# تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية في المملكة العربية السعودية دراسة تطبيقية على جامعة القصيم


**إن التطورات الحديثة في تقنية المعلومات والاتصالات أحدثت تغيرات مستمرة في أساليب العمل و الميادين كافة، والانتشار الواسع للنظم والبرامج وازدياد حجم البيانات التي يجب أن تعالج وتخزن وتسترجع عند الحاجة اليها , بالإضافة إلى رغبة المؤسسات والشركات المختلفة في اقتناء وتطبيق أحدث النظم والبرامج الإلكترونية دافعا أساسيا لاستخدام تقنية المعلومات والاتصالات وأداء العديد من المهام والوظائف المختلفة بصورة أسرع وأدق. وقد أدى هذا التطور السريع المتلاحق فى النظم والبرامج إلى ظهور قضية أمن وخصوصية المعلومات والتى أصبحت تهم كل من المستخدمين ، والمديرين والشركات التي تقدم خدمات المعلومات وكذلك الشركات المطورة للأجهزة والبرمجيات.**

**تمتلك مؤسسات التعليم العالى كميات كبيرة من البيانات لكل من الموظفين الإداريين وأعضاء هيئة التدريس والطلاب ، وتتمثل هذه المعلومات فى المعلومات الشخصية ، سجلات القبول ، الملفات الطبية ، البحوث العلمية. تهدف هذه المؤسسات إلى إدارة وتخزين هذه المعلومات والتحكم فى الوصول إليها بشكل فعال وتوفير الحماية والأمن من المخاطر والهجمات التى قد تتعرض لها المعلومات ، وذلك من خلال وضع السياسات والإجراءات اللازمة لضمان أمن وخصوصية المعلومات والتى تتمثل فى تحسين توافر المعلومات availability و تكاملها integrity و خصوصيتها confidentiality من داخل و خارج المؤسسة. ويهدف هذا البحث إلى تقييم سياسات أمن وخصوصية المعلومات الموضوعة فى المؤسسات التعليمية فى المملكة العربية السعودية ، يبدأ فى الجزء الأول باستعراض الدراسات السابقة فى هذا المجال ، ويتناول الجزء الثاني المفاهيم المختلفة لأمن وخصوصية المعلومات ، مكونات نظام أمن المعلومات ، سياسات أمن المعلومات ، متطلبات أمن المعلومات فى المؤسسات التعليمية ، المعايير الدولية لأمن المعلومات . ويتناول الجزء الأخير من البحث إجراء الدراسة التطبيقية على إحدى المؤسسات التعليمية فى المملكة العربية السعودية وهى جامعة القصيم من خلال إعداد استبيان خاص بتقييم السياسات الأمنية فى الجامعة ، وتم استخدام المنهج الوصفى التحليلى لتحليل إجابات عينة البحث واستخلاص النتائج والتوصيات.**



**إعداد :**

**د. إيناس محمد إبراهيم الشيتى**

**أستاذ مساعد بجامعة القصيم**

**المملكة العربية السعودية**

**enasmes@yahoo.com**


إن عالم اليوم يعتمد على التقنيات الحديثة بشكل كلي ، فالتطور في تقنية الحاسب الآلي والطفرة في تقنية المعلومات والاتصالات وما صاحبهما من انتشار في استخداماتها، جعل العالم في جهاز حاسب واحد،فالحاسب الآلي اصبح من ضرورات الحياة اليومية في أداء جميع الأعمال.

مع بداية التسعينات من القرنالمادي بدأت مرحلة جديدة في تطور المؤسسات التعليمية وذلك باستخدام تقنيات وشبكاتالمعلومات ، واعتمادها عليها في جميع المعاملات التعليمية والإدارية والمالية ، هذا بالإضافة إلى انتشار استخدام شبكةالمعلومات الدولية (الانترنت (Internet، واعتماد هذه المؤسسات عليها، في تنفيذ كافة الأعمال بها.

ومع تطور التقنية وانتشار استخداماتها في جميع مؤسسات التعليم العالى واعتماد هذه المؤسسات عليها بشكل كبير ، قد صاحب هذا التطور ظهور العديد من المخاطر والتهديدات التي تتعرض لها هذه المؤسسات نتيجة استخدام هذهالتقنية ، والتخوف من عدم قدرة هذه المؤسسات في الحفاظ على سرية المعلومات المخزنةبأجهزتها وتكاملها وسلامتها، وعدم تسريبها أو تغييرها أو حذفها نتيجة للأخطار التيتتعرض لها هذه الأجهزة والنظم من قبل المتسللين عبر الشبكات ، الإدخال المتعمد وغير المتعمد للبيانات الخاطئة من داخلالمؤسسة ، الفيروسات . أيضا الأشخاص الذين لهم حق الوصول للنظام قد يسببون تهديدات لنظم المعلومات ، فعلي الرغم من أنهم قد يكونوا مؤتمنين أو عاملين من ذوي النوايا الحسنة فإنهم بسبب التعب أو الإرهاق أو التدريب غير الملائم قد يقترفون أعمال غير متعمدة ، قد تسهم في حذف أو تخريب كميات كبيرة من البيانات الهامة للمنظمة التي يعملون بها.

كل هذه المشاكل جعلت أمن النظم والمعلوماتيتصدر قائمة الاهتمامات في مجال عمل المؤسسات التعليمية. ولهذا يهدف هذا البحث إلياستعراض الدراسات السابقة المرتبطة بموضوع

الدراسة ، مفاهيم أمن وخصوصية المعلومات ، عناصر نظام أمن المعلومات ، التعرف على سياسات أمن المعلومات ، المعايير الدولية لأمن المعلومات . وأخير إجراء الدراسة التطبيقية على إحدى المؤسسات التعليمية فى المملكة العربية السعودية وهى جامعة القصيم ، من خلال إعداد استبيان خاص بتقييم سياسات أمن المعلومات المنفذة في احدى المؤسسات التعليمية (جامعة القصيم) واقتراح السياسات والإجراءاتالتي ينبغي اتخاذها لحماية النظم والمعلوماتبهذه المؤسسات.

وتتمثل مشكلة البحث في الإجابة عنالتساؤلات التالية :

• كيف تستطيع المؤسسات التعليمية حماية أمن وخصوصية المعلومات للمستخدمين من خلال تطبيق السياسات الإدارية والبشرية لأمن وخصوصية المعلومات ؟

• إلى أى مدى يتوافر سياسات الحماية المادية لأمن وخصوصية المعلومات في جامعة القصيم؟

• إلى أى مدى يتوافر سياسات الحماية الفنية لأمن وخصوصية المعلومات في جامعة القصيم ؟

• ما المخاطر والتهديدات الناتجة عن عدم تطبيق سياسات وإجراءات لحماية وتأمين نظم المعلومات في جامعة القصيم ؟

**أهداف البحث :**

تهدف الدراسةإلى الأتي:

• التعرف على سياسات وإجراءات أمن نظم المعلومات فى المؤسسات التعليمية.

• التعرف على إجراءات حماية خصوصية المعلومات الشخصية فى نظام معلومات جامعة القصيم.

• التعرف على المعايير العالمية لأمن وخصوصية المعلومات.

• تقييم السياسات المادية والفنية والإدارية المستخدمة لتأمين نظم المعلومات فى جامعة القصيم.

• تحديد المخاطر المتوقع حدوثها نتيجة استخدام نظام المعلومات بالجامعة القصيم ومدى تكرارها.

• وضع الحلول والتوصيات الكفيلةبتوفير الأمن والحماية لهذه المؤسسات.

**أهمية البحث :**

تتضح أهميةالدراسةمنالعوامل الأتية :

• الاستخداممالمتزايدلنظمالمعلومات فيالمؤسسات التعليمية، الأمر الذى يستدعى توافر السياسات والإجراءات لتأمين وحماية هذه النظم.

• إمكانية الاستفادةمنالبحث فيتقييم سياسات أمن وخصوصية المعلومات فى كافة المؤسسات التعليمية (المدارس ، الكليات والمعاهد المختلفة)

• تقييم المخاطر التى تهدد نظم المعلومات وطرق التغلب عليها.

**فروض البحث :**

يهدف البحث إلى تحقيق الفروض التالية :

١. استخدام سياسات الحماية المادية والفنية والإدارية لأمن المعلومات يؤدى إلى الحفاظ على تكامل نظم المعلومات وتوافرها بشكل دائم فى المؤسسات التعليمية .

٢. ترجع أسباب تكرار حدوث المخاطر التي تهدد نظم المعلومات في المؤسسات التعليمية في المملكة العربية السعودية إلى:

١. عدم توافر متخصصون فى أمن المعلومات فى هذه المؤسسات.

٢. قلة الخبرة و الوعي والتدريب لمستخدمي تقنية المعلومات فى هذه المؤسسات.

٣. ضعف الأدوات والأجهزة والبرامج الرقابية المستخدمة.

حدود البحث :

يتكون مجتمع البحث من موظفي تقنية المعلومات فى جامعة القصيم والمستخدمين من موظفين إداريين وأعضاء هيئة التدريس وطالباتفى الفترة من نوفمبر ٢٠١٢ إلى فبراير ٢٠١٣.

**منهجية البحث :**

سوف يستخدم المنهج الوصفى التحليلي فى تحليل إجابات الاستبيان .

**أولا: عينةالبحث :**

تم اختيار عينة عشوائية من موظفي إدارات تقنية المعلومات فى الجامعة مكونة من ٣٠ مفردة ، عينة ثانية مستخدمى نظام المعلومات في جامعة القصيم مكونة من ٧٠ مفردة (أعضاء هيئة التدريس الإداريين في الأقسام الإدارية المختلفة فى الجامعة) ، وذلك لإجراء الدراسة الميدانية. وقد بلغ عدد أفراد العينة الذين تم إرسال الاستبيانات إليهم بالبريد الإلكتروني أو التسليم المباشر ١٠٠ ، وعدد الذين أجابوا عنها ٧٠ بنسبة ( ٧٠ ٪).

من أجل تحقيق أهداف الدراسة تم تصميم الاستبيان وتوزيعهعلى عينة البحث، وتم اختبار مدى صلاحية الاستبيان من خلال الأتي :-

١- التحكيم: للتأكد من دقة صياغة أسئلة الاستبيان وصحة فقراتها ووضوحها فقد تم عرضها على مجموعة من المحكمين المتخصصين في مجال تكنولوجيا المعلوماتمن لهم خبرة في مجال نظم المعلومات لأجل الاسترشاد بآرائهم حول الفقرات التي تضمنها الاستبيان. وقد اخذ بآراء وتعديلات المحكمين ، حيث تم حذف بعض الفقرات، كما تم تعديل فقرات أخرى، حتى تم التوصل للصورة النهائية للاستبيان.

٢- الصدق والثبات : يهدف اختبار درجة مصداقية البيانات ومدى توافر الثبات والاتساق الداخلي بين الإجابات على أسئلة الاستبيان فقد تم احتساب معامل المصداقية ألفا كرونباخ Cronbacks Alpha، وبلغ (٠,٨٩) مما يشير إلى توافر درجة عالية من المصداقية والثبات الداخلي للإجابات يمكن الاعتماد عليها في اختبار الفروض ، وتعتبر القيمة المقبولة لمعامل ألفا ٦٠٪ فأكثر

٣- استخدام الاحصاء الوصفي البسيط المتمثل في التكرارات والنسب المئوية للإجابة على أسئلة الدراسة ، وأدخلت بيانات الدراسة على الحاسب الآلي وتمت معالجة البيانات واستخراج التكرارات منها والنسب المئوية والمتوسطات الحسابية والانحراف المعيارى عن طريق باستخدام البرنامجالإحصائي SPSS.

تتضمن استمارة الاستبيان أربع محاور وهى على النحو التالي:

**١. المحور الأول : سياسات الحماية الإدارية لنظام المعلومات بالجامعة**

**٢. المحور الثاني : سياسات الحماية المادية لنظام المعلومات بالجامعة**

**٣. المحور الثالث : سياسات الحماية الفنية لنظام المعلومات بالجامعة**

**٤. المحور الرابع : تحديد المخاطر التى يتعرض لها نظام المعلومات بالجامعة ومدى تكرار حدوثها**

## ٢. الدراسات السابقة:

يعتبر موضوع أهمية سياسات أمن وخصوصية نظم المعلومات من المواضيع الهامة والحديثة نسبيا، حيث إنه من خلال مراجعة الدراسات والأبحاث السابقة والمتعلقة بهذا الموضوع نجد أن هناك ندرة في العالم العربي حول هذا الموضوع ( خاصة فى المؤسسات التعليمية) ، وهذا يدل على الحداثة النسبية لهذا الموضوع رغم أهميته الحيوية لكثير من المؤسسات والشركات المختلفة. ومن اهم الدراسات في هذا المجال التالي :

١- دراسة ( سلمان القحطاني ٢٠٠٣) ، بعنوان» أمن المعلومات في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة « ، عرضت الدارسة رؤية متعددة الجوانب للشبكات والاتصالات اللاسلكية الرقمية في الألفية الثالثة. عرض القسم الأول لمحة مختصرة عن التطور التقني لعالم الشبكات النقالة اللاسلكية وكيف تطورت الشبكات والخدمات وأمن الشبكات المحمولة والبعد الأمني لهذا التطور. وفي القسم الثاني ناقشت الورقة أمن المعلومات والعمليات الإلكترونية من حيث المخاطر والحلول. وقد تم توضيح مفهوم وضع السياسات الأمنية الجيدة. وتوصل البحث إلى ضروري بناء السياسات الأمنية القوية التي تضمن اتباع المؤسسة لوسائل الأمان الجيد ، ضرورة تضافر الجهود الإدارية والتي تعتبر هي العنصر الحيوي لتطبيق السياسات الأمنية الناجحة .

٢- دراسة (إريك جوهانسون و بونتوس جونسون، ٢٠٠٥) بعنوان « Assessment of Enterprise Information Security - An Architecture Theory Diagram Definition « وتهدف الدراسة الى تقديم طريقة كمية واضحة وشفافة لتقييم أمن معلومات المؤسسة. تعتمد الطريقة على توحيد أبرز المصادر على الموضوع والنتائج فى تقدير كمى واحد لمستوى أمن معلومات المؤسسة. تم التطبيق على شركة كهرباء أوربية (استوكهوم السويد) . تركز هذه الورقة على تطوير طريقة لتقييم أمن معلومات المؤسسات. ويتمثل الهدف العام للبحث فى تقديم وظيفة لمدير نظام المعلومات CIO بأدوات وأساليب لتخطيط واتخاذ القرارات بشأن نظام المعلومات. المعلومات وعمليات نظم المعلومات المؤسسة هى من الأصول الهامة ، لذلك يعتبر أمن المعلومات (الحفاظ على السرية ، سلامة والتوافر) ذو أهمية متزايدة لنظام الجودة . يعتبر الحفاظ على أمن المعلومات أمر أساسيا لتحقيق التنافسية ، التدفق النقدى والربحية والصفة القانونية والتجارية.

٣- دراسة (فكتورنو كيس، ٢٠٠٦) وهى بعنوان « AN INFORMATION SECURITY RISK ASSESSMENT MODEL FOR PUBLIC AND UNIVERSITY ADMINISTRATORS» ، وتهدف الدراسة إلى التعرف على أدبيات أمن المعلومات ، مكونات نظام أمن المعلومات ، التشريعات واللوائح والقوانين الخاصة بأمن المعلومات. وأخيرا إجراء دراسة استطلاعية لتقييم سياسات وإجراءات أمن المعلومات فى الجامعات والمؤسسات الحكومية. تضمن الاطار المقترح تصنيف البيانات في النظام ، تحديد الضوابط الإدارية ، الضوابط التشغيلية والضوابط الفنية واللازمة لتأمين نظم المعلومات في هذه المؤسسات. توصلت الدراسة إلى وضع إطار عمل مقترح لتقييم مخاطر أمن المعلومات ، يشمل تحديد الاجراءات والسياسات اللازمة لتأمين وحماية سرية وخصوصية البيانات فى المؤسسات الحكومية والجامعات الحكومية.

٤- دراسة (نور الدين حامد ٢٠٠٧) بعنوان « أمن نظم ومعلومات المصارفوحمايتها بإشارة خاصة للواقع السوداني ، هدفت الدراسة إلى عرض المخاطر والمهددات التي تواجهاستخدامات التقنية بصورة عامة وبالبنوك التجارية السودانية بصفة خاصة وذلك في ظل استخدام الشبكاتالخاصة بكل بنك، أو استخدامات الشبكات القومية لتبادل الخدمات بينها، وأيضاً في ظلاستخدامات الانترنت حيث تتنوع مصادر المخاطر بنوع الشبكات المستخدمة . وتوصلت الدراسة إلى توصيات من أهمها ضرورة سد الثغرات بالبنوك السودانية لتفادي أسبابالسرقات وللأخذ بأسباب الحماية لمنع جرائم الحاسوب بصورة شاملة ، ضرورة وضع طرق للوقاية من المهددات والمخاطر الأمنية ، وسائل اكتشاف الاختراقات ، وطريقةإيقافها ثم معالجة آثارها عند حدوثها.

٥- دراسة (ميشيل جونسن ٢٠٠٨) و هي بعنوان «An Evaluation of Privacy and Security Issues at a Small University»» . وتهدف هذه الدراسة إلى إجراء تقييم للإجراءات والسياسات الأمنية التي تنفذ فى إحدى الجامعات الصغيرة بهولندا ، وأيضا إجراء تقييم للمخاطر الأمنية التى تواجه الجامعة وذلك لتحديد الثغرات ونقاط الضعف فى نظام الأمن بالجامعة. كما تضمنت الدراسة وضع توصيات عن كيفية استخدام وتطبيق اجراءات وسياسات متطورة لضمان أمن وخصوصية المعلومات للمستخدمين.

٦- هدفت دراسة (باهلير ٢٠٠٨) وهى بعنوان ««Information Security Assessment and Reporting: Distributed Defense» ، تهدف هذه الدراسة إلى اقتراح خطة لتقييم أمن المعلومات فى المؤسسات التعليمية طبقا لثلاث مستويات من المؤسسات التعليمية (مؤسسات صغيرة ، مؤسسات متوسطة ومؤسسات كبيرة ) . تحديد المقاييس المقترحة لتقييم الأدوار والمسئوليات الرئيسية لأمن المعلومات. تساعد المقاييس المقترحة للتقييم على تحديد أولويات عمليات تقييم أمن المعلومات ، تقليل وقت الاستجابة لمعالجة الحوادث الأمنية. يتضمن البحث أيضا تحديد مسؤوليات موظفى تقنية المعلومات تجاه أمن نظام المعلومات فى المؤسسة ، حيث يتم الابلاغ الفورى عن الحوادث للمسئول أو مالك هذه المعلومات ويسلم هذا التقرير الى الشخص المسئول مباشرة .توصلت الدراسة إلى خفض زمن الاستجابة للحوادث الامنية ، تحديد الادوار والمسئوليات للمسئولين عن أمن المعلومات فى المؤسسة ، اصدار التقارير بالاستثناءات الامنية التى تحدث فور حدوث هذه الاستثناءات بدون الانتظار الى طلب جهات محددة وقد ساعدت هذه التقارير فى سرعة معالجة الاستثناءات ونقاط الضعف التى ظهرت فى نظام المعلومات.

٧- دراسة (عصام البحيصي وحرية الشريف ، ٢٠٠٨) ، بعنوان «مخاطر نظم المعلومات المحاسبية الالكترونية دراسة تطبيقية على المصارف العاملة في قطاع غزة « تهدف إلى التعرف على المخاطر التى تهدد نظم المعلومات المحاسبية الإلكترونية فى بيئة المصارف العاملة في قطاع غزة ومعدلات تكرارها, وأسباب حدوثها. التعرف على اجراءات الحماية التي تتبعها تلك المصارف للحد من المخاطر التي تهدد نظم معلومات المحاسبية الإلكترونية. وتوصلت هذه الدراسة إلى توصيات من أهمها ضرورة دعم الادارة العليا فى المصارف أمن المعلومات لديها وأن تعمل على إنشاء قسم خاص بتكنولوجيا المعلومات في كافة المصارف وتوفير كادر متخصص في تكنولوجيا المعلومات بحيث يكون له مندوبين في الفروع ذوي خبرة وكفاءة عالية لأجل العمل على حماية أمن نظم المعلومات المحاسبية لدى المصارف.

٨- دراسة (فادي عمروش، ٢٠١٠) ، بعنوان «إعداد السياسات الأمنية فى الشبكات اللاسلكية» ، تتناول الدراسة أسس أمن المعلومات، و أسس كتابة السياسة الأمنية ومكوناتها، وقد اقترحت الدراسةكيفية تطبيق المفاهيم السابقة فى الشبكات اللاسلكية عن طريق استخدام طرق المسح survey للمواقع اللاسلكية، شرح المفاهيم التقنية لكيفية تحقيق أمن المعلومات في الشبكات اللاسلكية، عرض المخاطر الأمنية العشر الأكثر شيوعاً في الشبكات اللاسلكية مع مجموعةً من المقترحات لكل منها.

٣- مفاهيم أمن وخصوصية المعلومات:

يعرف أمن المعلومات ، من زاوية اكاديمية ، بأنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها . ومن زاوية تقنية ، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية . ومن زاوية قانونية ، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها ( جرائم الكمبيوتر والإنترنت).

ويعرف أمن المعلومات أيضا بأنه « العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الادوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية « .

ويعرف أمن المعلومات بأنه "حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات ، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة وذلك في جميع مراحل تواجد المعلومة (التخزين – النقل – المعالجة)" .

وتتمثل أهمية أمن المعلومات في النقاط التالية :

١. القطاعات الأمنية والعسكرية والاقتصادية تعتمد على صحة ودقة المعلومات.

٢. حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق تغطي المخاطر التي يمكن أن تظهر عند التعامل مع الأطراف الأخرى.

٣. الحاجة المتزايدة لإنشاء بيئة إلكترونية آمنة تخدم القطاعين الخاص والعام.

٤. النمو السريع في استخدامات التطبيقات الإلكترونية والتي تتطلب بيئة آمنة.

٥. الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية وذلك من أجل استمرارية الأعمال التجارية.

٦. مع تطور التقنية المعلوماتية وازدهارها توفرت فرصاً للإجرام الإلكتروني

وتتضمن مفاهيم خصوصية المعلومات عدد من الأبعاد، وهي:

١- خصوصية الشخص (Privacyperson):تختص بسلامة

الفرد في جسده، مثل قضايا التطعيم أو نقل الدم دون الحصول على موافقة الشخص المعني، أو الإجبار على تقديم عينات من سوائل الجسد أو أنسجته.

١- خصوصية المعلومات Information Privacy ، والتي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية.

٢- خصوصية الاتصالات Telecommunication Privacy، والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الالكتروني والاتصالات الخلوية وغيرها من الاتصالات .

٣- الخصوصية الاقليمية ( الاقليم المكاني ) والتي تتعلق بالقواعد المنظمة للدخول الى المنازل وبيئة العمل أو الاماكن العامة والتي تتضمن التفتيش والرقابة الالكترونية والتوثيق من بطاقات الهوية .

**٤- عناصر نظام أمن المعلومات:**

يوضح الشكل التالي مكونات نظام أمن المعلومات

**شكل رقم (١)**
**مكونات نظام أمن المعلومات**

يتضح من الشكل السابق أن مكونات نظام أمن المعلوماتتتمثل في التالي :

أولاً: سرية المعلومات Data Confidentiality

يقصد بسرية المعلومات الإجراءات والتدابير اللازمة لمنع إطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها: المعلومات الشخصية للأفراد، الميزانية المالية للشركات قبل إعلانها، المعلومات والبيانات العسكرية الخاصة بالجيوش والمواقع العسكرية في البلاد.

**ثانياً: سلامة المعلومات Data Integrity**

سلامة المعلومات هي الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ. عندما يقوم شخص بقصد أو بغير قصد انتهاك سلامة أو الإضرار أو حذف ملفات البيانات الهامة وهو غير مخول بذلك فهذه انتهاك لسلامة البيانات ، وعندما يصيب فيروس كمبيوتر ويقوم بتعديل بيانات أو اتلافها فهذا انتهاك سلامة بيانات ، فمثلا عندما يكون الموظف قادرا على تعديل راتبه في قاعدة البيانات والمرتبات.

**ثالثاً: ضمان الوصول إلى المعلومات Availability**

يجب أن تكون المعلومات متوفرة عند الحاجة إليها ، وهذا يعني أن الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات ، والضوابط الأمنية المستخدمة لحمايته ، وقنوات الاتصال المستخدمة للوصول إلى ذلك يجب أن يعمل بشكل صحيح. توافر نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات ، ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات ومنع انقطاع الخدمة بسبب انقطاع التيار الكهربائي ، أو تعطل الأجهزة ، او نظام الترقيات والتحديث.

٥- سياسات أمن المعلومات:

السياسة الأمنية هي مجموعة قوانين أمنية تسيطر على نظام المعلومات و تزوده بمستوى حماية موثوق به ، وهذه السياسات يجب أن تُوجه الإدارة وسبل الحماية والمصادر المرتبطة بالمعلومات ونظام المعلومات.

تتمثل طرق إعداد سياسات و إجراءات أمن المعلومات في الخطوات التالية :

- تحديد جميع الممتلكات المطلوب حمايتها.
- تحديد جميع الثغرات و المخاطر.
- تقرير أي المعايير التي يمكنها حماية الممتلكات.
- نقل النتائج و الاكتشافات إلى الأقسام المعنية.
- مراقبة ومراجعة العملية باستمرار من أجل التطوير.

وتشمل السياسات الأمنية التي يتناولها البحث فى السياسات الحماية الإدارية ، سياسات تحديد الهوية الآلية ، سياسات الحماية الفنية وسياسات تقدير المخاطر كما موضح فى الجزء التطبيقي للبحث.

سمات سياسة أمن المعلومات الجيد :

- يجب أن تكون قابلة للتطبيقImplementable من خلال الإجراءات والتوجيهات الإدارية
- يجب تدعيمها بالأدوات الأمنية والقوانين والمراسيم الإدارية
- يجب تحديد المسؤوليات على كل مستويات الهيكل التنظيمي
- يجب أن تكون موزعةDistributed على كل وحدات

المنظمة

- يجب أن تكون موثقةDocumented (للمرجعية)

- يجب أن تكون مرنة وفعالة لأطول فترة ممكنة وحتى تتحقق هذه الخاصية فلابد من أن تكون مستقلة Independent عن أي Hardware أو Software لان هذين العنصرين يتغيران بشكل سريع.

**تتمثل أنواع سياسات أمن المعلومات فى التالي :**

١- سياسات الحماية الإدارية : ويقصد بها سيطرة إدارة تقنية المعلومات على ادارة نظم المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية او الاجنبية عن المنشأة ، ومسائل التحقيق باخلالات الأمن ، ومسائل الاشراف والمتابعة لأنشطة الرقابة اضافة الى القيام بانشطة الرقابة ضمن المستويات العليا ومن ضمنها مسائل مراقبة توقيعالموظفين علىالالتزامبكافةالسياس اتوالإجراءاتوالمعاييروالإرشاداتالخاصة بأمن المعلومات ، التأكد من حصول الموظفين بصورةمنتظمةبالتحديثاتالتيتتعمل ىالسياساتوالإجراءاتويكونلهاصلة بمسئولياتهمالوظيفية تجاه أمن المعلومات ، سحب حقوقوصلاحيات استخدام الموظف لموارد وأجهزة تقنية المعلومات عند إنهاءخدمته وإقامة الدورات التدريبية للموظفين الجدد حول سياسات وإجراءات امن المعلومات فى الجامعة.

٢- سياسات تحديد الهوية الآلية لأمن المعلومات : وتشمل كافة الوسائل التي تمنع الوصول الى نظم المعلومات وقواعدها ، مثل المقاييس الحيوية ، أدوات تكنولوجيا متقدمة وأنظمة الحماية البيئية التي تمنع الوصول الى الاجهزة الحساسة .

٣- سياسات الحماية الفنية: وهى تتعلق بالوسائل الخاصة بحماية الأجهزة وبرامج نظم التشغيل وبرامج التطبيقات وشبكات الاتصال ، مثل سياسات كلمات المرور ، سياسات برامج الحماية والجدران النارية، سياسات التحكم بالوصول ، سياسات إدارة أصول المعلومات ، تشفير البيانات ، سياسات النسخ الاحتياطي ، سياسات إدارة وصول المستخدمين ، وسياسات التعامل مع البريد الالكتروني.

٤- سياسات تقدير المخاطر: وتشمل تقدير المخاطر والتهديدات التى يتعرض لها نظام معلومات الجامعة نتيجة قلة الخبرة و الوعي والتدريب لمستخدمى نظام المعلومات بالجامعة ، وتقدير المخاطر والتهديدات التى يتعرض لها نظام معلومات الجامعة نتيجة لعدم توافر أو ضعف الأدوات والأجهزة والبرامج الرقابية المستخدمة.

٦- المعايير الدولية لأمن المعلومات:

تشمل المعايير الدولية لأمن المعلومات في المعايير التالية :

اولا : معيار ISO/IEC ٢٧٠٠٢

هذا المعيار هو أحد معايير المنظمة العالمية للمعايير International Organization for Standardization (ISO)) , وهي معنية بإعداد معايير لمختلف المجالات ومن ضمنها مجال تقنية المعلومات. وقد طور هذا المعيار بالتعاون مع منظمة الكهروتقنية الدولية International Electro technical Commission واختصارا IEC. وهذا المعيار جزء من مجموعة من المعايير تسمى عائلة ISO/IEC ٢٧٠٠٠ أو يطلق عليها معايير تقنية المعلومات – تقنيات الأمن – كود الممارسة الأفضل لإدارة أمن المعلومات.

ويهدف هذا المعيار إلى إيجاد خطط ومبادئ أساسية لإنشاء وتنفيذ وصيانة وتطوير نظم إدارة أمن المعلومات في المنظمة. وينقسم هذا المعيار إلى مجموعة من الأجزاء الفرعية يجب على المنظمة الراغبة في الحصول على هذا المعيار تطبيقها ، وهي :

- تقييم المخاطر.
- أنواع السياسات الأمنية المطبقة.
- الهيكل التنظيمي لأمن المعلومات.
- إدارة الأصول.
- إدارة أمن الموارد البشرية.
- أمن المرافق والبيئة المحيطة.
- إدارة العمليات والاتصالات.
- التحكم في الوصول.
- إدارة الحوادث العرضية لتقنية المعلومات.
- إدارة استمرارية الخدمة.
- إدارة التوافقية مع الأنظمة والتشريعات.

**ثانيا : معيار COBIT**

تم تطوير وتصميم معيار COBIT عام ١٩٩٥م من قبل معهد حوكمة تقنية المعلومات IT Governance Institute وهو الآن في نسخته الرابعة [٥]. وكلمة COBIT اختصار لـ ضوابط المعلومات والتقنيات المتعلقة بها Control Objectives for Information and related Technology.و هذا المعيار عبارة عن هيكلية تهدف إلى ربط تقنية المعلومات بأهداف ومتطلبات أعمال المنظمة عن طريق إيجاد نموذج عام لأنشطة تقنية المعلومات في المنظمة مما يؤدي إلى التعرف على موارد تقنية المعلومات المهمة وتعزيزها و ربط ذلك كله بضوابط تحكم هذه العمليات والأنشطة والموارد. ويركز هذا المعيار على أربع أجزاء رئيسية هي:

- التخطيط والتنظيم لتقنية المعلومات.
- الاستحواذ وتطبيق تقنية المعلومات.
- توصيل ودعم تقنية المعلومات.
- المراقبة والمتابعة.

**ثالثا : معيار ITIL**

معيار ITILاختصار لـ Information Technology Infrastructure Library

أو مكتبة البنية الأساسية لتقنية المعلومات و يصدر عن مكتب التجارية الحكومية البريطاني Office of Government Commerce (OGC). وهذا المعيار عبارة عن مجموعة من المفاهيم والسياسات لإدارة وتطوير خدمات تقنية المعلومات والعمليات المتعلقة بها. وفي هذا المعيار هناك وصف تفصيلي للمهام والعمليات المتعلقة بتقنية المعلومات مع قوائم مرجعية متكاملة بحيث تستطيع أي منظمة تستخدم تقنية المعلومات موائمته حسب احتياجاتها.وفي هذا المعيار يجب أن تتوافق إدارة أمن المعلومات في المنظمة مع ما يلي:

- السياسات الحالية و المستقبلية لأمن إدارة الأعمال.
- متطلبات الأمن.
- المتطلبات التشريعية والقانونية.
- إدارة تقييم مخاطر الأعمال وتقنية المعلومات.

**رابعا : المعيار العالمي لأمن المعلومات (ISO١٧٧٩٩)**

يحتوي على أفضل الممارسات في المراقبة وفي السياسات والضوابط التي تتبع في إدارة أمن المعلومات في المجالات التالية:

١- تقييم المخاطر : تحديد المخاطر التي تتعرض لها المنظمة ، مثل المخاطر التي قد تؤثر على معلومات المنظمة المهمة أو على موظفيها أو ممتلكاتها, ويكون هذا التقييم بناءً على شيئين رئيسيين وهما :

١. تحديد مدى تأثير هذه المخاطر على المنظمة: حيث أن هذه المخاطر من المؤكد أن يكون لها تأثير سلبي على المنظمة لكن هذا التأثير يختلف من خطر لآخر بناءً على تكلفة الخسائر التي يسببها للمنظمة.

٢. احتمالية حدوث هذه المخاطر من خلال تحديد احتمال حدوث هذا الخطر في المنظمة فإذا كانت نسبة حدوث هذا الخطر قليل جداً يتم تجاهل هذا الخطر.

٢- السياسات الأمنية: هي مجموعة من المعايير والأنظمة التي تقوم بتطبيقها المنظمة لحماية معلوماتها ومرافقها من خلال فرض قوانين وقواعد تلزم المنظمة موظفيها على إتباعها, مثل أن تفرض المنظمة على موظفيها أن يكون الرقم السري لحسابه على شبكة المنظمة لا يقل عن ٨ أحرف أو أن قاعدة بيانات المنظمة لا يسمح الوصول لها إلا عن طريق موظفين معينين. فالهدف منها هو توفير الدعم والتوجيه في إدارة أمن المعلومات.

٧- نتائج تحليل الدراسة الميدانية لنظام معلومات جامعة القصيم:

يتناول هذا الجزء نتائج التحليل الاحصائي للدراسة الميدانية والتي تم الحصول عليها عبر تحليل البيانات التي شملها الاستبيان لنظام معلومات جامعة القصيم ، وسوف يكون العرض وفقا مجموعة المحاور الرئيسية المذكورة سابقا. تتمثل عينة البحث في موظفي تقنية المعلومات فى جامعة القصيم ومستخدمي تقنية المعلومات من أعضاء هيئة التدريس وطالبات الجامعة. تتضمن البيانات المجمعة عن الاسم ، المؤهل الدراسي ، الوظيفة ، جهة العمل ، الخبرة ومدى توافر سياسات الحماية المادية والفنية والإدارية لأمن المعلومات. تم ترميز المتغيرات لإدخالها إلى برنامج التحليل الاحصائي SPSS طبقا للآتي :

أولا : خصائص عينة الدراسة طبقا لمتغيرات المؤهل الدراسي ، المسمى الوظيفي ، جهة العمل وسنوات الخبرة. وتم تفريغ البيانات في برنامج SPSS الإحصائي وفقا للتصنيف التالي :

**(١) تصنيف المؤهل العلمي**

| المؤهل العلمي | ثانوية عامة | بكالوريوس | ماجستير | دكتوراه |
|---|---|---|---|---|
| التصنيف | 1 | 2 | 3 | 4 |

ويوضح الجدول التالي خصائص عينة الدراسة طبقا للمؤهل الدراسي :

**جدول رقم (١)**
**خصائص عينة الدراسة طبقا للمؤهل الدراسي**

| المؤهل العلمي | التكرار | النسبة % |
|---|---|---|
| ثانويةعامة | 34 | 48.6 |
| بكالوريوس | 22 | 31.4 |
| ماجستير | 4 | 5.7 |
| دكتوراه | 10 | 14.3 |
| الإجمالي | 70 | 100.0 |

يتضح من الجدول السابق أن أعلى نسبة التى أجابت على الاستبيان هم طالبات جامعة القصيم بنسبة (٤٨,٦ ٪) وهم من مستخدمى تقنية المعلومات بالجامعة ، يليهم نسبة الحاصلين على البكالوريوس وهم المسئولين عن إدارة وصيانة ومتابعة شبكات المعلومات فى الجامعة وكانت نسبتهم (٣١,٤ ٪) ، وأقلهم نسبة فى الاجابة على الاستبيان هم المستخدمين من أعضاء هيئة التدريس الحاصلين على درجة الماجستير والدكتوراه ، وذلك لضعف خبرة أعضاء هيئة التدريس بسياسات وإجراءات أمن نظم المعلومات.

**(١) تصنيف المسمى الوظيفي**

| الوظيفة | مدير شبكة المعلومات | مسئول أمن المعلومات | مسئول صيانة تقنية المعلومات | مستخدمين |
|---|---|---|---|---|
| التصنيف | 1 | 2 | 3 | 4 |

ويوضح الجدول التالى خصائص عينة الدراسة طبقا للمسمي الوظيفي :

**جدول رقم (٢)**
**خصائص عينة الدراسة طبقا للمسمي الوظيفي**

| المسمىالوظيفي | التكرار | النسبة % |
|---|---|---|
| مدير شبكة المعلومات | 2 | 2.9 |
| مشرفى تقنية المعلومات | 8 | 11.4 |
| مسئول صيانة الأجهزة والشبكات | 12 | 17.1 |
| مسئول أمن المعلومات | 0 | 0 |
| مستخدمين | 48 | 68.6 |
| الإجمالي | 70 | 100 |

يتضح من الجدول السابق أن نسبة الأفراد المستخدمين لتقنية المعلومات فى جامعة القصيم أعلى نسبة فى عينة الدراسة حيث بلغت (٤٨ ٪) ، وذلك لأن عدد المتخصصين فى تقنية المعلومات قليل وأن إدارات تقنية المعلومات حديثة الإنشاء وتشتمل على عدد قليل من المتخصصين فى إدارة وصيانة الشبكات ، ولا تشتمل عمادة تقنية المعلومات على أى متخصصين فى أمن المعلومات.

**(١) تصنيف جهة العمل**

| جهة العمل | عمادة تقنية المعلومات | الكليات العلمية | الكلية الادبية والعلوم الانسانية |
|---|---|---|---|
| التصنيف | 1 | 2 | 3 |

ويوضح الجدول التالي عن توزيع عينة الدراسة طبقا لجهات العمل فى جامعة القصيم.

**جدول رقم (٣)**
**خصائص عينة الدراسة طبقا لجهة العمل**

| جهة العمل | التكرار | النسبة |
|---|---|---|
| عمادة تقنية المعلومات | 12 | 17.1 |
| الكليات العلمية | 10 | 14.3 |
| الكلية الأدبية والعلوم الانسانية | 48 | 68.6 |
| الإجمالى | 70 | 100.0 |

يتضح من الجدول السابق أن نسبة عينة الدراسة المستجيبة للإجابة على الاستبيان كانت فى الكليات الأدبية والعلوم الإنسانية (٦٨,٦ ٪) ، يليهم نسبة الأفراد العاملين فى عمادة تقنية المعلومات بنسبة (١٧,١ ٪) ، وكانت نسبة الأفراد المستجيبين للإجابة على الاستبيان من الكليات العلمية (١٠ ٪) .

(١) الخبرة

| الخبرة | اقل من 5 سنوات | من 5-10 سنوات | اكثر من 10 سنوات |
|---|---|---|---|
| التصنيف | 1 | 2 | 3 |

ويوضح الجدول التالي خصائص عينة الدراسة المستجيبة طبقا لسنوات الخبرة فى العمل :

**جدول رقم (٤)**
**خصائص عينة الدراسة طبقا لسنوات الخبرة**

| الخبرة | التكرار | النسبة % |
|---|---|---|
| اقلمن5سنوات | 18 | 25.7 |
| 5 - 10سنوات | 45 | 64.3 |
| أكثر من 10 سنوات | 7 | 10 |
| الإجمالي | 70 | 100 |

يتضح من الجدول السابق أن خبرة عينة الدراسة مناسبة ، حيث أن أعلى نسبة (٦٤,٣ ٪) كانت للأفراد المستجيبين للإجابة على الاستبيان الذى لديهم خبرة من خمس إلى عشر سنوات ، تليها نسبة الأفراد الذى لديهم خبرة أقل من خمس سنوات وهى (٢٥,٧ ٪) ، أقل نسبة للأفراد الذى لديهم خبرة أكثر من عشر سنوات.

ثانيا : نتائج تحليل الدراسة الميدانية لسياسات أمن المعلومات فى جامعة القصيم

| التصنيف | موافق بشدة | موافق | محايد | غير موافق | غير موافق بشدة |
|---|---|---|---|---|---|
| الدرجة | 5 | 4 | 3 | 2 | 1 |

وتم وضع أسماء لمتغيرات أسئلة الدراسة مثل q١ ,q٢ ,q٣ ..... q٧٠ لإدخالها فى برنامج SPSS الإحصائي لاستخراج التكرارات والنسبة المئوية والمتوسط الحسابي والانحراف المعيارى.

كلما اقتربت النتيجة من الدرجة (٥)؛ ازدادت شدة الموافقة على العبارة في حين تزداد شدة المعارضة كلما اقتربت النتيجة من الدرجة (١) ، وإذا كانت الإجابة هى الدرجة (٣)؛ فإن ذلك يكون في الاتجاه المحايد. واستخدم هذا المقياس في المجالات الأول و الثانية و الثالثة ، أما في المجال الرابعفقد كان المقياس المستخدم هو :

| التصنيف | مرة على الأقل يوميا | مرة على الأقل أسبوعيا | مرة على الأقل شهريا | مرة على الأقل سنويا | لا يحدث مخاطر أبدا |
|---|---|---|---|---|---|
| الدرجة | 5 | 4 | 3 | 2 | 1 |

كلما اقتربت الإجابة من الدرجة (٥)؛ فان عدد مرات حدوث المخاطر ينخفض الى درجة انعدام حدوث المخاطر ، ويزداد عدد مرات حدوث المخاطر كلما كانت الإجابة (١) ، أما إذا كانت الإجابة هى (٣)؛ فإن ذلك يعني ان عدد مرات حدوث مخاطر نظم المعلومات في الجامعة متوسطا نسبيا.

(١) الإجابات على أسئلة مدى توافر سياسات الحماية الإدارية فى نظام المعلومات بجامعة القصيم.

يوضح الجدول التالي نتائج التحليل الإحصائي لمتغيرات الدراسة والتي تشمل المتوسطات الحسابية والانحراف المعيارى للأسئلة الخاصة بتوافر السياسات الإدارية فى نظام معلومات جامعة القصيم :

**جدول رقم (٥)**
**نتائج التحليل الإحصائي لتوافر السياسات الإدارية فى نظام معلومات جامعة القصيم**

| الرقم | بنود التقييم | الوسط الحسابى | الانحراف المعيارى | درجة الموافقة |
|---|---|---|---|---|
| 1 | يوجد إدارة خاصة بأمن المعلومات فى الجامعة | 1.6143 | 0,51900 | 2 |
| 2 | توافر موظفون متخصصون بأمن المعلوماتوحمايتها | 1.8000 | 0,55430 | 2 |
| 3 | توافر سياسات وإجراءات ومواصفات قياسية لأمنالمعلومات | 2.8143 | 0,95239 | 3 |
| 4 | اهتمام الإدارة العليا بأمنالمعلومات كبير جدا | 2.9714 | 0,86764 | 3 |
| 5 | توقيعالموظفين علىالالتزامبكافةالسياساتوالإجراءاتوالمعاييروالإرشاداتالخاصة بأمن المعلومات | 2.1429 | 0,66563 | 2 |
| 6 | التأكد من حصول الموظفين بصورةمنتظمةبالتحديثاتالتيتتمعلىالسياساتوالإجراءاتويكونلها صلة بمسئولياتهمالوظيفية تجاه أمن المعلومات | 2.6143 | 0,88944 | 3 |
| 7 | توافر دورات تدريبية للموظفين الجدد حول سياسات وإجراءات امن المعلومات فى الجامعة | 1.8286 | 0,48068 | 2 |
| 8 | سحب حقوقوصلاحيات استخدام الموظف لموارد وأجهزة تقنية المعلومات عند إنهاءخدمته | 3.9000 | 0,78297 | 4 |
| | **إجمالى سياسات الحماية الإدارية لأمن المعلومات** | 2.4607 | 0,22526 | 2 |

يتضح من الجدول السابق ما يلى :

• كل عينة الدراسة تؤكد على عدم توافر إدارة خاصة لأمن المعلومات فى الجامعة وأيضا عدم توافر موظفون متخصصون فى أمن المعلومات ، ضرورة توقيع الموظفين على الالتزام بسياسات أمن المعلومات المتوافرة فى الجامعة ، وهذا يرجع لحداثة إنشاء إدارات تقنية المعلومات فى الكليات المختلفة فى الجامعة وعدم توافر كوادر مدربة وحاصلة على شهادات تخصصية فى أمن المعلومات ، وقد بلغ المتوسط الكلى لإجابات عينة الدراسة لهذه الأسئلة من (١,٦١٤٣) إلى (٢,١٤٢٩) . وهذا مؤشر على عدم توافر إدارة ومتخصصون فى أمن المعلومات وعدم إعطاء الموظفين الحاليين فى عمادة تقنية المعلومات دورات تدريبية متخصصة فى أمن المعلومات.

• إجابات غالبية الدراسة محايدة بالنسبة لبند أهمية توافر سياسات وإجراءات لأمن المعلومات فى الجامعة حيث بلغ المتوسط الكلي للإجابات على البند (٢,٨١٤٣) ، بالنسبة لبند اهتمام الإدارة العليا فى الجامعة بتوافر هذه السياسات والإجراءات فى نظام المعلومات بالجامعة كانت الإجابات عالية وبمتوسط حسابى مقداره (٢,٩٧١٤) ، وأيضا بند حصول الموظفين على التحديثات التى تتم على السياسات والإجراءات الخاصة بنظام المعلومات عالية وكانت بمتوسط حسابى (٢,٦١٤٣)، وهذا يدل على اهتمام الإدارة بأمن وخصوصية المعلومات على الرغم من عدم توافر إدارات خاصة بأمن المعلومات وموظفين متخصصين فى أمن المعلومات.

• موافقة غالبية عينة الدراسة على توافر سياسات خاصة بسحب حقوق وصلاحيات استخدام نظام المعلومات فى الجامعة للموظفين الذين تم إنهاء خدمتهم ،وقد بلغ المتوسط الكلي ٣,٩٠٠٠ ، وهذا يدل على حرص إدارة تقنية المعلومات على غلق حسابات الموظفين فور إنهاء خدمتهم وذلك لحماية المعلومات من الإدخال غير المقصود أو تسريب المعلومات من الجامعة.

(٢) الإجابات على أسئلة مدى توافر سياسات الهوية الآلية لأمن المعلومات فى نظام المعلومات بجامعة القصيم.يوضح الجدول التالي نتائج التحليل الإحصائي لمتغيرات الدراسة والتي تشمل المتوسطات الحسابية والانحراف المعيارى للأسئلة الخاصة بتوافر سياسات الهوية الآلية لأمن المعلومات فى نظام معلومات جامعة القصيم :

**جدول رقم (٦)**
**نتائج التحليل الإحصائي لتوافر الهوية الآلية لأمن المعلومات فى نظام المعلومات بجامعة القصيم**

| الرقم | بنود التقييم | المتوسط الحسابى | الانحراف المعيارى | درجة الموافقة |
|---|---|---|---|---|
| أولا : المقاييس الحيوية | | | | |
| 9 | نمط شبكية العين | 1.6286 | 0,48668 | 2 |
| 10 | بصمة الأصابع | 2.0857 | 0,67551 | 2 |
| 11 | نمط الصوت | 1.5429 | 0,67428 | 1 |
| 12 | نمط الضغط على لوحة المفاتيح | 2.5571 | 0,79191 | 2 |
| ثانيا : أدوات تكنولوجيا متقدمة | | | | |
| 13 | الهوية المعرفة بترددات الراديو | 2.0857 | 0,60775 | 2 |
| 14 | البطاقة الذكية | 2.0000 | 0,58977 | 2 |
| 15 | أنظمة الانذار | 3.5714 | 0,79073 | 4 |
| 16 | أنظمة المراقبة المرئية ، مثل كاميرات المراقبة | 3.4714 | 0,86345 | 4 |
| 17 | استخدام زجاج غير شفاف لغرف الحاسبات | 3.7714 | 0,42294 | 4 |
| ثالثا : أنظمة الحماية البيئية | | | | |
| 18 | تركيب أنظمة كشف الدخان | 3.8571 | 0,57195 | 4 |
| 19 | وضع طفايات الحريق بالقرب من غرف الخادمات | 4.1571 | 0,40417 | 4 |
| 20 | جعل جميع غرف الخادمات فى درجة حرارة باردة | 4.2429 | 0,43191 | 4 |
| | إجمالى السياسات الهوية الآلية | 1.7486 | 2.23912 | 2 |

يتضح من الجدول السابق الأتي :

• تعتبر سياسات الهوية الآلية لأمن المعلومات من السياسات الضرورية لتوفير الحماية الكاملة لنظم المعلومات ، على الرغم من ذلك يتضح من الجدول السابق عدم توافر العديد من سياسات تحديد الهوية الآلية فى نظام معلومات الجامعة ، فمثلا لا توافق غالبية عينة الدراسة على توافر سياسة « نمط شبكية العين « فى تحديد الهوية للأفراد العاملين فى نظام المعلومات والتى جاءت بمتوسط حسابى قدره (١,٦٢) وبانحراف معيارى مقدره (٠,٤٨٦).

• كانت درجة الموافقة منخفضة على إتباع سياسات الهوية الآلية لأمن المعلومات والتى تتمثل فى سياسة تحديد « نمط الصوت « فى تحديد الهوية للأفراد العاملين فى نظام المعلومات والتى جاءت بمتوسط حسابى قدره (١,٥٤) وبانحراف معيارى مقدره (٠,٦٧٤).

• كذلك كانت درجة الموافقة على توافر سياسات تحديد « بصمة الأصابع ، نمط الضغط على لوحة المفاتيح ،الهوية المعرفة بترددات الراديو والبطاقة الذكية « فى نظام معلومات وكانتوبمتوسط حسابي قدره (٢,٠٨ ، ٢,٥٥ ، ٢,٠٨) على التوالى. وأشارت بعض عينة الدراسة أنه لا يوجد حاجة لتطبيق هذه السياسات لعدم توافر بيانات على درجة عالية من الحساسية والتى تستلزم تطبيق هذه السياسات.

• موافقة كل عينة الدراسة على توافر بعض سياسات تحديد الهوية الآلية فى نظام معلومات الجامعة ، مثل توافر أنظمة المراقبة المرئية ، أنظمة الانذار وذلك بمتوسط حسابى قدره ٣,٤٧) ، ٣,٥٧) على التوالى.

• كانت درجة الموافقة عالية على توافر بعض سياسات تحديد الهوية الآلية فى نظام معلومات الجامعة ، مثل توافر زجاج غير شفاف لغرف الحاسبات ، تركيب أنظمة كشف الدخان ، وضع طفايات الحريق بالقرب من غرف الخادمات ، جميع غرف الخادمات فى درجة حرارة باردة فكان متوسط الإجابات لتوافر هذه السياسات (٣,٧٧ ، ٣,٨٦ ، ٤,١٦ ، ٤,٢٤) على التوالى.

(٣) الإجابات على أسئلة مدى توافر سياسات الحماية الفنية فى نظام المعلومات بجامعة القصيم.

يوضح الجدول التالي نتائج التحليل الإحصائي لمتغيرات الدراسة والتي تشمل المتوسطات الحسابية والانحراف المعيارى للأسئلة الخاصة بتوافر السياسات الفنية فى نظام معلومات جامعة القصيم :

**جدول رقم (٧)**

**نتائج التحليل الإحصائي لتوافر السياسات الفنية فى نظام معلومات الجامعة**

| الرقم | بنود التقييم | المتوسط الحسابى | الانحراف المعيارى | درجة الموافقة |
|---|---|---|---|---|
| أولا : سياسات كلمات المرور | | | | |
| 21 | وضع كلمات المرور والتي تشمل قوة وطول كلمة المرور ، واشتمالها على حروف وأرقام ورموز. | 4.7143 | 0,44698 | 5 |
| 22 | تغيير كلمة المرور فى فترات زمنية محددة وعدم استخدام نفس كلمة المرور بشكل دائم لكل المستخدمين | 4.1000 | 0,42221 | 4 |
| 23 | المحاولاتالفاشلةلتسجيلالدخول ( تعطيلالحساببعد3 محاولات فاشلة | 4.6429 | 0,43191 | 5 |
| 24 | انتهاءصلاحيةكلمةالمرور ( بعدأولعمليةتسجيل،ومنثمبعد– مرور60يوماعلىأخرتغييرلكلمةالسر | 3.9714 | 0,37960 | 4 |
| ثانيا : سياسات برامج الحماية وتأمين نظام المعلومات والشبكات | | | | |
| 25 | توافر برامج مكافحة الفيروسات أصلية ومرخصة ومحدثة بصفة مستمرة | 4.6714 | 0,47309 | 5 |
| 26 | توافر برامج قوية لكشف التسلل والاختراق في شبكة الجامعة | 3.8286 | 0,50994 | 4 |
| 27 | توافر برامج الجدران النارية لحماية وتأمين شبكات المعلومات ومنع الوصول غير المسموح به من خارج الجامعة لخدمات الشبكة | 4.2571 | 0,58199 | 4 |
| 28 | توافر برامج تقيد استخدام الشبكة اللاسلكية ويكون الوصول اليها لموظفين الجامعة فقط | 4.3286 | 0,50279 | 4 |
| ثالثا : سياسات التحكم بالوصول | | | | |
| 29 | تحديد صلاحيات المستخدمين المصرح لهم بالدخول لنظام معلومات الجامعة | 4,6143 | 0,47717 | 5 |
| 30 | توافر سياسات لتقييد الوصول وتصفح مواقع إنترنت معينة | 4,6429 | 0,45686 | 5 |
| 31 | ضبط الدخول إلى نظام التشغيل ، برامج التطبيقات وقواعد البيانات | 4.5714 | 0,62720 | 5 |
| 32 | تقييد استخدام وسائط التخزينية القابلة للإزالة في الجامعة طبقا لحاجة العمل | 3.3429 | 0,88278 | 3 |
| 33 | تخزين كافة الوسائط في بيئة آمنة ومحمية | 3.9571 | 0,46425 | 4 |
| رابعا : سياسات حماية خصوصية البيانات | | | | |
| 34 | الحفاظ على سرية المعلومات الحساسة | 3.5429 | 0,75538 | 4 |
| 35 | إتاحة المعلومات الخاصة للمستخدمين المسموح لهم بالإطلاع عليها فقط طبقا لحاجة العمل | 4,6143 | 0,42455 | 5 |
| 36 | تحديد صلاحيات الدخول للأطراف الخارجية لنظام المعلومات بالجامعة | 4,9143 | 0,79387 | 5 |
| 37 | الابلاغ الفورى عن نقاط الضعف فى حماية المعلومات الخاصة | 3.4714 | 0,81154 | 3 |
| خامسا : سياسات إدارة أصول المعلومات | | | | |
| 38 | تخصيص مالك لكل أصل من أصول المعلومات ، يكون له الحق فى اصدار تراخيص الاستخدام لهذا الأصل | 3.8857 | 0,64926 | 4 |
| 39 | تصنيف أصول المعلومات على أساس الحساسية ، الأهمية ، الخصوصية ، المعلومات العامة | 3.8571 | 0,68706 | 4 |
| 40 | مراجعة أصول المعلومات بصورة دورية للتأكد من تصنيفها بشكل سليم | 3.8571 | 0,88932 | 4 |
| 41 | يتم تحديد اجراءات تداول ، تخزين نقل وإتلاف أصول المعلومات وفقا للقواعد المحددة في نظام أمن المعلومات للجامعة | 3.9143 | 0,73707 | 4 |
| 42 | تحديد الأفراد والمجموعات المخولة من قبل مالك المعلومات بالوصول للمعلومات الحساسة | 4.1286 | 0,53626 | 4 |
| سادسا : سياسات تشفير البيانات | | | | |
| 43 | وضع سياسات التشفيرالخاصةبالجامعةمتوافقةمعالمعايير العالمية لتشفير البيانات والرسائل | 3,2143 | 1.03969 | 3 |
| 44 | تشفيرنسخالحفظالاحتياطيالتيتتضمنمعلوماتسرية وهامة | 3.3143 | 0,90958 | 3 |
| 45 | توافر اجراءات للتخلص من وسائط التخزين المختلفة المنتهية الصلاحية. | 3.5429 | 0,81090 | 4 |
| سابعا : سياسات إدارة وصول المستخدمين | | | | |
| 46 | توافر إجراءات وأنظمة خاصة بإنشاء وإدارة حسابات المستخدمين وحذفها ، وسحب حقوق الدخول | 4.5857 | 0,64814 | 5 |
| 47 | تخصيص لكل مستخدم من مستخدمى نظم المعلومات هوية وكلمة مرور فريدة | 4.7571 | 0,52297 | 5 |
| 48 | تحديد مسئوليات المستخدمين طبقا لطبيعة عمل كل منهم | 4.3714 | 0,64091 | 4 |
| 49 | إلزام كافة المستخدمين بقراءةاتفاقيةعدم الإفشاءالخاصةبالجامعةوالتوقيععليها. | 4.2857 | 0,60318 | 4 |

| | | | | |
|---|---|---|---|---|
| | ثامنا : سياسات النسخ الاحتياطي | | | |
| 50 | إجراءحفظاحتياطي لبرامجالتطبيقاتونظامالتشغيل ،وقواعدالبيانات ،ومعلومات التهيئةالخاصة بالمستخدمين بصفة دورية | 3.7000 | 0,59831 | 4 |
| 51 | اختباركافةنسخالحفظالاحتياطيعلىفترات منتظمة ،وذلكلضمانإمكانيةقراءةالبيانات | 3.1571 | 0,97261 | 3 |
| 52 | الاحتفاظ بالنسخ الاحتياطية للسجلاتوكافة المعلومات المهمة داخل غرفة الحاسبات | 4.3143 | 0,49761 | 4 |
| | تاسعا : سياسات إدارة الحوادث الأمنية | | | |
| 53 | التزام الموظفين بإعداد تقارير بالحوادث الأمنية للمعلومات بصفة دورية | 3.3000 | 0,76802 | 3 |
| 54 | إنشاء أحداثورسائل التنبيه الخاصةبكشفالتسللبحيثتقومبالاستجابةدون تأخير | 3.7286 | 0,56264 | 4 |
| 55 | توافر إجراءات تعقبالتعديلات Audit Trails بحيثيمكنتعقب هويةوأنشطةالمستخدمينالمربوطينبالشبكة | 3.7000 | 0,64494 | 4 |
| 56 | استخدامأدواتالمسح للتعرف على نقاطضعفالحمايةالتييمكنأنيتماستغلالهامنقبلأشخاصخارجيين | 2.8000 | 0,87807 | 3 |
| 57 | توافر سياسات واضحة وفعالة لتقييم الثغرات ونقاط الضعف في نظام أمن المعلومات | 3.6143 | 0,70798 | 4 |
| | عاشرا : سياسات التعامل مع البريد الالكتروني | | | |
| 58 | استخدام بروتوكول للبريد الالكتروني S/MIME لتشفير رسائل البريد الالكتروني | 3.9714 | 0,77966 | 4 |
| 59 | استخدام خاصية عدم التحميل التلقائي للملفات المرفقة | 4.2429 | 0,62405 | 4 |
| 60 | التأكد من تشغيل برنامج المضاد للفيروسات لفحص رسائل البريد الالكتروني | 4.3857 | 0,64365 | 4 |
| | مجموع السياسات الفنية | 3.9154 | 0,21862 | 4 |

يتضح من الجدول السابق الأتي :

• موافقة غالبية عينة الدراسة بشدة على توافر العديد من سياسات الحماية الفنية فى نظام معلومات الجامعة ، مثل البنود ( ٢١ ، ٢٣ ، ٢٥ ، ٢٩ ، ٣٠ ، ٣١ ، ٣٥ ، ٣٦ ، ٤٦ ، ٤٧) والتى حصلت على درجة موافقة عالية جدا وبلغ المتوسط الحسابى لها (٤,٧١ ، ٤,٦٤ ، ٤,٦٧ ، ٤,٦١ ، ٤,٦٤ ، ٤,٥٧ ، ٤,٦١ ، ٤,٩١ ، ٤,٥٨ ، ٤,٧٦ )على التوالي، وهذا يعكس اهتمام إدارات تقنية المعلومات بتوافر سياسات الحماية الفنية لتأمين وحماية خصوصية البيانات للمستخدمين من طلاب وموظفين إداريين وأعضاء هيئة التدريس بالجامعة وخاصة هذه السياسات والتى تختص بوضع كلمات المرور القوية لحماية حسابات المستخدمين ، استخدام برامج مضادة للفيروسات قوية ومحدثة بصفة مستمرة ، إدارة ومراقبة صلاحيات دخول المستخدمين لنظام المعلومات .

• موافقة غالبية عينة الدراسة على توافر العديد من سياسات الحماية الفنية فى نظام معلومات الجامعة ، مثل البنود (٢٢ ، ٢٤ ، ٢٦ ، ٢٧ ، ٢٨ ، ٣٣ ، ٣٤ ، ٣٨ ، ٣٩ ، ٤٠ ، ٤١ ، ٤٢ ، ٤٥ ، ٤٨ ، ٤٩ ، ٥٠ ، ٥٢ ، ٥٤ ، ٥٥ ، ٥٧ ، ٥٨ ، ٥٩ ، ٦٠ ) وكانت الاجابات بمتوسط يتراوح بين ٣,٥٤ إلى ٤,٣٨٥ . تشير هذه النتائج أن إدارات تقنية المعلومات بالجامعة تطبق كم كبير من سياسات الحماية الفنية لتأمين وحماية نظام المعلومات بها ، وذلك لقوة هذه السياسات وتكلفتها المنخفضة مقارنة بسياسات تحديد الهوية الآلية.

• كانت عينة الدراسة محايدة فى الإجابة على توافر سياسات الحماية الفنية فى نظام معلومات الجامعة والخاصة فى البنود (٣٢ ، ٣٧ ، ٤٣ ، ٤٤ ، ٥١ ، ٥٣ ، ٥٦) وبلغ المتوسط الحسابى لهذه الاجابات على التوالي ( ٣,٣٤٢ ، ٣,٢١٤ ، ٣,٣١٤ ، ٣,١٥٧ ، ٣,٣٠٠ ، ٢,٨٠٠ ) ، وهى متوسطات منخفضة عن البنود السابقة ، مما يفسر عدم اهتمام ادارات تقنية المعلومات بتطبيق هذه السياسات لتأمين وحماية نظام معلومات الجامعة وذلك لعدم توفر متخصصين فى أمن المعلومات فى إدارات تقنية المعلومات بالجامعة .

(٤) الإجابات على أسئلة المخاطر التى يتعرض لها نظام المعلومات بجامعة القصيم ومدى تكرار حدوثها.يوضح الجدول التالي نتائج التحليل الإحصائي لمتغيرات الدراسة والتي تشمل المتوسطات الحسابية والانحراف المعيارى للأسئلة الخاصة بتكرار المخاطر فى نظام معلومات جامعة القصيم :

**جدول رقم (٨)**

**نتائج التحليل الإحصائي لتكرار حدوث المخاطر فى نظام معلومات الجامعة**

| | بنود التقييم | مرة على الأكثر يوميا (النسبة %) | مرة على الأكثر أسبوعيا (النسبة %) | مرة على الأكثر شهريا (النسبة %) | مرة على الأكثر سنويا (النسبة %) | لا يحدث مطلقا (النسبة %) | المتوسط الحسابي | الانحراف المعياري |
|---|---|---|---|---|---|---|---|---|
| | أولا : المخاطر والتهديدات التي يتعرض لها نظام معلومات الجامعة نتيجة قلة الخبرة و الوعي والتدريب لمستخدمي نظام المعلومات بالجامعة | | | | | | | |
| 61 | سرقة بيانات الهوية من نظام المعلومات في الجامعة | 0 | 5.7 | 14.3 | 34.3 | 45.7 | 1.8000 | 0.8944 |
| 62 | العبث بالبيانات أو إتلافها من قبل المستخدمين لنظام المعلومات في الجامعة | 0 | 14.3 | 38.6 | 7.1 | 20 | 2.6714 | 0.9588 |
| 63 | سوء استغلال الصلاحيات الممنوحة لمستخدمي نظام المعلومات في الجامعة | 0 | 5.7 | 40 | 45.7 | 8.6 | 2.4286 | 0.7336 |
| 64 | شيوع استخدام وتبادل كلمات المرور بين المستخدمين لنظام المعلومات في الجامعة | 0 | 11.4 | 48.6 | 3.4 | 8.6 | 2.6286 | 0.8016 |
| 65 | الادخال غير المقصود للبيانات الخاطئة من قبل المستخدمين | 2.9 | 10 | 44.3 | 38.6 | 4.3 | 2.6857 | 0.8260 |
| 66 | عمل نسخ غير مصرح بها من البيانات الهامة | 0 | 18.6 | 60 | 14.3 | 7.1 | 2.9000 | 0.7829 |
| 67 | الوصول غير المرخص به لنظام معلومات بواسطة أشخاص من خارج الجامعة | 0 | 1.4 | 12.9 | 62.9 | 22.9 | 1.9286 | 0.6442 |
| | ثانيا : المخاطر والتهديدات التي يتعرض لها نظام معلومات الجامعة نتيجة لعدم توفر أو ضعف الأدوات والأجهزة والبرامج الرقابية المستخدمة. | | | | | | | |
| 68 | دخول الفيروسات في نظام المعلومات بالجامعة | 2.9 | 10 | 48.6 | 18.6 | 20 | 2.5714 | 1.0134 |
| 69 | التلاعب/الخداع من المخترقين والقراصنة لموقع الجامعة على شبكة الانترنت | 2.9 | 15.7 | 31.4 | 50 | 0 | 2.7143 | 0.8365 |
| 70 | الالتقاط السلكي وتحليل الاتصالات/عمليات استراق السمع وسرقة المعلومات المتبادلة عبر الأسلاك | 1.4 | 5.7 | 17.1 | 37.1 | 38.6 | 1.9429 | 0.9613 |
| 71 | إغراق النظام بجعل شبكة المعلومات أو النظام مشغولا بصورة دائمة وذلك بإرسال الرسائل البريدية الالكترونية دفعة واحدة | 0 | 0 | 17.2 | 35.7 | 47.1 | 1.7000 | 0.7489 |
| 72 | الاحتيال عبر البريد الإلكتروني وسرقة المعلومات الخاصة بالمستخدمين | 0 | 7.2 | 14.3 | 47.1 | 31.4 | 1.9714 | 0.8676 |
| 73 | تكرار حدوث عدم توفر الخدمة Denial of service Attack في نظام المعلومات بالجامعة | 0 | 0 | 8.6 | 60 | 31.4 | 2.4857 | 0.6537 |
| 74 | اختراق الشبكات اللاسلكية | 12.9 | 11.4 | 25.7 | 31.4 | 18.6 | 2.6857 | 1.2688 |
| 75 | الكوارث الطبيعية ، مثل الحرائق ، الأبخرة والغازات | 0 | 20 | 24.3 | 31.4 | 24.3 | 2.4000 | 1.0686 |
| | الاجمالي | 1.3 | 8.3 | 30 | 33.2 | 27.1 | 1.7257 | 0.2476 |

يتضح من الجدول السابق الأتي :

• يلاحظ من الجدول السابق أن درجة تكرار خطرسرقة بيانات الهوية من نظام المعلومات فى الجامعة غير عالية ، حيت تتركز أغلب التكرارات ما بين مرة سنويا أو شهريا ، وأن نسبة (٤٥,٨ ٪) أفادت أن سرقة بيانات الهوية لا تحدث أبدا فى نظام معلومات الجامعة . وقد حصل هذا البند على درجة أهمية منخفضة بلغت فى المتوسط (١,٨٠ ) وبانحراف معيارى قدره (٠,٨٩٤٤٣) ، ويرجع هذا إلى حرص المستخدمين على عدم تسريب بيانات الهوية الشخصية للدخول على نظام معلومات الجامعة.

• درجة تكرار خطر العبث بالبيانات أو اتلافها من قبل المستخدمين لنظام المعلومات فى الجامعة عالية ، حيث تتركز أغلب التكرارات ما بين مرة واحدة شهريا بنسبة (٥٨,٦ ٪) وبمتوسط حسابى عالى (٢,٦٧١٤) ، وهذا يدل على كثرة تلف البيانات أو فقدها بسبب مستخدمى النظام بدون قصد. لذلك يجب على مديرى نظام المعلومات مراجعة البيانات المدخلة ومراقبة صلاحيات المستخدمين ومنع الدخول غير المصرح به للنظام.

• يتضح من الجدول السابق أن خطر سوء استغلال الصلاحيات الممنوحة لمستخدمي نظام المعلومات فى الجامعة نادرا ما تتكرر فى نظام معلومات الجامعة ، حيث أجابت نسبة (٤٥,٧ ٪) من عينة الدراسة أن هذا الخطر تحدث مرة على الأقل سنويا وبمتوسط حسابى منخفض قدره (٢,٤٢٨) ، وهذا يدل على وعى مستخدمى نظام المعلومات على أهمية الحفاظ على أمن وسرية المعلومات المخزنة فى نظام معلومات الجامعة.

• أظهرت النتائج من الجدول السابق أن شيوع استخدام وتبادل كلمات المرور بين المستخدمين لنظام المعلومات فى الجامعة يحدث بشكل متكرر ، حيث أفادت نسبة (٤٨,٦ ٪) من عينة الدراسة أن هذا الخطر يحدث مرة على الأقل شهريا ، وتعتبر هذه المشكلة من أكثر المخاطر التى تواجه نظام معلومات حيث حصلت درجة أهمية متوسطة وبلغ المتوسط الحسابى قدره (٢,٦٢) وبانحراف معيارى مقداره (٠,٨٠١٦٥) . وقد أفاد بعض من مديرى إدارات نظم المعلومات بالجامعة أنه لا يوجد الزام للمستخدمين بالتوقيع على إجراءات وسياسات أمن المعلومات.

• أفادت نسبة كبيرة من عينة الدراسة أنهيوجد مخاطر كثيرة تحدث بشكل متكرر مرة على الأقل شهريا فى نظام معلومات ، مثل الوصول غير المرخص به لنظام معلومات بواسطة أشخاص من خارج الجامعة بنسبة ( ٦٢,٩ ٪) وبدرجة أهمية مرتفعة بمتوسط حسابى قدره (٢,٩٢٨) ، عمل نسخ غير مصرح بها من البيانات الهامة بنسبة ( ٦٠ ٪) وبدرجة أهمية مرتفعة بمتوسط حسابى قدره (٢,٩) ، دخول الفيروسات فى نظام المعلومات بالجامعة بنسبة ( ٤٨,٦ ٪) بدرجة أهمية متوسطة بمتوسط حسابى قدره (٢,٥٧) ، الادخال غير المقصود للبيانات الخاطئة من قبل المستخدمينبنسبة ( ٤٤,٣ ٪) وبدرجة أهمية متوسطة حيث بلغ المتوسط الحسابى قدره (٢,٦٨).

• اتضح من الجدول السابق أن درجة تكرار خطر التلاعبوالخداع من المخترقين والقراصنة لموقع الجامعة على شبكة الانترنت غير مرتفعة ، حيث كانت أكبر تكرار بنسبة ( ٥٠ ٪) هي مرة واحدة على الأقل سنويا ، وتراوحت باقى التكرارات ما بين مرة على الأقل شهريا أو أسبوعيا. لا يحدث هذا الخطر بشكل متكرر يوميا ، حيث بلغ نسبة حدوثه (٢,٩). ومن حيث الأهمية ، يعتبر هذا الخطر متوسط الأهمية لدى عينة الدراسة ، بلغ متوسط أهميته (٢,٧١).

• يعتبر خطر الالتقاط السلكي وتحليل الاتصالاتبغرضاستراق السمع وسرقة المعلومات المتبادلة عبر الأسلاك من الأخطار التى تحدث بشكل متكرر ، حيث كانت نسبة تكرار حدوثه (٣٨ ٪) من مرة على الأقل شهريا أو سنويا ، ومن حيث الأهمية يعتبر منخفض الأهمية لدى عينة الدراسة بلغ بمتوسط (١,٩٤).

• يتضح من الجدول السابق ندرة حدوثخطر إغراق النظام بجعل شبكة المعلومات أو النظام مشغولاًبصورة دائمة ، حيث نسبة (٤٧,١ ٪) من عينة الدراسة أجابت أن هذا الخطر منخفض الأهمية لدى عينة الدراسة ، بلغ متوسطه (١,٧٠٠) ، وهذا يدل على توافر سياسات وإجراءات لتنظيم وتأمين وصول المستخدمين لنظام المعلومات وتقسيمصلاحياتالوصولإلىالمعلوماتبينأكثرمنمس توىإداري ،الأمرالذييحيل دخول الغير مصر ح لهم بالوصول إلى نظام المعلومات

• إلىالنظاموالوصولإلىهذهالمعلوماتبالأمر غيرالسهللمنلايملكمثله ذهالصلاحيات

• اتضح من الجدول السابق أن نسبة مرتفعة (٤٧,١ ٪) من عينة الدراسة أجابت بأن خطر الاحتيال عبر البريد الإلكتروني يتكرر حدوثه من مرة على الأقل شهريا إلى مرة على الأقل سنويا، وكانت درجة الأهمية منخفضة بمتوسط حسابى (١,٩٧) ، ويرجع ذلك لوجود برامج الجدران النارية المطبقة فى نظام معلومات الجامعة لحماية البريد الالكتروني من العبث والاختراق.

• يعتبر خطر اختراق الشبكاتاللاسلكية من الأخطار التى يتكرر حدوثها كثير فى نظام معلومات الجامعة ، حيث أجابت نسبة (١٢,٩ ٪) بأن هذا الخطر يحدث مرة على الأقل يوميا ، ونسبة (٢٠ ٪) أجابت بأن خطر اختراق الشبكاتاللاسلكية يحدث من مرة على الأقل شهريا إلى مرة على الأقل أسبوعيا ، وكانت درجة الأهمية لهذا الخطر مرتفعة حيث بلغ متوسطه (٢,٦٨) ، وهذا يدل على سهولة التقاط كلمات المرور للشبكات اللاسلكية الموصلة بالجامعة وضعف اجراءات الامن المطبقة لحماية هذه الشبكات.

• تعتبر أخطار الكوارث الطبيعية ، مثل الحرائق ، الأبخرة والغازات تحدث بدرجة قليلة فى نظام معلومات الجامعة ، حيث أجابت نسبة (٣٣,٢ ٪) من عينة الدراسة أن هذا الخطر يحدث مرة على الأقل سنويا، ونسبة (٣٠ ٪) أجابت بأن هذا الخطر قد يحدث مرة على الأقل شهريا وكانت درجة أهمية هذا الخطر متوسطة بالنسبة للجامعة ، حيث بلغ متوسطه الحسابي (٢,٤٠)، وهذا يدل على وجود سياسات وإجراءات أمنية قوية لمواجهة الأخطار والكوارث الطبيعية.

**٨- النتائج والتوصيات:**

إن استخدام تقنية المعلومات فى الجامعات دون اتخاذ الاجراءات اللازمةالكافية لحماية الأجهزة والبرمجيات وشبكات الاتصال ، يؤدى إلى حدوث مخاطر عديدة تؤثر على أداء النظام وتوفر الخدمة للمستخدمين ، عدم قدرة الادارة العليا على اتخاذ القرارات السليمة لعدم توفر المعلومات الصحيحةوالكاملةلدعم اتخاذ القرارات فى الوقت المطلوب. هدفت هذه الدراسة على إلى التعرف على سياسات وإجراءات أمن المعلومات المطبقة فى جامعة القصيم ، من حيث سياسات الحماية الإدارية ، سياسات تحديد الهوية الآلية ، سياسات الحماية الفنية والمخاطر التى يتعرض لها نظام معلومات الجامعة ، وقد توصلت الدارسة إلى مجموعة من النتائج والتوصيات من هذه الدراسة.

**أولا : النتائج:**

• يعتمد على تقنية المعلومات وشبكات الحاسبات بشكل كبير فى جامعة القصيم فى النواحي التعليمية والنواحي الإدارية ، إلا أن هذا الاعتماد لا يتفق مع عدد الموظفين المتخصصين فى تقنية المعلومات وخاصة فى مجال أمن المعلومات ، حيث اتضح من الدراسة التحليلية لنظام معلومات الجامعة عدم توافر متخصصين فى أمن المعلومات فى عمادة تقنية المعلومات والإدارات التابعة لها فى الكليات المختلفة. وأيضا عدم إعطاء الموظفين الحاليين فى إدارات تقنية المعلومات دورات تدريبية متخصصة فى أمن المعلومات.

• موافقة غالبية عينة الدارسة على عدم توفر العديد من سياسات الحماية الإدارية فى نظام معلومات جامعة القصيم ، مثل توافر إدارة خاصة بأمن المعلومات فى الجامعة ، توافر موظفون متخصصون بأمن المعلومات ، توقيعالموظفين علىالالتزامبكافةالسياساتوالإج راءاتوالمعاييروالإرشاداتالخاصة بأمن المعلومات ، عدم إعطاء دورات تدريبية للموظفين الجدد حول سياسات وإجراءات امن المعلومات فى الجامعة.

• موافقة كل عينة الدراسة على اتباع بعض اجراءات وسياسات تحديد الهوية الآلية لحماية أمن وخصوصية البيانات فى الجامعة مثل توافر أنظمة المراقبة المرئية ، أنظمة الانذار ، زجاج غير شفاف لغرف الحاسبات، تركيب أنظمة كشف الدخان ، وضع طفايات الحريق بالقرب من غرف الخادمات ، جميع غرف الخادمات فى درجة حرارة باردة.

• اهتمام إدارات تقنية المعلومات بإتباع العديد من سياسات وإجراءات الحماية الفنية لتأمين وحماية خصوصية البيانات للمستخدمين من طلاب وموظفين إداريين وأعضاء هيئة التدريس بالجامعة ، مثل وضع كلمات المرور القوية لحماية حسابات المستخدمين ، استخدام برامج مضادة للفيروسات قوية ومحدثة بصفة مستمرة ، إدارة ومراقبة صلاحيات دخول المستخدمين لنظام المعلومات ، إنشاء أحداث ورسائل التنبيه الخاصة بكشف التسلل ، الاحتفاظ بنسخ احتياطية للسجلات وكافة المعلومات المهمة داخل غرف الحاسبات الرئيسية.

• حدوث مخاطر فى نظم معلومات الجامعة بشكل متكرر ترجع إلى أسباب تتعلق بموظفي تقنية المعلومات نتيجة قلة الخبرة والوعي والتدريب، أسباب تتعلق بعدم وجود سياسات واضحة ومكتوبة وضعف الاجراءات والأدوات الرقابية المطبقة.

• تعتبر مخاطر العبث بالبيانات أو اتلافها من قبل المستخدمين لنظام المعلومات فى الجامعة، شيوع استخدام وتبادل كلمات المرور بين المستخدمين لنظام المعلومات فى الجامعة، الادخال غير المقصود للبيانات الخاطئة من قبل المستخدمين، عمل نسخ غير مصرح بها من البيانات الهامة من اكثر المخاطر تكرارا حيث قد تحدث أكثر من مرة شهريا إلى مرة أسبوعيا.

• وجود بعض المخاطر التى قد تحدث مرة على الأقل يوميا فى نظام معلومات الجامعة ، مثل الادخال غير المقصود للبيانات الخاطئة من قبل المستخدمين ، دخول الفيروسات فى نظام المعلومات بالجامعة ، اختراق الشبكاتاللاسلكية.

• موافقة غالبية عينة الدراسة على عدم حدوث مخاطر تتعلق سرقة بيانات الهوية من نظام المعلومات فى الجامعة ، الالتقاط السلكي وتحليل الاتصالاتبغرضاستراق السمع وسرقة المعلومات المتبادلة عبر الأسلاك ، إغراق النظام بجعل شبكة المعلومات أو النظام مشغولاًبصورة دائمة وذلك بإرسال الرسائل البريدية الالكترونية دفعة واحدة.

**ثانيا: التوصيات:**

شملت التوصيات الأتي :

• أهمية تطوير سياسات أمن نظم المعلوماتوحمايتها ووضع معايير ومواصفات قياسية لاستخدامات نظم المعلومات وتطبيقها بصورةفاعلة.

• ضرورة تحديد الأهداف الأمنية الأساسية وهي

• ضرورة التأكيد على تكامل وتوفرالخدمة وجاهزيتها، وذلك بوضع توصيات لسد الثغرات الأمنية فى نظام المعلومات لتفادي أسبابالسرقات للهوية وكلمات المرور ، ومنع التسلل والاختراق للشبكات اللاسلكية المتصلة بنظام معلومات الجامعة.

• أهمية وجود إدارات مؤهلة ومختصة فى أمن نظم المعلومات ومراجعتهاوتدقيقها بصفة دورية.

• أهمية نشر الوعي الأمني لجميع العاملين فى الجامعة بشتى مستوياتهم،

• إجراء عمليات تدقيق دوري لتقييم السياسات والإجراءات الأمنية المطبقة وتحديد نقاط الضعف والثغرات الأمنية فور حدوثها ، ثم معالجة آثارها عند حدوثها.

• تشجيع البحوث في مجال أمن المعلومات وطرق التشفير وغيرها من مجالات أمن المعلومات في الجامعات ومراكز البحوث المحلية .

• ضرورة وضع ضوابط أمن ورقابة المعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أم اتصالات سلكية ولاسلكية والإنترنت ، والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية.

**المراجع:**


1- الدليل الفنى لتقييم أمن المعلومات ، http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

2- رجب عبد الحميد حسنين (2012)، «أمن شبكات المعلومات الالكترونية : المخاطر والحلول» ، http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=629:networks&catid=257:studies&Itemid=90

3- سلمان بن علي بن وهف القحطاني (2003) ، « أمن المعلومات في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة»

faculty.ksu.edu.sa/المعلومات/20%أمن.doc /alhomoudy/392

4- عائض المرى (2013)، «امن المعلومات ماهيتها وعناصرها وإستراتيجياتها « ، http://www.dralmarri.com/show.asp?field=res_a&id=205.

5- عبد الفتاح القاهرى (2010)، «معنى أمن المعلومات» ، http://jabzea.3arabiyate.net/t47-topic .

6- عصام البحيصي وحرية الشريف (2008) «مخاطر نظم المعلومات المحاسبية الالكترونية دراسة تطبيقية على المصارف العاملة في قطاع غزة» ، site.iugaza.edu.ps/ibuhaisi/files/2010/02/AIS_Threats.doc .

7- فادي عمروش (2010) ، «إعداد السياسات الأمنية فى الشبكات اللاسلكية» ، http://mpra.ub.uni-muenchen.de/28011/1/MPRA_paper_28011.pdf

8- فواز الحربي و حسين عبده موكلي (2010) ، «معايير أمن المعلومات: دراسة تلخيصية» ، http://coeia.ksu.edu.sa/

9- ما هو المعيار العالمي لأمن المعلومات ((ISO-17799 ، http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/55-information-assurance-management-and-governance/953-iso-17799.html

10- محمد ابراهيم الرباعى ، «أمن الشبكات» ، faculty.mu.edu.sa/download.php?fid=4045 ، 2010.

11- محمد بن عبدالله القحطانى وخالد بن سليمان الغثنبر ، «أمن المعلومات بلغة ميسرة « ، مكتبة الملك فهد الوطنية ، الرياض ، 2009 ، ص22.- http://coeia.edu.sa/im-ages/stories/books/Information-Security.pdf

12- محمد محمد الهادى ، « توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية « ، http://www.journal.cybrarians.info/index.php?option=com_content&view=article&id=370:2009-07-15-09-59-43&catid=161:2009-05-20-10-01-08&Itemid=70

13- معايير أمن المعلومات (2011) ، http://www.cert.sd/ar/index5567.html

14- نور الدين محمد حامد ( 2007) « أمن نظم ومعلومات المصارفوحمايتها بإشارة خاصة للواقع السوداني» ، http://www.newkerma.net/vb/showthread.php?t=273 .

15- يونس عرب «الخصوصية وامن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي» ، 2001 ، http:// www.yemen-nic.info/contents/Informatics/studies/7.pdf

16- Erik Johansson, Pontus Johnson,(2005) «Assessment of Enterprise Information Security - An Architecture Theory Diagram Definition», http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.75.2922 , accessed in 17/9/2012

17- Victoriano Casas , (2006), « AN INFORMATION SECURITY RISK ASSESSMENT MODEL FOR PUBLIC AND UNIVERSITY ADMINISTRATORS», https://digital.library.txstate.edu/bitstream/handle/10877/3674/fulltext.pdf, accessed in 19/9/2012.

18- Michael Jones, (2008) ,»An Evaluation of Privacy and Security Issues at a Small University», http://www.ijme.us/cd_08/PDF/123,it301.pdf

19- D.S. Bhilare and et al, (2008), «Information Security Assessment and Reporting: Distributed Defense», http://www.csi-sigegov.org/emerging_pdf/11_89-101.pdf

20- Fred H. Cate (2006), «The Privacy and Security Policy Vacuum in Higher Education»,http://www.educause.edu/ero/article/privacy-and-security-policy-vacuum-higher-education