المستخدم بذلك، ويعني ذلك أن الكلمات السرية للشركات وقواعد البيانات السرية وكل البيانات المالية (بم) في ذلك أرقام بطاقات الائتمان الشخصية والخاصة بالشركات) معرضة للخطر.تأمين البيانات النقالةأفضل وأول طريقة لحماية أصول المعلومات السرية هي إزالة المعلومات السرية وغير الضرورية وغير المستخدمة من على الجهاز ولا ينبغي تخزين البيانات السرية على الأجهزة النقالة إلا بإذن صريح من إدارة تقنية المعلومات IT أو رئيس وحدة النشاط التجاري، أو مجلس حوكمة المعلومات (IG) للقيام بذلك. ويتضمن ذلك قوائم الأسعار والخطط الإستراتيجية والمعلومات التنافسية والصور الفوتوغرافية الخاصة بمباني الشركة وعمالها والبيانات المالية مثل، أرقام الضرائب التعريفية وبطاقة ائتمان الشركة والبيانات البنكية والمعلومات السرية الأخرى.إذا كان من اللازم تخزين البيانات الحساسة على الأجهزة النقالة، فهناك خيارات لتأمين البيانات بطريقة أكثر إحكاماً باستخدام مشغلات "يو إس بي USB" مشغلات فلاش ومشغلات صلبة مزودة بإمكانيات هوية رقمية متكاملة وتقنيات التشفير.إدارة الأجهزة النقالةتساعد برامج إدارة الأجهزة النقالة MDM – Mobile Device Management) الشركات السيطرة وتأمين وإدارة أجهزة مثل الهواتف الذكية والأجهزة اللوحية الشخصية PCS ' عن بعد وتحسن عملية إدارة الأجهزة النقالة من تأمين وإدارة خطوط الانسياب بالشركة من خلال تقديم طرق للاتصال بالأجهزة عن بعد بشكل فردي أو جماعي لإضافة أو ترقية أو إلغاء برامج أو تغيير إعدادات التهيئة وحذف أو مسح البيانات أو إدخال أي تحديثات أو تغييرات تتعلق بعملية التأمين، وتستطيع بعض عروض إدارة الأجهزة النقالة المتطورة إدارة ليس فقط الأجهزة النقالة MDM المتجانسة المملوكة للشركة ولكن أيضا الأجهزة التي يستخدمها الموظفون في مكان العمل في بيئة عمل تتطلب إحضار جهازك المحمول (Bring-your-own-device – BYOD).وتمكن القدرة على التحكم في إعدادات التهيئة وتأمين البيانات عن بعد المؤسسات من التحكم بشكل أفضل والسيطرة على الأجهزة النقالة،حوكمة المعلومات للأجهزة النقالة٣٥٥البائعون الأساسيون في أسواق إدارة الأجهزة النقالة MDM هم إير وتش AirWatch، آبل Appleبروفايل المدير Profile Manager آيسينس AppSense، بوكس تون BoxTone، سينترفاي Centrify سيتريكس Citrix، جود تقني Good Technology (IBM) آي بي إم (مدير النقطة النهائية للأجهزة النقالة Endpoint Manager for Mobile Devices) لانديسك LANDesk ، موبايلآيرون MobileIron، ساب SAP (إدارة الجهاز المحمول أفاريا Africa MDM)، سيمانتيك Symantec مجموعة برامج إدارة الجوال(٢٠١٨Mobile Management Suite ويتوقع أيضاً فروست وسوليفان Frost & Sullivan أن سوق إدارة الأجهزة النقالة MDM بالشركات سوف ينمو من ١٧٨,٦ مليون دولار أمريكي إلى ٧١٢ مليون دولار أمريكي بحلول عام ٢٠١٨ .اتجاهات إدارة الأجهزة النقالةسنناقش ستة اتجاهات في سوق إدارة الأجهزة النقالة MDM فيما يلي: . تطور وتوسع إدارة الأجهزة النقالة يعتقد العديد من الخبراء تطور إدارة الأجهزة النقالة ووصولها إلى ما بعد النقاط النهائية النقالة لتتضمن التكامل العميق مع البنية التحتية والتطبيقات النقالة "، فضلا عن التحكم فيه وإدارة التكاليف من خلال إدارة النفقات بشكل متكامل . .. . إدارة الأجهزة النقالة السحابية MDM ستصبح القاعدة الثابتة وليس الاستثناء وسوف يحدث ذلك سريعا إلى حد ما.٤. التأكيد على سياسة الأجهزة النقالة ستعمل التقنية وتكون مفيدة بقدر ما تمتلك المؤسسة من سياسات وعمليات حوكمة المعلومات IG وممارسات مراجعة داخلية مكونة ومختبرة ومتابعة، حيث يتعين أن يكون لدى إدارة تقنية المعلومات IT اتجاه واضح حول البيانات والأجهزة التي ينبغي تأمينها ومتابعتها مع توضيح وتوصيل مسئوليات وحقوق الموظفين.٣٥٦حوكمة المعلومات ـ مبادئ، واستراتيجيات، وأفضل الممارسات تنويع وتوسيع التأمين والمتابعة النقالة: يعني ذلك أن إدارة الأجهزة النقالة سوف تذهب أبعد من الأجهزة النقالة الحالية، وتتضمن أدوات وآلات بعيدة تنقل البيانات في التطبيقات مثل إدارة المعالجة والنقل وإدارة موارد المؤسسة.٦. السحابية، وتصبح البناء الجديد لنموذج البنية التحتية مما يعني ظهور أدوات لإدارة كل تلك الأجزاء بشكل شمولي ومركزي.حوكمة المعلومات للحوسبة النقالةتعتبر إرشادات جامعة ستانفورد أساسًا مساعدًا في عملية حوكمة معلومات الأجهزة النقالة،الهواتف الذكية والكمبيوتر اللوحي (تابلت):● تشفير الاتصالات بالنسبة للهواتف التي تدعم الاتصالات المشفرة تقوم (طبقة الوصلات الآمنة [SSL] والشبكة الخاصة الافتراضية [VPN] وتأمين لغة نقل النصوص المتصلة [http] دائمابضبط العيوب لاستخدام التشفير. التخزين المشفر: يتعين تشفير المخزون الضخم للهواتف المسموح بوصولها للمعلوماتالسرية رسميا بشفرة مادية.● حماية كلمة المرور: يجب إنشاء كلمة مرور للوصول إلى واستخدام الجهاز وينبغي أن تتكون كلمات المرور الخاصة بالأجهزة التي تصل إلى أصول المعلومات السرية من سبعة رموز على الأقل وتتضمن حروفًا كبيرة وحروفًا صغيرة وأرقامًا مع تغيير الكود السري كل ٣٠ يوما. . وقت الانتظار: إعداد الجهاز بحيث يغلق بعد مدة من الإيقاف عن العمل أو الانتظار ربما تكون تلك المدة قصيرة؛ لمدة دقائق معدودة. التحديث:

تحديث كل الأنظمة والتطبيقات بما في ذلك أنظمة التشغيل والتطبيقات المثبتة ممايسمح بتثبيت أحدث البرامج والتطبيقات والتصحيحات والتدابير الأمنية لمواجهة التهديدات المستمرة. . الحماية من التراجع: لا ينبغي كسر القيود المفروضة على الهواتف المصرح بوصولها إلى المعلوماتوالبيانات السرية والمقيدة (مدعومة الوصول المميز على الهواتف الذكية باستخدام نظام تشغيل المعلومات آبل) أو بتثبيتها (تشير نمطيا إلى كسر القيود على الهواتف الذكية التي تعمل بنظام تشغيل آندرويد) و تختلف عملية التثبيت من جهاز لأخر وتتضمن عادة استغلال ضعف التأمين في البرامج المثبتة من جانب المصنع،