

إليك ملخص الفصل السابع من الملف "Guidelines and Best Practices in Recent Trends" (مثل BYOD و IoT): ---  
عناصر سياسة 1: BYOD. إدارة كلمات المرور 2. حماية الخصوصية 1. وضع سياسة أمنية قوية: تشمل التشفير، تجنب الواي فاي العام، 3. بناء ثقافة أمنية: توعية الموظفين بدورهم في الأمن السيبراني. 5. فصل البيانات الشخصية عن بيانات العمل: باستخدام تطبيقات مخصصة و VPN. التحكم بتثبيت التطبيقات: مثل حظر App Store أو استخدام Android Enterprise. 9. القوائم السوداء: حظر التطبيقات غير المرغوب بها. القوائم البيضاء: السماح فقط للتطبيقات المعتمدة. إدارة الأجهزة المحمولة (MDM) VPN) مدير كلمات المرور --- ثانياً: حماية أجهزة إنترنت الأشياء (IoT) هي أجهزة ذكية متصلة بالإنترنت تؤدي وظائف محددة، إرشادات الحماية: 2. التحديثات المنتظمة: لتجنب الثغرات الأمنية. 4. تشفير البيانات: أثناء النقل والتخزين. 6. مراقبة الأجهزة: لرصد السلوكيات الغريبة. 8. اختيار الموردين الآمنين. 10. 12. شبكة آمنة. تخزين بيانات محمي.