إرشادات تأمين

المعلومات والوثائق الأكاديمية والإدارية

إرشادات لتأمين المعلومات والوثائق الأكاديمية والإدارية والبيانات الخاصة بمنسوبي الجامعة

يمكن حماية المعلومات والحفاظ عليها في اتجاهين رئيسين :

١ – الحماية التقنية للمعلومات :

- عمل نسخة احتياطية عادية ، وحفظ أهم ملفات البيانات من خلال تقنية التخزين عن بعد .
- عمل نسختين احتياطيتين لجميع النظم الفرعية للشبكة المتعلقة بأمن البيانات .
- إمكانية استدعاء مصادر الشبكة عند حدوث خلل بسبب المستخدمين .
- اللجوء للتخزين السحابي لتأمين الملفات المهمة :
- استخدام برامج الجدار الناري fire wall التي تحافظ علي سرية المعلومات .
- تشغيل أنظمة تزويد الطاقة الكهربائية الاحتياطية عند حدوث خلل ما .
- التأكيد من حماية المعلومات من التلف في حال حدوث حريق أو وصول ماء إليها .
- تثبيت البرامج التي تمنع الوصول إلي قواعد البيانات أو أي معلومات لمن ليس لديهم الحق في ذلك .

٢ – <u>الحماية البرمجية للمعلومات</u>

- تستطيع الطرق البرمجية حماية المعلومات بالشكل الآتي :
- إمكانية إعداد كلمة مرور لأجهزة الحاسبات ، مما يتطلب معرفة ألية اختيار كلمة مرور قوية ، والمحافظة عليها بالاستعانة بأدلة الأمان الأساسية الموجودة في أنظمة التشغيل Windows, Linux
- تشفير عملية تخزين البيانات والمعلومات علي أجهزة الحاسبات ، والأجهزة اللوحية ، والأجهزة الذكية .
- تشغيل قفل الشاشة في حال ترك الحاسب ، وذلك متاح في أنظمة Windows, Linux, Mac فهي تحتوي علي اختصارات تمكن إجراء ذلك بسرعة وسهولة .
- استخدام خصائص Bios_الخاصة بنظام الحماية والموجودة في إعددات الكمبيوتر ، بحيث تمنع أولاً الدخول إلي نظام التشغيل من جهاز Usb أو CD.Rom أو DVD ، ثم يتم تحديد كلمة مرور قوية علي Bios نفسه.