

الفصل السابع

امن المعلومات
والمسؤولية الاخلاقية
والاجتماعية

اعداد المدرس المساعد
عرفات اليوسف
جامعة البصرة / كلية الادارة والاقتصاد /
قسم نظم المعلومات الادارية

ماهي استراتيجيه وسياسات امن المعلومات

استراتيجية امن المعلومات // تتمثل بشأن اقتناء الاجهزة التقنية وادواتها والبرمجيات واللول المتصلة بالعمل وادارة النظام وكذلك تتضمن الاتي :-

- ١- استراتيجية الخصوصية المعلوماتية
- ٢- استراتيجية الاشتراكات في شبكتها من قبل الغير
- ٣- التعامل مع المخاطر والافطاء واجراء الابلاغ عنها للجهات ذات العلاقة
- ٤- تحقيق النجاح في استراتيجية امن المعلومات يحتاج ان تكون واضحة ودقيقة في محتواها ومفهومها لدى كافة المعنيين

سياسة امن المعلومات // هي مجموعة القواعد التي يطبقها اشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشاة وتتضمن بشأن الدخول الى المعلومات والعمل على انظمتها وادارتها

اهداف استراتيجية امن المعلومات

- ١- تعريف المستخدمين والإداريين وبالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات وكذلك لحماية المعلومات بكافة أشكالها سواء في مراحل ادخالها ومعالجتها و تخزينها ونقلها واعادة استرجاعها
- ٢- تحديد الاليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على كل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر
- ٣- بيان الاجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بذلك

منطلقات استراتيجية امن المعلومات

تنطلق استراتيجية امن المعلومات من ((تحديد المخاطر ، اغراض الحماية ، ومواطن الحماية ، وانماط الحماية اللازمة ، واجراء الوقاية من المخاطر))
اجراء الاجابة على الاسئلة الآتية :-
- ماذا اريد ان احمي ؟
- ممن احمي المعلومات ؟
- كيف احمي المعلومات ؟

مناطق امن المعلومات

١- امن الاتصالات :- حماية البيانات عندما يتم تبادلها من

نظام لآخر

٢- امن الحاسب :- حماية المعلومات داخل النظام بكافة انواعه

وانماطه كحماية نظام التشغيل ، برامج التطبيقات ، ادارة

البيانات ، قواعد البيانات بأنواعه المختلفة .

انماط امن البيانات

١- الحماية المادية:- وتشمل كافة الوسائل التي تمنع الوصول الى نظم المعلومات وقواعدها (الاقفال والحواجز والغرف المحصنة)

٢- الحماية الشخصية :- تتعلق بالموظفين العاملين على النظام التقني من حيث وسائل التعريف بهم / تدريب وتأهيل / الوعي بمسائل الامن ومخاطر الاعتداء على المعلومات .

٣- الحماية الادارية :- السيطرة على ادارة نظم المعلومات وقواعدها مثل التحكم بالبرمجيات الاجنبية والخارجية عن المنشأة ووسائل التحقيق بأخلاء الامن والاشراف والمتابعة والرقابة

٤- الحماية المعرفية :- كالسيطرة على اعادة انتاج المعلومات وعلى عملية اتلاف مصادر المعلومات عند القرار بعدم استخدامها

المخاطر التي يمكن ان تواجه نظم المعلومات

- ١- اختراق الانظمة :- دخول شخص غير مفول الى نظام الحاسوب
- ٢- الاعتداء على حق التحويل :- استخدام المفول النظم لغرض ما غير المفول به
- ٣- زراعة نقاط الضعف :- اقتحام من قبل شخص غير مفول به
- ٤- مراقبة الاتصالات :- المراقبة من قبل نقاط الاتصال حتى يتم اختراقها مستقبلا
- ٥- اعتراض الاتصالات :- اعتراض المعطيات المنقولة واجراء التعديلات التي تناسب مع غرض الاعتداء
- ٦- انكار الخدمة :- القيام بنشاط يمنع المستخدم الشرعي من الوصول للخدمة مثل ارسال بريد الكتروني ضخم
- ٧- عدم اقرار القيام بالتصرف :- انكار الارسال طلب الشراء عبر الانترنت من قبل الشخص المرسل وايضا المستلم

نهاية المحاضرة الثالثة