1. AMAÇ

Bu politikanın amacı, Süleyman Demirel Üniversitesi bünyesinde kullanılan ve kurumsal bilgi varlıklarını barındıran taşınabilir ortam ve cihazların güvenli kullanımına ilişkin kuralları belirlemek; bu cihazlarda bulunan bilgilerin yetkisiz erişim, kayıp, hırsızlık, kötü amaçlı yazılım, veri sızıntısı ve yetkisiz değişikliklere karşı korunmasını sağlamaktır.

2. KAPSAM

Bu politika; Üniversite bünyesinde kullanılan veya Üniversite bilgilerine erişim sağlayan;

- Dizüstü bilgisayarlar,
- Tabletler,
- Kurumsal mobil telefonlar,
- USB bellekler,
- Harici diskler,
- CD/DVD ve benzeri çıkarılabilir medya,
- Diğer taşınabilir veri depolama ortamları,
- Bilgi işleme veya depolama özelliğine sahip taşınabilir cihazları kapsar.

Politika, bu cihazların Üniversite personeli, ilgili taraflar veya görev kapsamında bilgi varlıklarına erişen diğer kullanıcılar tarafından kullanımını kapsar.

3. SORUMLULUKLAR

Bu politikanın uygulanmasından;

- Tüm çalışanlar,
- Birim yöneticileri,
- Cihaz ve bilgi varlığı sahipleri,
- Bilgi İşlem Daire Başkanlığı,
- Bilgi Güvenliği Yönetim Sistemi kapsamında görev ve sorumluluğu bulunan kişiler sorumludur.

Kendisine taşınabilir cihaz veya ortam tahsis edilen kullanıcı, ilgili cihazın güvenliğinden ve amacı doğrultusunda kullanılmasından sorumludur.

4. UYGULAMA

4.1. Cihazların Zimmeti ve Kullanımı

1. Kuruma ait bilgi içeren taşınabilir cihaz ve ortamlar, mümkün olduğunda ilgili kullanıcıya zimmet karşılığında teslim edilir.
2. Kullanıcı, kendisine teslim edilen cihazın fiziksel güvenliğini sağlamak, cihazı amacı dışında kullanmamak ve yetkisiz kişilerin erişimini engellemekle yükümlüdür.
3. Cihazın başka bir kullanıcıya devredilmesi halinde ilgili birim tarafından gerekli zimmet/devir işlemleri gerçekleştirilmelidir.
4. Kurumsal amaçla tahsis edilen cihazlar, görev gerektirmediği sürece aile fertleri, arkadaşlar veya diğer üçüncü kişiler tarafından kullanılmamalıdır.
5. Taşınabilir cihazlar halka açık alanlarda, araçlarda veya benzeri ortamlarda gözetimsiz bırakılmamalıdır.
6. Cihazların kaybolması, çalınması veya yetkisiz kişiler tarafından ele geçirilmesi halinde durum derhal ilgili birime ve gerekli olması halinde Olay İhlal Bildirim ve Yönetimi sürecine göre bildirilmelidir.

4.2. Erişim ve Kimlik Doğrulama

1. Taşınabilir cihazlara erişim için kurum tarafından belirlenen uygun kimlik doğrulama yöntemi kullanılmalıdır.
2. Cihazların otomatik ekran kilitleme özelliği etkinleştirilmelidir.
3. Destekleyen cihazlarda, kurumun belirlediği güvenlik gereksinimlerine uygun şekilde çok faktörlü kimlik doğrulama kullanılmalıdır.
4. Parola ve benzeri kimlik doğrulama bilgileri cihaz üzerinde görünür şekilde tutulmamalı ve başka kişilerle paylaşılmamalıdır.
5. Cihaz üzerinde bulunan kurumsal hesapların yetkisiz kişiler tarafından kullanılmasına izin verilmemelidir.

4.3. Kurumsal Bilgilerin Taşınabilir Cihazlarda Bulundurulması

1. Kurumsal bilgiler taşınabilir cihazlarda yalnızca **iş** gerekliliği ve yetki kapsamında bulundurulmalıdır.
2. Kişisel veri, özel nitelikli kişisel veri, Hizmete Özel, Gizli ve Çok Gizli sınıfta bulunan bilgiler taşınabilir cihazlarda gereksiz şekilde tutulmamalıdır.
3. Taşınabilir cihazda hassas veya gizli bilgi tutulması gerekiyorsa, kurumun belirlediği güvenlik tedbirleri uygulanmalı ve gerekli durumlarda şifreleme kullanılmalıdır.

4. Taşınabilir cihazlarda bulunan bilgi miktarı, işin yürütülmesi için gerekli olan asgari seviyede tutulmalıdır.
5. Taşınabilir cihazlarda bulunan kurumsal bilgilerin yetkisiz kişiler tarafından görüntülenmesini veya kopyalanmasını önleyecek tedbirler alınmalıdır.
6. Taşınabilir cihazlarda bulunan bilgiler, Üniversitenin bilgi sınıflandırma kurallarına uygun şekilde değerlendirilmelidir.
7. Taşınabilir cihazlarda bulunan bilgilerin sınıfına göre gerekli erişim, şifreleme, saklama ve aktarım tedbirleri uygulanmalıdır.

4.4. Taşınabilir Veri Depolama Ortamları

1. USB bellek, harici disk, CD/DVD ve benzeri çıkarılabilir ortamlar yalnızca kurumsal ihtiyaç ve yetkilendirme kapsamında kullanılmalıdır.
2. Kurum tarafından onaylanmamış veya kaynağı güvenilir olmayan taşınabilir depolama ortamları kurumsal bilgisayarlara bağlanmamalıdır.
3. USB bellek ve harici disk gibi ortamlar kullanılmadan önce kötü amaçlı yazılım riskine karşı kontrol edilmelidir.
4. Hassas bilgi içeren taşınabilir depolama ortamlarında gerekli olması halinde **şifreleme** uygulanmalıdır.
5. Taşınabilir depolama ortamlarında bulunan bilgiler, bilgi sınıflandırma seviyelerine uygun şekilde korunmalıdır.
6. Taşınabilir ortamların aktarımı sırasında kaybolma, çalınma veya yetkisiz kişilerin erişimine karşı gerekli fiziksel ve teknik tedbirler alınmalıdır.
7. Kurum tarafından izin verilmeyen taşınabilir depolama ortamları bilgi sistemlerinde kullanılmamalıdır.
8. Taşınabilir depolama ortamlarının kullanımı, gerektiğinde teknik olarak sınırlandırılabilir veya kontrol altına alınabilir.

4.5. Yazılım ve Uygulama Güvenliği

1. Taşınabilir cihazlarda yalnızca görev için gerekli ve kurum tarafından izin verilen yazılımlar kullanılmalıdır.
2. Korsan, lisanssız veya güvenilir olmayan kaynaklardan edinilen yazılımlar kurumsal cihazlara yüklenmemelidir.
3. Uygulamalar ve dosyalar güvenilir kaynaklardan edinilmelidir.
4. Cihazlarda bulunan antivirüs, uç nokta güvenliği ve benzeri güvenlik yazılımları kullanıcı tarafından devre dışı bırakılmamalıdır.

5. İşletim sistemi ve uygulamaların güvenlik güncellemeleri kurumun belirlediği yöntem ve sürelerde gerçekleştirilmelidir.
6. Kurumsal cihazlara kötü amaçlı yazılım, yetkisiz yazılım veya güvenliği tehlikeye atabilecek içeriklerin yüklenmesi engellenmelidir.

4.6. Taşınabilir Cihazlarda Veri Yedekleme

1. Kurumsal bilgilerin yedeklenmesi, Üniversitenin belirlediği Yedekleme Politikası/Prosedürü ve ilgili teknik kurallar doğrultusunda gerçekleştirilmelidir.
2. Taşınabilir cihazların kullanıcı tarafından kontrolsüz şekilde kişisel USB bellek, harici disk veya benzeri ortamlara yedeklenmesine izin verilmemelidir.
3. Yedekleme amacıyla taşınabilir ortam kullanılması halinde, ortamın kurum tarafından onaylanmış olması ve gerekli güvenlik tedbirlerinin uygulanması gerekir.
4. Taşınabilir cihaz üzerinde bulunan tek kopya niteliğindeki kritik kurumsal bilgiler bulundurulmamalıdır.

4.7. Fiziksel Güvenlik ve Taşıma

1. Taşınabilir cihazlar taşınması ve kullanılması sırasında fiziksel hasar, kayıp ve hırsızlığa karşı korunmalıdır.
2. Cihazlar araç içerisinde görünür şekilde bırakılmamalıdır.
3. Halka açık alanlarda kullanılan cihazların ekranlarının yetkisiz kişiler tarafından görülmesi engellenmelidir.
4. Taşınabilir ortamlar, taşıma sırasında yetkisiz kişilerin erişemeyeceği şekilde muhafaza edilmelidir.
5. Hassas bilgi içeren taşınabilir ortamların elden teslim edilmesi gerektiğinde, yalnızca yetkili kişilere teslim edilmelidir.

4.8. Cihazların Yeniden Kullanımı, İade ve İmha

1. Kurumsal bir cihazın başka bir kullanıcıya tahsis edilmesi, iade edilmesi veya kullanım dışı bırakılması öncesinde cihaz üzerinde bulunan kurumsal bilgilerin yetkisiz kişilerin erişimine açık kalmaması sağlanmalıdır.
2. Cihazlarda bulunan bilgilerin silinmesi, temizlenmesi, yeniden kullanıma hazırlanması veya cihazın imhası işlemleri Bilgi Varlıkları ve Bilgi Sınıflandırma Politikası ile İmha Politikası/Prosedürü doğrultusunda gerçekleştirilmelidir.
3. Basit dosya silme işleminin verileri her durumda geri döndürülemez şekilde ortadan kaldırmayabileceği dikkate alınmalıdır.

4. Kullanıcılar, cihaz veya taşınabilir ortam üzerinde kendi başlarına güvenli silme veya imha işlemi gerçekleştirmemeli; kurum tarafından belirlenen yetkili birim veya yöntemleri kullanmalıdır.
5. İmha işlemleri gerektiğinde kayıt altına alınmalı ve ilgili imha kayıtları/tutanakları oluşturulmalıdır.

4.9. Kayıp, Çalınma ve Güvenlik Olayları

1. Taşınabilir cihaz veya ortamın kaybolması, çalınması, yetkisiz kişilerce kullanılması veya içindeki bilgilerin yetkisiz kişiler tarafından erişildiğinin düşünülmesi halinde olay derhal ilgili birime bildirilmelidir.
2. Olayda kişisel veri bulunması halinde Kişisel Veri İhlali Yönetimi süreci de değerlendirilmelidir.
3. Cihazın kaybolması veya çalınması durumunda gerekli görülmesi halinde cihazın uzaktan kilitlenmesi, hesabın devre dışı bırakılması veya diğer teknik güvenlik tedbirleri uygulanmalıdır.
4. Güvenlik olaylarının değerlendirilmesi ve müdahalesi ilgili Olay Yönetimi Prosedürü doğrultusunda gerçekleştirilir.

5. BİLGİ SINIFLANDIRMASI VE ETİKETLEME

Taşınabilir ortam ve cihazlarda bulunan bilgiler, Üniversitenin Bilgi Sınıflandırma ve Etiketleme Politikası kapsamında belirlenen sınıflandırma seviyelerine göre korunmalıdır. Özellikle Hizmete Özel, Gizli ve Çok Gizli sınıftaki bilgiler taşınabilir cihaz veya ortamlarda tutulduğunda, yetkisiz erişimi önlemek amacıyla gerekli erişim kontrolü, fiziksel güvenlik ve şifreleme tedbirleri uygulanmalıdır. Taşınabilir ortamın veya cihazın kendisi, üzerinde bulunan bilgi varlıklarının gerektirdiği güvenlik seviyesine uygun şekilde korunmalıdır.

5. YAPTIRIM

Bu politikada belirtilen kurallara aykırı hareket edilmesi halinde, olayın niteliğine göre ilgili EYS süreçleri işletilir ve gerekli olması halinde Disiplin Prosedürü hükümleri uygulanır.