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 أو رئيس وحدة النشاط التجاري، أو مجلس حوكمة IT السرية على الأجهزة النقالة إلا بإذن صريح من إدارة تقنية المعلومات للقيام بذلك. ويتضمن ذلك قوائم الأسعار والخطط الإستراتيجية والمعلومات التنافسية والصور الفوتوغرافية (IG) المعلومات 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 مشغلات فلاش ومشغلات صلبة مزودة بإمكانيات هوية رقمية متكاملة "USB بطريقة أكثر إحكاماً باستخدام مشغلات "يو إس بي الشركات (Mobile Device Management – MDM وتقنيات التشفير.إدارة الأجهزة النقالةتساعد برامج إدارة الأجهزة النقالة عن بعد وتحسن عملية إدارة الأجهزة ' PCS السيطرة وتأمين وإدارة أجهزة مثل الهواتف الذكية والأجهزة اللوحية الشخصية 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، المتجانسة المملوكة للشركة ولكن MDM وتستطيع بعض عروض إدارة الأجهزة النقالة المتطورة إدارة ليس فقط الأجهزة النقالة (Bring–your–own– أيضا الأجهزة التي يستخدمها الموظفون في مكان العمل في بيئة عمل تتطلب إحضار جهازك المحمول وتمكن القدرة على التحكم في إعدادات التهيئة وتأمين البيانات عن بعد المؤسسات من التحكم بشكل أفضل.(device – BYOD MDM والسيطرة على الأجهزة النقالة،حوكمة المعلومات للأجهزة النقالة٣٥٥البائعون الأساسيون في أسواق إدارة الأجهزة النقالة سينترفاي، BoxTone بوكس تون، AppSense آيسينس Profile Manager بروفايل المديرApple آبل، AirWatch هم إير وتش Endpoint آي بي إم (مدير النقطة النهائية للأجهزة النقالة (Good Technology IBM) جود تقني، Citrix سيتريكس Centrify إدارة الجهاز المحمول أفاريا) SAP ساب، MobileIron موبايلآيرون ، LANDesk لانديسك (Manager for Mobile Devices ويتوقع أيضاً ٢٠١٨(Mobile Management Suite)مجموعة برامج إدارة الجوال Symantec سيمانتيك، Africa MDM) بالشركات سوف ينمو من ١٧٨,٦ مليون دولار MDM أن سوق إدارة الأجهزة النقالة Frost & Sullivan فروست وسوليفان أمريكي إلى ٧١٢ مليون دولار أمريكي بحلول عام ٢٠١٨ .اتجاهات إدارة الأجهزة النقالةسنناقش ستة اتجاهات في سوق إدارة فيما يلي: . تطور وتوسع إدارة الأجهزة النقالة يعتقد العديد من الخبراء تطور إدارة الأجهزة النقالة ووصولها MDM الأجهزة النقالة إلى ما بعد النقاط النهائية النقالة لتتضمن التكامل العميق مع البنية التحتية والتطبيقات النقالة "، فضلا عن التحكم فيه وإدارة ستصبح القاعدة الثابتة وليس MDM التكاليف من خلال إدارة النفقات بشكل متكامل . .. . إدارة الأجهزة النقالة السحابية الاستثناء وسوف يحدث ذلك سريعا إلى حد ما.٤. التأكيد على سياسة الأجهزة النقالة ستعمل التقنية وتكون مفيدة بقدر ما تمتلك وممارسات مراجعة داخلية مكونة ومختبرة ومتابعة، حيث يتعين أن IG المؤسسة من سياسات وعمليات حوكمة المعلومات اتجاه واضح حول البيانات والأجهزة التي ينبغي تأمينها ومتابعتها مع توضيح وتوصيل IT يكون لدى إدارة تقنية المعلومات 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 والشبكة الخاصة الافتراضية [SSL] الاتصالات بالنسبة للهواتف التي تدعم الاتصالات المشفرة تقوم (طبقة الوصلات الآمنة دائمابضبط العيوب لاستخدام التشفير. التخزين المشفر: يتعين تشفير [http] وتأمين لغة نقل النصوص المتصلة [VPN] 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:

Summarized by © lakhasly.com

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،

Summarized by © lakhasly.com