatik olarak devreye girmesi sağlanmalıdır. Cihazların çalınma riskine karşı kullanıcıların özellikle halka açık mekanlarda cihazlarını gözetimsiz bırakmamaları ve cihazların fiziksel güvenliğini sağlamaları esastır. Kişiye zimmetlenen mobil cihazların kullanılmak üzere üçüncü kişilere teslim edilmemesi gerekmektedir.

* 1. Harici taşınabilir cihazların içi mekanik yapıya sahip olduğundan dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir.
  2. Kuruluşa ait bilgisayar, mobil cihazlar, taşınabilir bellek ve PDA cihazlara dışarıdan herhangi bir yazılım, siyasi propaganda, ırkçılık, şiddet, pornografi veya erotizm içeren resim, film veya müzik kopyalanmamalı ve cihaz içerisinde bulundurulmamalıdır.
  3. Kurum telefon hatları ve bilgisayarlar üzerinden üçüncü taraf kişilerle borç alacak ilişkisi, tehdit, küfür, Kurum itibarını zedeleyecek şeyler ve yasa dışı olan iletişim kurulmamalıdır.
  4. Dahili hatlar üzerinden kurum dışı arama gerçekleştirilirken santral üzerinden erişim sağlanır.
  5. Taşınabilir bilgisayarlar üzerinde yapılan kuruma ait çalışmalar ve oluşturulan dosyalar mutlaka ağ üzerinde ilgili adrese kaydedilmelidir. Mobil cihazda hassas ve gizli bilgiler mümkün olduğunca saklanmamalı, veriler periyodik olarak yedeklenerek güncel bir kopyası farklı bir yerde saklanmalıdır.
  6. Tüm taşınabilir bilgisayarlar kişisel ağ geçidi ve antivirüs korumalı olmalı ve bu yazılımlar hiçbir şekilde devre dışı bırakılmamalıdır. Taşınabilir cihazlara indirilen (download) uygulamalar ya da dosyalar indirilmeden önce indirilen program/dosya kaynaklarının güvenilirliğinden emin olunmalıdır. Taşınacak veri eğer usb disk ile taşınacaksa bu usb diskin tehdit unsuru olan bir yazılım içermediğine emin olunmalıdır.
  7. Taşınabilir bilgisayarlara korsan ve yasal olmayan yazılımlar yüklenmemelidir.
  8. Taşınabilir cihazlar, içerisindeki bilgilerin bütünlüğüne ve erişilebilirliğine zarar verme ihtimalinden dolayı manyetik alanlardan uzak tutulmalıdır
  9. Taşınabilir bilgisayarın kaybolması durumunda, zaman kaybetmeden ilgili birim amirinin bilgisi dahilinde BGYS Ekibi’ne haber verilmelidir.

1. **FİZİKSEL ORTAM AKTARIMI VE ORTAMIN YOK EDİLMESİ**
   1. Ortam artık ihtiyaç kalmadığında imha politikasında belirtilen hususlar dahilinde güvenli bir şekilde ortamın yok edilmesi süreçleri izlenir.
   2. Bilgi içeren ortam, aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunmalıdır. Süreçle ilgili ihlal olaylarında “PR-033-Bilgi Güvenliği İhlal Olayları ve Disiplin Soruşturması Prosedürü” kapsamında gerekli işlemler gerçekleştirilir.
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.