1.1.Mobil Cihaz Politikası

Kontrol: Mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmelidir.

Uygulama Kılavuzu: Mobil cihazlar kullanılırken, is bilgilerinin ele geçirilmemesini temin için özel bir önem gösterilmelidir. Mobil cihaz politikası, korumasız ortamlarda mobil cihazların çalışması riskini hesaba katmalıdır.

Mobil cihaz politikası aşağıdaki hususları dikkate almalıdır:

a) Mobil cihazların kaydı,

b) Fiziksel koruma için gereksinimler,

c) Yazılım kurulum kısıtlaması,

d) Mobil cihaz yazılım sürümleri ve yamaların uygulanması için gereksinimler,

e) Bilgi hizmetlerine bağlantı kısıtlaması,

f) Erişim kontrolleri,

g) Kripto grafik teknikler,

h) Kötücül yazılım koruması,

i) Uzaktan devre dışı bırakma, silme ya da kilitleme,

j) Yedekleme,

k) Web servislerinin ve web uygulamalarının kullanımı.

Halka açık yerlerde, toplantı odalarında ve diğer korumasız alanlarda mobil cihazların kullanımına dikkat edilmelidir. Bu cihazlar tarafından saklanan ve islenen bilginin, açıklanmasına ya da yetkisiz erişimine karsı koruma bulunmalıdır. Örneğin; kartografi teknikleri kullanmak (bk. Madde 10) ve gizli kimlik doğrulama bilgisinin kullanımını zorlamak (bk. Madde 9.2.4).

Mobil cihazlar; araba ve diğer ulaşım araçları, otel odaları, konferans merkezleri ve toplantı salonları gibi yerlerde hırsızlığa karsı fiziksel olarak da korunmalıdır. Mobil cihazların çalınması ya da kaybolması durumları için yasal, sigorta ve kurulusun diğer güvenlik gereksinimleri dikkate alınarak özel bir prosedür oluşturulmalıdır.

Önemli, hassas ya da kritik is bilgilerini taşıyan cihazlar sahipsiz bırakılmamalı, mümkünse fiziksel olarak kilitlenmeli ya da cihazı güvenli hale getirmek için özel kilitler kullanılmalıdır.

Mobil cihaz kullanan personeller için, bu şekilde çalışmalardan kaynaklanan riskler ve uygulanması gereken kontroller ile ilgili olarak farkındalıklarının arttırılması amacıyla eğitim düzenlenmelidir.

Mobil cihaz politikası kişisel mobil cihazların kullanımına izin veriyorsa, politika ve diğer güvenlik önlemlerinde aşağıdaki hususlara dikkat edilmelidir:

a) Cihazların özel ve is kullanımının ayrılması. Bu ayrım özel cihazda bulunan iş verisinin ayrılması ve korunması gibi yazılımların kullanılmasını içerir,

b) Kullanıcıların görevlerini kabul ettikleri son kullanıcı anlaşmasını imzalamalarından sonra iş bilgilerine erişim sağlanması (fiziksel koruma, yazılım güncelleme vb.), is verilerinin sahipliğinden feragat, cihazın çalınması ya da kaybolması ya da hizmetin kullanımı yetkilendirmesi için vakit olmadığında kuruluş tarafından verilerin uzaktan silinmesine izin verilmesi. Bu politikada mahremiyet mevzuatının dikkate alınması gerekmektedir.

Diğer Bilgiler: Mobil cihazların kablosuz ağ bağlantıları (wi-fi) diğer ağ bağlantısı türlerine benzer, ancak; kontrollerin tanımlanmasında önemli farklılıklara dikkat edilmelidir. Tipik farklılıklar şunlardır:

a) Bazı kablosuz güvenlik protokolleri olgunlaşmamıştır ve bilinen açıklıklara sahiptir,

b) Mobil cihazlarda depolanan bilgiler, kısıtlı ağ bant genişliği ya da yedeklemelerin planlandığı zamanlarda mobil cihazların bağlanamaması nedeniyle yedeklenemeyebilir. Mobil cihazlar sabit kullanım cihazları ile genellikle ağ, internet erişimi, e-posta ve dosya isleme gibi ortak fonksiyonları paylaşır. Bilgi güvenliği kontrolleri mobil cihazlar için genellikle sabit

kullanım cihazlarında kabul edilen kontrollerden ve bu cihazların kurulusun tesisi dışındaki kullanımı ile gündeme gelen tehditleri ele alan kontrollerden oluşur.

c) Kuruluşa ait bilgi içeren taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilmelidir.

d) Her çalışan kendisine zimmetlenen mobil cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.

e) Etki alanı dâhilindeki bilgisayarlar istisnalar dışında admin yetkisi sınırlandırılarak yalnızca User yetkilendirmesi ile ilgili kişiye teslim edilmelidir. Etki alanından bağımsız olan bilgisayarların sorumluluğu personele aittir.

f) Mobil cihazlara yetkisiz erişime karşı şifre tanımlanmalıdır.

g) Cep telefonları veya tablet bilgisayarlara kurum e-postası kurulması halinde cihazın güvenliğinin sağlanması adına şifre koruması olması zorunludur.

h) Etki alanı dâhilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar birimlere ait ilgili ortak alana kaydedilmelidir.

ı) Mobil cihazların (Dizüstü Bilgisayar, Tablet vb.) aile bireyleri dâhil zimmetlenen kişiler dışında kullanılması yasaktır.

i) Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.

j) Verilerin yedekleri alınmalı ve güncel bir kopyası farklı bir yerde saklanmalıdır.

k) Mobil cihazların uzaktan devre dışı bırakma ve silme özellikleri mutlaka kullanılmalıdır.