BAŞARILI BYOD BT POLİTİKASI İÇİN ÖNERİLER

MAKALE

EĞER BİR BYOD (KENDİ CİHAZINI GETİR) POLİTİKASI GELİŞTİRMEDİYSENİZ VEYA GÜNCEL OLMAYAN BİR POLİTİKAYA SAHİPSENİZ; BU MAKALE SİZE CİHAZ GÜVENLİĞİ, BT HİZMETİ, UYGULAMA KULLANIMI VE ETKİLİ BİR BYOD POLİTİKASININ DİĞER ÖNEMLİ BİLEŞENLERİ KONULARINDA YARDIMCI OLACAKTIR.

2015 yılı sonunda dünya genelinde 2 milyar akıllı telefonun dolaşımda olacağı tahmin ediliyor. Eğer çalışanların kendi cihazlarıyla kurumsal e-maile, takvim yönetimine ve iletişim sistemlerine erişmesini desteklemediyseniz bu durum artık değişecek, değişmek zorunda. Şirket personelin genelinin taleplerini şimdilik göz ardı etseniz bile CEO'lar ve üst yöneticiler akıllı telefonlar ve tabletleri yaygın olarak kullanıyorlar ve bu cihazları seyahatleri, toplantıları için yararlı buluyorlar. Bu baskı sizde kısa bir süre içinde bir BYOD politikasının nasıl geliştirileceği ve en iyi şekilde nasıl uygulanacağı konusunda merak uyandırabilir. Bir BYOD politikası geliştirirken; her bir fikir kendinize, BT departmanınıza ve yönetim ekibinize sormanız gereken önemli soruları da beraberinde getirir. Bu makale 7 temel başlık/ipucu altında doğru bir BYOD programı ile ilgili sorularınızı cevaplamak için hazırlarlanmıştır.

Hangi cihazlara izin verileceğini belirleyin.
Bu konu Blackberry'nin eski günlerinde gayet basit ve açıktı, çünkü Blackberry'nizi sadece iş için kullanıyordunuz. Fakat şimdi yoğunlukla iOS ve Android tabanlı telefon ve tabletlerin oluşturduğu geniş bir seçim yelpazesi bulunmakta.

Burada önemli olan 'Kendi Cihazını Getir' derken tam olarak neyin ifade edildiğine karar vermek. Hangi cihazın getirilip getirilemeyeceği konusunda açıklık getirmeli, sadece iPhone veya iPad mi yoksa Android bir cihaz mı kullanılabilir?

Tüm cihazlar için sıkı güvenlik politikası oluşturun.
Kullanıcılar kişisel cihazlarında şifrelere veya kilitli ekranlara karşı direnç gösterme eğilimindedir. Bunları içeriğe ve fonksiyonlara kolay ulaşmak için bir engel olarak görürler. Fakat bu kişisel cihazların kurumsal sistem altında kullanıldığı durumlarda geçerli bir şikayet değildir. Çünkü önemli bilgilerin olduğu bir sistemden serbestçe bilgi sızdırılmasına izin vermemek için sisteme bağlanan cihazların kontrol edilmesi gerekir.

Eğer kullanıcılarınız kendi cihazlarını sizin sisteminizi kullanmak istiyorlarsa, her zaman için kendi cihazlarına bütünleştirilmiş karmaşık bir parola yapısını kabul etmek zorundadırlar. Sizin sistem güvenliği için ihtiyacınız olan basit 4 haneli sayısal bir şifre değil güçlü ve uzun bir alfanumerik bir şifredir.

BYOD kapsamındaki cihazlar için açık bir destek politikası tanımlayın.
Bu durum, çalışanların kişisel cihazlarından kaynaklanacak soru ve sorunlarının sınırlarını anlamaları için önemlidir. Bu sınırları ayarlamak için aşağıdaki soruları cevaplamak gerekir.

- Kişisel cihazlardan ağınıza gelecek bağlantılar için desteğiniz hangi düzeyde olacak ?
- BT temsilcileri bozuk cihazlar için ne tür bir destek sağlayacak ?
- Kişisel cihazlarda yüklü olan uygulamalar için ne tür bir destek sağlanacak?
- E-mail, takvim ve diğer kişisel bilgi içeren uygulamalara erişim sorunlarında "Yardım" konusunda sınırlama getirilecek mi ?
- Daha önceden belirlediğiniz bir durumda kişisel uygulamadan kaynaklanan bir sorun çıktığında ne olacak?
- Desteğiniz aslında bir "silme ve tekrar yapılandırma" operasyonu mu ?
- Çalışanlarınızın kendi telefon veya tabletleri servisteyken onlara ödünç cihaz vermeyi önerecek misiniz ?

Hangi uygulama ve bilginin sahibinin kim olduğuna açıklık getirin.
Şirketin, çalışanların cihazlarıyla girdiği sunucularda saklanan kişisel bilgilerin sahibi olduğu görünüşte mantıklıdır. Fakat bu durum , kayıp ve çalıntı durumlarında cihazın silinmesi problemi dikkate alındığında daha sorunlu bir hale gelir. Telefonu temizlediğinde, kişisel fotoğraflar ve müzikler dahil geleneksel içeriğin yanında uygulamalar da silinir. Bazen bu öğeleri yerine getirmek imkansızdır.

Sizin BYOD politikanız cihazı silme konusunda hak iddia etme konusuna açıklık getiriyor mu? Eğer öyleyse, siz çalışanlarınız için kendi içeriklerini koruma ve herhangi bir cihaz değişikliğinde kişisel bilgilerinin eski haline getirilmesi konularında rehberlik sağlıyor musunuz ?

Hangi uygulamalara izin verileceği, hangilerinin yasaklanacağına karar verin.
Bu kurumsal ya da kişisel olsun, çalışma ortamınızı bağlanacak herhangi bir cihaz için geçerlidir. Bu konudaki önemli hususlar genel olarak sosyal medya, yedek e-posta, VPN veya diğer uzaktan erişim uygulamalarını içermektedir.

Buradaki soru kullanıcıların, hassas kurumsal kaynaklara erişebilecek güvenlik veya yasal risk içeren uygulamaları indirmesi, kurması ve kullanması üzerinedir. Varsayımsal olarak kötü yazılmış veya güvenlik açığı olan uygulamalar yüzünden şirketin özel bilgilerine 3. kişiler erişebilir.

BYOD planınızla kullanım politikanızı entegre edin.
Kişisel cihazların VPN bağlantısına imkan verilmesi hangi aktivitelere izin verilip hangilerine verilmeyeceği şüphelerini de ortaya koyar.

- Bir iPhone üzerinden VPN tünel kurmak ve çalışanların buradan Facebook'a bağlanması bir ihlal midir?
- Ya çalışanlarınız kendi cihazlarının VPN'inden sakıncalı web sitelerine göz atarlarsa ?
- Çalışanlarınız kendi kişisel cihazlarını kullanarak ağınız üzerinden isteyerek veya istemeden uygunsuz öğe iletimi durumunda ne olur ? Bu tür bir olayda yaptırım nedir?
- Ne tür görüntüleme stratejileri ve araçları bü tür politikaların uygulanması için kullanılabilir?
- Bu alanda kuralları düzenlemek için hangi haklara sahipsiniz ?

Çalışanların sistemden çıkış stratejisi kurun.
Sizin BYOD platformunuzda cihazıyla çalışanların şirketten ayrıldığında neler yapmanız gerektiğini belirlemeyi unutmayın. E-mail, veri ve diğer özel uygulamalarla bilgilere erişilmesini nasıl engelleyeceksiniz? Bunun için bazı şirketler e-mail ve senkronizasyonu devre dışı bırakırken, güvenlik bilinci daha fazla olan şirketler de zorunlu çıkış stratejisi olarak BYOD cihazını silmeyi tercih eder. Fakat bu silme yönteminin kullanılabilmesi için de kullanıcının kişisel fotoğraflarının ve kendisinin satın aldığı uygulamaların geri getirilebileceği bir metodolojiye sahip olunmalıdır.

İSTANBUL
T 0 212 288 31 00
F 0 212 275 40 01
istanbul@karel.com.tr

ANKARA
T 0 312 293 01 00
F 0 312 267 21 05
ankara@karel.com.tr

İZMİR
T 0 232 445 55 55
F 0 232 441 73 73
izmir@karel.com.tr

ANTALYA
T 0 242 323 13 13
F 0 242 323 09 83
antalya@karel.com.tr

BURSA
T 0 224 244 74 84
F 0 224 244 98 00
bursa@karel.com.tr

VAN
T 0 312 293 01 00
F 0 312 267 21 05
van@karel.com.tr

www.karel.com.tr

BYOD Ver. 1.0 - 15/06/12