

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 النقلة أفضل وأول طريقة لحماية أصول المعلومات السرية هي إزالة المعلومات السرية وغير الضرورية وغير المستخدمة من على الجهاز ولا ينبغي تخزين البيانات السرية على الأجهزة النقلة 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 و بطاقة ائتمان الشركة والبيانات البنكية والمعلومات السرية الأخرى. إذا كان من اللازم تخزين البيانات الحساسة على الأجهزة النقلة، 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 النقلة تساعد برامج إدارة الأجهزة النقلة (Mobile Device Management – MDM) الشركات للسيطرة وتأمين وإدارة أجهزة مثل الهواتف الذكية والأجهزة اللوحية الشخصية PCS¹ عن بعد وتحسن عملية إدارة الأجهزة النقلة 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 النقلة المتطورة إدارة ليس فقط الأجهزة النقلة MDM المتجانسة المملوكة للشركة ولكن أيضاً 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 النقلة، حوكمة المعلومات للأجهزة النقلة ٢٥ه٠ البائعون الأساسيون في أسواق إدارة الأجهزة النقلة MDM هم إير وتش AirWatch، آبل Apple بروفايل المدير Profile Manager آيسينس AppSense، بوكس تون BoxTone، سينترفاي Centrifry سبتريكس Citrix، جود تقني (IBM) Good Technology (آي بي إم) (مدير النقطة النهائية للأجهزة النقلة Endpoint Manager for Mobile Devices) لانديسك LANDesk، موبايلايرون MobileIron، ساب SAP (إدارة الجهاز المحمول أفاريا Africa MDM)، سيمانتيك Symantec مجموعة برامج إدارة الجوال (٢٠١٨) Mobile Management Suite ويتوقع أيضاً فروست وسوليفان Frost & Sullivan أن سوق إدارة الأجهزة النقلة MDM بالشركات سوف ينمو من ١٧٨,٦ مليون دولار أمريكي إلى ٧١٢ مليون دولار أمريكي بحلول عام ٢٠١٨. اتجاهات إدارة الأجهزة النقلة سنناقش ستة اتجاهات في سوق إدارة الأجهزة النقلة MDM فيما يلي: . تطور وتوسع إدارة الأجهزة النقلة يعتقد العديد من الخبراء تطور إدارة الأجهزة النقلة ووصولها إلى ما بعد النقاط النهائية النقلة لتتضمن التكامل العميق مع البنية التحتية والتطبيقات النقلة"، فضلاً عن التحكم فيه وإدارة التكاليف من خلال إدارة النفقات بشكل متكامل . . . إدارة الأجهزة النقلة السحابية MDM ستصبح القاعدة الثابتة وليس الاستثناء وسوف يحدث ذلك سريعاً إلى حد ما. ٤. التأكيد على سياسة الأجهزة النقلة 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 مسؤوليات وحقوق الموظفين. ٥٦. حوكمة المعلومات - مبادئ، واستراتيجيات، وأفضل الممارسات تنوع وتوسيع التأمين والمتابعة النقلة: يعني ذلك أن إدارة الأجهزة النقلة سوف تذهب أبعد من الأجهزة النقلة 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 النقلة تعتبر إرشادات جامعة ستانفورد أساساً مساعداً في عملية حوكمة معلومات الأجهزة النقلة، 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]) دائماً بضبط العيوب لاستخدام التشفير. التخزين المشفر: يتعين تشفير المخزون الضخم للهواتف المسموح بوصولها للمعلومات السرية رسمياً 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 حروفاً كبيرة وحروفاً صغيرة وأرقاماً مع تغيير الكود السري كل ٣٠ يوماً. . 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 مما يسمح بتثبيت أحدث البرامج والتطبيقات والتصحيحات والتدابير الأمنية لمواجهة التهديدات المستمرة. . الحماية من التراجع: لا ينبغي كسر القيود المفروضة على الهواتف المصرح بوصولها إلى المعلومات والبيانات 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 أندرويد) و تختلف عملية التثبيت من جهاز لآخر وتتضمن عادة استغلال ضعف التأمين في البرامج المثبتة من جانب المصنع،