

**MOBİL CİHAZ KULLANIM POLİTİKASI**

NETPAK Ambalaj olarak, mobil cihazların kullanımı ile ortaya çıkan risklerin yönetilmesi amacı ile bir politika ve destekleyici güvenlik önlemleri belirlenmiştir.

Uygulama kılavuzu Mobil cihazlar kullanılırken, iş 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 almaktadır:

a) Mobil cihazların kaydı,   
b) Fiziksel koruma için gereksinimler,   
c) Yazılım kurulum kısıtlaması,   
d) Mobil cihaz yazılım sürümleri ve programların yamaların uygulanması için gereksinimler,

e) Bilgi hizmetlerine bağlantı kısıtlaması,   
f) Erişim kontrolleri,   
g) Kripto grafik teknikler,   
h) Zararlı (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 işlenen bilginin, açıklanmasına ya da yetkisiz erişimine karşı koruma bulunmalıdır. Örneğin; kriptografi teknikleri kullanmak ve gizli kimlik doğrulama bilgisinin kullanımını zorlamak.

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

Önemli, hassas ya da kritik iş 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 iş 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.), iş 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 işleme gibi ortak fonksiyonları paylaşır. Bilgi güvenliği kontrolleri mobil cihazlar için genellikle sabit kullanım cihazlarında kabul edilen kontrollerden ve bu cihazların kuruluşun tesisi dışındaki kullanımı ile gündeme gelen tehditleri ele alan kontrollerden oluşur. Mobil cihazların kullanımı ve uzaktan çalışma, kuruluşların BGYS için potansiyel bir tehlikedir. Çünkü; cihazlar ve kullanıcılar fiziksel olarak firmamızın ve networkümüzün dışındalar. Konuya gerekli önemin verilmemesi ve gerekli önlemlerin alınmaması büyük problemler yaratabilir

HAZIRLAYAN ONAYLAYAN

KALİTE MÜDÜRÜ YÖNETİM KURULU ÜYESİ