واقع ودوافع الالتزام بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية دراسة حالة جامعة الخليل

*بلال عمرو**

ملخّص

يُعَدّ أمن نظم المعلومات مطلبًا مهمًا في سبيل تطوير واستخدام نظم المعلومات الحاسوبية الذي بدوره يوفر الأمان الكامل للمعلومات ويحافظ على خصوصية الأفراد؛ حيث يُعَدّ العامل البشري من العوامل المهمة في هذا المجال. ومن الممارسات البشرية التي تساهم في تعريض نظم الملومات الحاسوبية للخطر: الجهل والإهمال واللامبالاة وقلة الوعي بأمن المعلومات... الخ. في هذا البحث سيتم إلقاء الضوء على أهمية الالتزام بتطبيق معايير أمن المعلومات في مؤسسات التعليم العالي الفلسطينية –دراسة حالة جامعة الخليل.تكمن أهمية هذا البحث في معرفة واقع سياسات أمن نظم المعلومات في الجامعات الفلسطينية ومعرفة العوامل المؤثرة على الالتزام بسياسات أمن نظم المعلومات مثل المعرفة بأمن المعلومات والخبرة والتحصيل العلمي. وقد خلصت الدراسة إلى أن درجة المعرفة بأمن نظم المعلومات والالتزام بها لدى موظفي جامعة الخليل كانت عالية. كما خلصت الدراسة إلى وجود فروقات ذات دلالة إحصائية لمدى التزام الموظفين بسياسات أمن نظم المعلومات تبعا للمؤهل العلمي وسنوات الخبرة. وقد أوصت الدراسة بضرورة العمل على متابعة تطبيق سياسات أمن نظم المعلومات وتحديثها ومراجعتها بما يتناسب متطلبات المرحلة القادمة وما يشهده العالم من تطور تكنولوجي هائل.

الكلمات الدالة: أمن المعلومات، سياسات أمن المعلومات، التعليم العالي.

المقدمة

مما لا شك في أن التطور الهائل في مجال الاتصالات وتكنولوجيا المعلومات أحدث ثورة في عالم الأعمال والمؤسسات الخدماتية. حيث أصبحت الشركات والمؤسسات تعتمد على نحو كبير على التكنولوجيا في انجاز المهام والمعاملات بسهولة ويسر. واتجهت معظم حكومات العالم نحو توفير الخدمات الإلكترونية للمواطنين تحت اطار ما يسمى بالحكومة الالكترونية. حيث انتشرت تلك الخدمات على نحو كبير ولاقت اقبالًا لا مثيل له من قبل المواطنين. كما أتاحت الإتصالات وتكنولوجيا المعلومات المجال للعديد من الشركات بممارسة أعمالها على نحو الكتروني كامل، والاستثمار في مجالات وأماكن متعددة دون الحاجة الى التواجد في تلك الأماكن. وقد اصبح معيار التقدم التكنولوجي من أهم المعايير التي يتم تقييم العديد من المؤسسات بناءً عليها.

و مع هذا التطور الهائل والاستخدام الواسع للتكنولوجيا في المؤسسات والشركات، ظهر الجانب الآخر لتطبيق هذه التكنولوجيا والمتمثل بالجرائم الإلكترونية كالقرصنة، والتصيد الالكتروني، وانتحال الشخصية، والفيروسات، وبرامج التجسس وغيرها. وقد كان لهذا الجانب الأثر الكبير في تقنين انتشار التكنولوجيا على نحو أوسع، كما كان له الأثر الكبير في العديد من الخسائر المادية للعديد من الشركات. ومما يبعث على القلق لدى مستخدمي التكنولوجيا هو الزيادة المطردة في أعداد الهجمات الإلكترونية عالميا وخاصة في مجال التصيد الالكتروني حيث يشير التقرير الصادر عن معهد التدريب المتخصص في أمن الشبكات والمعلومات (SANS institute) (https://www.sans.org) إلى إرتفاع جرائم التصيد الإلكتروني بنسبة 250٪ بين العامين 2018 و2019 (Pescatore, 2019).

يُعَدّ وجود سياسات تنظم كافة الأعمال التكنولوجية في المؤسسات والشركات من العوامل الأساسية في التقليل من الجريمة الإلكترونية، وبالتالي التقليل من الآثار الناجمة عنها. ففي دراسة أعدها باحثون من الولايات المتحدة الامريكية حول تأثير السياسات الأمريكية في العالم الإفتراضي (فضاء الشابكة)، وجد الباحثون أن هذه السياسة نجحت في التخفيف الملحوظ من هذه

* جامعة الخليل، فلسطين.

تاريخ استلام البحث 2020/6/10، وتاريخ قبوله 2020/9/22.

الهجمات (Kumar, Benigni, & Carley, 2016).

و تأثرت فلسطين كغيرها من دول العالم بهذا التقدم التكنولوجي حيث أصبحت التكنولوجيا إحدى أعمدة الاقتصاد، والركيزة الأساسية في أداء الخدمات في كافة مؤسسات الوطن. وقد رافق ذلك ازديادا ملحوظا في أعداد الجرائم الإلكترونيةفي فلسطين حيث تشير تقارير الشرطة الفلسطينية إلى ارتفاع في نسبة الجريمة الالكترونية في العام 2018 بمعدل 26.6٪ (الشرطة الفلسطينية، 2019). وتتنوع أسباب الجريمة الإلكترونية في فلسطين ودوافعها كغيرها من دول العالم، حيث تشير الأبحاث والدراسات المحلية والعالمية بأن تلك الأسباب تعود إلى غياب الوعي لدى المستخدمين (Amro, 2018) (Bruijn & Janssen, 2017).

ونظرا إلى ارتباط انخفاض معدل الجريمة الإلكترونية بتطبيق سياسات إستخدام التكنولوجيا كما أشرنا سابقا (Kumar، Benigni، و Carley، 2016) فإن دراسة واقع سياسات أمن نظم المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل سيساهم في إلقاء الضوء على نحو أدق على واقع سياسات أمن نظم المعلومات في الجامعات الفلسطينية، والمشاكل التي تعاني منها تلك المؤسسات بهدف وضع الحلول اللازمة لرفع مستوى الأمان، والتقليل من الجرائم الإلكترونية في المستقبل، وتعزيز أنظمة المؤسسات بتطبيق السياسات الفاعلة.

مشكلة الدراسة:

يرافق كل تطور في وسائل الأمن والحماية لتكنولوجيا المعلومات والاتصالات تطورًا في الجانب الآخر الخاص بإختراق هذه الأنظمة، متمثلا بالجريمة الإلكترونية بكافة أشكالها. ومنذ بداية استخدام التكنولوجيا وظهور الجرائم الالكترونية، تعمل المؤسسات والأفراد على مسابقة الزمن في الحصول على أفضل تقنيات الحماية والأمان للحفاظ على أمن معلوماتهم وخصوصيتهم أو خصوصية زبائنهم.

غير أن الإعداد الأمثل لأنظمة تكنولوجية آمنة لا يقتصر على توظيف التكنولوجيا الحديثة مثل مضادات الفيروسات، والجدران النارية، وأنظمة كشف التسلل فحسب. بل يتطلب ذلك إعداد وتوظيف كوادر بشرية قادرة على استخدام التكنولوجيا على نحو آمن. ويتطلب ذلك من المؤسسات اعداد برامج تدريبية دورية للموظفين، وعمل نشرات توعوية للزبائن لإرشادهم الى سبل الاستخدام الآمن للتكنولوجيا، وتوظيفها لخدمة مصالحهم.

وحتى تتمكن الشركات والمؤسسات من ضبط استخدام التكنولوجيا من قبل الموظفين والزبائن، فإنها بحاجة أيضا إلى وضع سياسات الاستخدام الآمن لأدوات التكنولوجيا بما فيها الإنترنت. ويتطلب الموضوع كذلك تطبيق هذه السياسات، والمراقبة والتقييم المستمرين لهذه السياسات، وتغييرها عند الحاجة؛ لضمان أفضل الوسائل وطرق الاستخدام الآمن.

و كغيرها من المؤسسات الفلسطينية، فان الجامعات الفلسطينية كانت ولا زالت سباقة في تطبيق أنظمة تكنولوجيا المعلومات لتوفير خدمات إلكترونية آمنة وموثوقة. وقد كانت هناك العديد من المحاذير والمخاوف من تطبيق التكنولوجيا لحساسية البيانات، وخصوصية بعض الإجراءات ذات العلاقة بالمعاملات المالية أو حتى ملفات الطلبة الأكاديمية. وبالرغم من تلك المخاطر إلا أن الجامعات قطعت شوطا طويلا في تبني التكنولوجيا المتقدمة لتقديم الخدمات الإلكترونية.

و في ظل جائحة كورونا، وانتقال الجامعات الفلسطينية الى التعليم الالكتروني، أصبحت الحاجة ملحة لحماية بيانات المستخدمين وضمان استمرارية تقديم الخدمات عن بعد. وحيث أن التوسع في استخدام التكنولوجيا سلاح ذو حدين، فان أنظمة المعلومات الإلكترونية في الجامعات الفلسطينية بما فيها جامعة الخليل عرضة لشتى اشكال الجرائم الالكترونية. ومن وسائل التخفيف من حدة تلك الجرائم هو تطبيق سياسات أمن نظم المعلومات ومتابعة تنفيذها. من هنا أتت فكرة هذه الدراسة لكي تلقي الضوء وبصورة ميدانية فاعلة على واقع سياسات أمن المعلومات في الجامعات الفلسطينية – دراسة حالة جامعة الخليل –، لمعرفة مدى تطبيق تلك السياسات والإلتزام بها والتوصيات اللازمة لتحسين واقع سياسات أمن نظم المعلومات، إضافة الى معرفة قدرة تلك الجامعات في الصمود أمام التحديات المستقبلية فيما يخص تطور التكنولوجيا. حيث تكمن مشكلة الدراسة في الأسئلة الرئيسية التالية:

1. ما هو واقع معرفة الموظفين بسياسات أمن نظم المعلومات في جامعة الخليل؟
2. ما هو واقع وجود وتطبيق سياسات امن المعلومات في جامعة الخليل؟
3. ما هو مدى الالتزام بسياسات امن المعلومات في جامعة الخليل؟

أهداف الدراسة

تتمثل أهداف الدراسة في هدف رئيسي وأهداف فرعية. أما الهدف الرئيسي هو:

- تعرُّف واقع سياسات أمن نظم المعلومات في جامعة الخليل، ودوافع الالتزام بهذه السياسات من قبل الموظفين.

وينبثق عن الهدف الرئيسي الأهداف الفرعية التالية:

- تعرُّف مدى معرفة الموظفين بسياسات أمن نظم المعلومات في جامعة الخليل.
- تعرُّف مدى التزام الموظفين في جامعة الخليل بسياسات امن نظم المعلومات.
- تعرُّف وجود فروقات ذات دلالة إحصائية عند مستوى الدلالة ($\propto \leq 0.05$) على مستوى معرفة الموظفين في جامعة الخليل بسياسات أمن نظم المعلومات وأثر تلك المعرفة في الالتزام بتطبيق تلك السياسات.

أهمية الدراسة:

تكمن أهمية هذه الدراسة من الناحية النظرية في:

1) تسليط الضوء على واقع سياسات أمن نظم المعلومات في مؤسسات التعليم العالي الفلسطينية.
2) توضيح أهمية تطبيق سياسات أمن نظم المعلومات في مؤسسات التعليم العالي الفلسطينية.
3) اثراء الأدب النظري بتزويد المكتبة الفلسطينية والمكتبات العربية بهذا النوع من الدراسات.

من الناحية التطبيقية، ستسهم هذه الدراسة في الأمور التالية:

1. مساعدة أصحاب الإختصاص وصانعي القرار في جامعة الخليل والجامعات الفلسطينية لرفع الجاهزية لمواجهة الجرائم الإلكترونية، من خلال الإطلاع على واقع السياسات المستخدمة، وتطوير وتطبيق السياسات الامنة ان لزم الامر.
2. مساعدة أصحاب القرار في وزارة التربية والتعليم العالي لاتخاذ الإجراءات اللازمة لتطوير سياسات أمن نظم المعلومات في مؤسسات التعليم العالي.
3. مساعدة أصحاب القرار في وزارة الاتصالات وتكنولوجيا المعلومات بالاطلاع على واقع سياسات أمن نظم المعلومات في الجامعات الفلسطينية، وتطبيق دراسات مشابهة على المؤسسات والشركات الفلسطينية، للخروج بتصور شامل ووضع سياسات أمنية عصرية ومتطورة لمواجهة الجريمة الالكترونية.

حدود الدراسة:

- الحدود الموضوعية: هدفت هذه الدراسة إلى تعرُّف واقع سياسات أمن نظم المعلومات في جامعة الخليل ودوافع الالتزام بها.
- الحدود المكانية: مجال الدراسة المكاني هو جامعة الخليل في فلسطين
- الحدود النوعية: شملت الدراسة عينة عشوائية من موظفي وطلبة جامعة الخليل.
- الحدود الزمنية: تم جمع البيانات والمعلومات الخاصة بالدراسة في عام 2020.

مصطلحات الدراسة:

- نظم المعلومات: يمكن تعريف أنظمة المعلومات على أنها تركيبة مكونة من مكونات مادية للحواسيب والبرمجيات والافراد والبيانات وشبكات الاتصال، تتفاعل مع بعضها بعض حسب علاقات معينة يتم من خلالها جمع البيانات ومعالجتها وعرضها والحصول على المعلومات منها. (ياسين، 2009)
- أمن نظم المعلومات: عرف المشهداني أمن نظم المعلومات بأنه: الحفاظ على معلومات النظام المعلوماتي من المخاطر مثل الضياع أو الإستخدام غير الصحيح أو الكوارث الطبيعية او غيرها. (المشهداني، 2001). كما عرفه غيطاس على أنه: مزيج من الرؤى والإجراءات والسياسات التي يتم تصميمها وتنفيذها على مستويات مؤسساتية ومجتمعية تهدف الى تحقيق عناصر الحماية التي بدورها تضمن تحقيق السرية والموثوقية والتوافرية وسلامة البيانات. (غيطاس، 2007)
- سياسات امن نظم المعلومات: عرف الغثبر والقحطاني سياسات أمن المعلومات بأنها مجموعة التوجيهات واللوائح والممارسات والقواعد التي تحدد كيفية القيام بإدارة وتوزيع المعلومات وحمايتها. (الغثبر و القحطاني، 2009). كما عرفها Dulany بأنها مجموعة قوانين وتوجيهات أمنية تضبط نظام المعلومات وتعطيه مستوى موثوق به من الحماية. ويجب أن توجه هذه السياسات الإدارة ووسائل الحماية والوقاية المرتبطة بالمعلومات ومصادرها. وعادة ما تكون هذه السياسات مرتبطة بمستويات من المخاطر المنوي تجنبها. (Dulany, 2002).

الإطار النظري:

أولا: نظم المعلومات

يعرف النظام بأنه مجموعة من المكونات التي تتفاعل مع بعضها بعض لتحقيق هدف معين. وعليه يمكن تعريف نظم المعلومات بأنه النظام القائم على تجميع البيانات ومعالجتها بهدف الحصول على المعلومات منها وتخزينها او عرضها بالطريقة المناسبة. وبحسب Satir and Reynolds، فإن أي نظام معلومات يتكون من العناصر التالية حتى يحقق الأهداف المرجوة منه: (Stair & Reynolds, 2012)

1. المكونات التقنية: وتعرف بأنها المكونات الملموسة وغير الملوسة التي تشكل ما يمكن تسميته بتكنولوجيا المعلومات والاتصالات التي يمكن تصنيفها بما يلي:

- أجهزة الحواسيب: وهي التي تشكل العتاد المادي وتشمل مكونات جهاز الحاسوب من وحدات الادخال والذاكرة ووحدات التخزين والمعالجة والإخراج.
- البرمجيات: التعليمات التي ينفذها العتاد المادي وتنقسم إلى قسمين أساسيين برمجيات النظم وهي التي تتحكم بتشغيل العتاد المادي وتنظيم عمله والبرمجيات التطبيقية التي تستخدم لأهداف محددة
- معدات الشبكات والاتصال: وتستخدم لربط أجهزة الحواسيب ببعضها بعض محليا أو إقليميا او دوليا. وهي أهم مصدر لتبادل البيانات والمراسلات بسرعة وفاعلية.

2. البيانات؛ حيث تُعَدّ البيانات كنزا مهما بالنسبة لنظام المعلومات، وهي أساس العمل ومحرك التطوير في المؤسسة، حيث يقوم نظام المعلومات بالعديد من العمليات على البيانات وتشمل:
   - تجميع البيانات.
   - تخزين البيانات.
   - تحليل ومعالجة البيانات.
   - عرض البيانات.
   - تحديث البيانات.
3. الأفراد: وهم مستخدمو نظام المعلومات سواء كانوا مستخدمين مباشرين أم غير مباشرين. وبحسب Loudon and Loudon، يمكن تحديد فئات المستخدمين لأنظمة المعلومات ضمن الشرائح التالية: (Loudon & Loudon, 2010)

- المستخدمين النهائيين: ويطلق عليهم باللغة الإنجليزية مصطلح End Users. ويقصد بهم كل من يستخدم نظام المعلومات ويستفيد من مخرجاته في تنفيذ مهامه وأداء الأعمال الموكلة اليه.
- مستخدمو المعرفة ويطلق عليهم باللغة الإنجليزية Knowledge Workers، وهم منتجو المعرفة عن طريق معالجة البيانات وتخزينها وتوزيعها. وعادة ما ينتسبون الى المستويات الإدارية العليا.
- خبراء ومختصي تكنولوجيا المعلومات: ويطلق عليهم باللغة الإنجليزية مصطلح IT experts، وهم العاملون في مجالات تكنولوجيا المعلومات المختلفة مثل المبرمجين ومحللي النظام ومدير الشبكة وغيرهم.

4. الإجراءات والسياسات: يقصد بها مجموعة من الخطوات المحددة والتعليمات الواضحة والمتسلسلة لإنجاز العمليات في أنظمة المعلومات. حيث يحدد من خلالها عمل النظام وكافة وظائفه ضمن تسلسل منطقي يحقق كافة الأهداف المرجوة من النظام بعيدا عن التعقيد (Stair & Reynolds, 2012)

ثانيا: تعريف أمن المعلومات وأمن نظم المعلومات:

تعددت تعريفات مصطلح أمن نظم المعلومات وتطورت مع تطور الاتصالات وتكنولوجيا المعلومات. حيث ظهر في بداية الستينيات مصطلح حماية أو أمن الحاسوب الذي يعني أن نقوم بحماية أجهزة الحواسيب وقواعد البيانات. ومع تطور التكنولوجيا وانتشار استخدام أجهزة الحواسيب تطور المفهوم إلى أمن البيانات في فترة السبعينات، حيث تم التركيز على استخدام كلمات المرور والتحكم بالوصول للبيانات. أما في مراحل الثمانينات والتسعينات فقد اصبح المصطلح أمن المعلومات نظرا إلى انتشار شبكات الحاسوب ومشاركة البيانات والمعلومات. وأصبح من الضروري المحافظة على المعلومات بتطبيق الإجراءات الأمنية المناسبة. وظهرت في هذه الفترة مصطلحات اختراق نظم المعلومات والهجمات المختلفة (الغثبر و القحطاني، 2009).

ويمكن تعريف أمن المعلومات حسب Whitman and Mattord بأنه " الحفاظ على سرية وتوافر وسلامة المعلومات

كأصل، في مراحل المعالجة والحفظ والنقل، ويتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعلم والتدريب" (Whitman & Mattord, 2012). وقد اتفق الجميع على أن أمن المعلومات يجب أن يحقق مثلث الحماية الأساسي (السرية، المصداقية، والتوافرية) ويتم اختصارها باللغة الإنجليزية بالأحرف الثلاث CIA (Confidentiality, Integrity, and availability). (Bourgeois & Bourgeois, 2014) (Easttom, 2019)

ويقسم Jason Andress مكونات أمن نظم المعلومات الى:(Andress, 2014)

1. تأمين العمليات.
2. تأمين المورد البشري (المستخدمين).
3. التأمين الفيزيائي للمعدات.
4. تأمين الشبكة.
5. تأمين نظام التشغيل.
6. تأمين التطبيقات المستخدمة.

حيث يتم ذلك من خلال تقنيات الأمان المختلفة التي تتضمن: التشفير والتعرف والتحقق من المستخدمين والتحقق من الصلاحيات وحق الوصول والتدقيق والمساءلة. وهذا يتطلب وجود قواعد وتعليمات لتحقيق السياسات الأمنية المرجوة.

و قد ركز العديد من الباحثين وخبراء أمن المعلومات على ضرورة وضع وتطبيق سياسات أمن المعلومات للحفاظ على أمن المعلومات وسريتها. (غيطاس، 2007)

و يلاحظ من التعريفات السابقة بأن أمن نظم المعلومات:

- إجراءات إدارية وتقنية.
- تهدف للحفاظ على كافة مكونات النظام.
- تحمي النظام من الإختراق والسرقة والتجسس وغيرها من الهجمات.

ثالثا: تعريف سياسات أمن نظم المعلومات وأنواعها

من التعريفات السابقة يمكن لنا تعريف أمن نظم المعلومات بأنه مجموعة من السياسات التي يتم تحقيقها عبر مجموعة تقنيات تهدف بمجملها إلى الحفاظ على عناصر أمن البيانات الأساسية وهي السرية والتوافرية والمصداقية.

تهديدات امن نظم المعلومات:

وبحسب الدنف فانه يمكن تعريف التهديد بأنه كل انتهاك أو خرق لنظام المعلومات بقصد او بدون قصد ما ينتج عنه فقد او تعديل للبيانات وحتى الاطلاع عليها من قبل غير المصرحين لهم بذلك. (الدنف، 2013)

و تتنوع مصادر تهديد أمن نظم المعلومات وتختلف تصنيفاتها باختلاف مصادر التهديد من حيث التهديدات الداخلية او التهديدات الخارجية وذلك حسب تصنيف بسيوني. (بسيوني، 2007). وقد اختلف المختصون في تقييم مخاطر التهديدات الخارجية والداخلية، فمنهم من اعتقد بأن معظم التهديدات تأتي من مصادر خارجية. ولكن ذلك لا يمنع الأشخاص الداخليين الذين يمتلكون صلاحيات عالية على النظام من أن يكونوا أكثر فتكا بالنظام. ومن وجهة نظر الشبلي (الشبلي، 2009) فان أفضل وأبسط تصنيف لتهديدات أمن نظم المعلومات هو:

- تهديدات مصدرها مكونات نظم المعلومات نفسها مثل:أخطاء التشغيل أو ثغرات البرمجيات أو أخطاء المستخدمين.
- تهديدات تنتج عن أفعال ضارة هادفة من قبل جهات معينة.
- تهديدات ناتجة عن الكوارث الطبيعية كالزلازل والحرائق وغيرها.

ثالثا: إدارة مخاطر نظم المعلومات:

نظرا إلى زيادة المخاطر والتهديدات المتعلقة بأمن نظم المعلومات، فإن الشركات والمؤسسات بحاجة الى الإعداد والتخطيط المتقن لإدارة مخاطر نظم المعلومات. وبحسب Reynolds فإن عملية تقييم المخاطر تشتمل على الخطوات التالية(Reynolds, 2014):

- تحديد الأصول المادية وغير المادية.
- تحديد المخاطر التي يمكن أن تحدث واحتمالية حدوثها وكذلك تأثيرها على المؤسسة.
- تحديد وسائل الوقاية من هذه المخاطر ودراسة جدوى كل واحدة من هذه الوسائل.

- تحليل التكلفة والفائدة لكل وسيلة من وسائل الوقاية لإختيار الأنسب.
- في كل مرحلة من المراحل السابقة يتم إعادة التقييم عند الحاجة.

و لعل من أهم العوامل اللازمة لمواجهة التهديدات المحيطة بالشركات هي تبنيي وتطبيق سياسات أمن المعلومات في المؤسسات، وتحديثها باستمرار لمواكبة المستجدات في عالم التهديد الالكتروني. (عوض و خلف، 2003).

و قد عرفت سياسات أمن نظم المعلومات إجرائيا بانها " مجموعة من الإجراءات والقواعد الأمنية التي تساهم في تعريف المستخدمين بمسؤولياتهم وواجباتهم لضمان امن وحماية المعلومات " (عبد الواحد، 2015) وتهدف سياسات أمن المعلومات الى:

1. تعريف الافراد بمسؤولياتهم وواجباتهم تجاه نظام المعلومات في المؤسسة.
2. توضيح الآليات المستخدمة لتنفيذ وتحقيق سياسات أمن المعلومات.
3. توضيح الإجراءات الواجب اتباعها لضمان عدم إختراق نظام المعلومات.

و يجب أن تتسم سياسات أمن المعلومات بما يلي (داود، 2004):

- بساطة اللغة.
- وضوح البنود.
- ذات تكلفة معقولة.
- تتوافق مع القوانين المتبعة.
- قابلة للتطوير والمراجعة.

و فيما يخص الهيكل الهرمي لإدارة سياسات أمن المعلومات فقد قام Hare بتقسيمه الى (Hare, 2001):

التشريعات: ويتم اعدادها من قبل الحكومات.

السياسات: ويتم وضعها من قبل المؤسسة بموافقة الإدارة العليا.

المعايير: تشتق من السياسات وتقيس مدى التزام العاملين بتلك السياسات.

الإجراءات: تعليمات توضيحية للمستخدم عن كيفية تطبيق السياسات على شكل خطوات محددة.

التوجيهات: توصيات اختيارية تتضمن تفضيلات المؤسسة لما تحب ان تراه.

وتنوعت الأمثلة على السياسات في مجال أمن نظم المعلومات، ومن الأمثلة عليها حسب Maynard وآخرون (Maynard, Ruighaver, & Sandow-Quick, 2002):

- سياسة البريد الالكتروني.
- سياسة الإنترنت.
- سياسة الخصوصية.
- سياسة البرمجيات.
- سياسة قبول الإستخدام.

كما يمكن ان يضاف اليها أمثلة أخرى حسب الشبلي (الشبلي، 2009) ومنها:

- سياسة الحماية الفيزيائية.
- سياسة تأمين الشبكات.
- سياسة الحماية من الفيروسات.

كما يمكن أيضا اعتماد سياسة كلمات المرور وسياسة استخدام الشبكات اللاسلكية وغيرها من العديد من السياسات. وفي هذا السياق قامت العديد من المؤسسات وحتى الدول بتطوير سياسات أمن نظم المعلومات وتطبيقها لما لها من أهمية كبيرة في الحفاظ على نظم المعلومات وسلامتها. وقد وضعت العديد من المرجعيات في عالم الأمن والحماية معاييرا دولية للحفاظ على أمن نظم المعلومات. ومن هذه المرجعيات معهد التدريب المتخصص بأمن الشبكات والمعلومات (SANS) الذي يُعَدّ من المرجعيات الاكاديمية والتدريبية في مجال أمن المعلومات؛ حيث قام هذا المعهد بوضع نماذج سياسات متعددة في مجالات مختلفة في نظم المعلومات، وبإمكان أي مؤسسة اختيار نموذج السياسة المناسب وتقييم وضع نظام المعلومات بناء عليه.

وتُعَدّ مؤسسة ISO (https://www.iso.org/about-us.html) من المؤسسات العالمية غير الحكومية والمختصة في وضع المعايير العالمية في قطاعات مختلفة. ومن هذه المعايير ISO/IEC 27001:2013 الذي يهتم بتكنولوجيا المعلومات بما

فيها أمن نظم المعلومات والسياسات المستخدمة. ونظرا إلى حساسية بعض أنظمة المعلومات فقد عمدت المؤسسة أيضا الى إيجاد معايير متخصصة لهذه الأنظمة مثل الخصوصية والحماية في أنظمة المعلوماتية الصحية التي تحمل الرقم ISO/TS 14441:2013 (Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment, 2020)

دراسات سابقة

في هذا الباب، سيتم عرض بعض الدراسات العربية والأجنبية التي اهتمت بسياسات أمن المعلومات في المؤسسات. حيث قام العديد من الباحثين بالتطرق لموضوع أمن نظم المعلومات لما له من أهمية كبيرة في تطور عمل المؤسسات والشركات. وقد ركز معظمهم على أمن نظم المعلومات والوسائل والتقنيات اللازمة لتعزيز نظم المعلومات، الا أن القليل منهم تحدث عن واقع تطبيق سياسات أمن نظم المعلومات ودورها في رفع مستوى الأمان في المؤسسات والشركات. وفي هذا السياق نشرت دراسة تبحث في واقع إدارة أمن نظم المعلومات في المؤسسات السورية (يونس، 2017). حيث استخدمت الباحثة المنهج البحثي الوصفي مستعينة بدراسات سابقة والإستبانة كأدوات لدراستها. وقد خلصت الباحثة ان الإدارات العليا في المؤسسات والوزارات تدرك أهمية سياسات أمن نظم المعلومات إلا أنه لا يوجد سياسات مطبقة على نحو واضح في تلك المؤسسات. وخلصت الباحثة إلى ضرورة تبني سياسات فاعلة ومراقبة تطبيقها واعتماد برنامج تدريبي يهدف إلى تسهيل تطبيق السياسات وتطويرها.

وفي دراسة مشابهة، قامت آن عبد الواحد (عبد الواحد، 2015) بدراسة سياسات أمن المعلومات وعلاقتها بفاعلية نظم المعلومات الإدارية في الجامعات الفلسطينية في قطاع غزة. حيث اعتمدت المنهج الوصفي التحليلي مستخدمة الإستبانة بعينة عشوائية طبقية كأداة للبحث. وقد خلصت الدراسة إلى أهمية سياسات أمن نظم المعلومات ووجود درجة مرتفعة من الموافقة على فاعلية نظم المعلومات الإدارية عند تطبيق سياسات أمن نظم المعلومات. كما وجدت هناك فروق في الإستجابة في مجال سياسات أمن نظم المعلومات تعزى إلى متغير الجنس والتخصص العلمي. وقد خلصت الدراسة بضرورة دعم وتحفيز الجامعات على تطبيق سياسات أمن نظم المعلومات وتقييمها بإستمرار.

وفي سياق مشابه، قام الدنف (الدنف، 2013) بدراسة واقع إدارة نظم المعلومات في الكليات التقنية في قطاع غزة وسبل تطويرها. وقد استخدم الباحث المنهج الوصفي للدراسة معتمدا على الإستبانة كأداة للبحث إضافة الى المقابلات بهدف تجميع أكبر قدر ممكن من المعلومات. حيث أشار الباحث إلى توافر البنى التحتية بدرجة متوسطة مع عدم وجود سياسات معمول بها على أسس واضحة. وأوصى الباحث بضرورة الإهتمام بالبنى التحتية وبناء سياسات أمن نظم معلومات في هذه الكليات ومراقبة تطبيقها وتقييمها، ونوه الباحث إلى ضرورة الإعتناء بالتدريب لتحقيق أفضل نتائج في مجال تطبيق السياسات.

و في عمل مشابه (نبي، مرزا، و الغثبر، 2010)، قام سيد عرفان نبي وآخرون بدراسة عملية حول أمن المعلومات في المنظمات السعودية؛ حيث هدفت الدراسة إلى تعرُّف واقع أمن المعلومات في المملكة العربية السعودية. وقد استخدم الباحث المنهج الاستقصائي، وتوصلت الدراسة إلى أن غالبية المؤسسات تمتلك سياسة أمن نظم المعلومات وأن 89٪ منها يعمل مراجعة دورية لتلك السياسات. وأوصت الدراسة بضرورة رفع مستوى الوعي الأمني لدى مستخدمي نظم المعلومات من خلال برامج تدريبية ونشرات إرشادية متخصصة.

وقد قدم الصاحب (الصاحب، 2013)عرضا لأهمية أمن المعلومات ووجود سياسات لأمن المعلومات في الجامعات الفلسطينية من خلال دراسة حالة جامعة بوليتكنك فلسطين، واستعرض أيضا التهديدات التي تواجه نظم المعلومات في الجامعات والدوافع وراء ضرورة إعتماد وتطوير أمن نظم المعلومات في الجامعات. كما قام المؤلف بعرض مجموعة من الإجراءات والتعليمات الضرورية لتحقيق أفضل أمان في الجامعات.

و في دراسته لقياس كفاءة سياسات أمن المعلومات على شركة في الامارات العربية المتحدة، استخدم القرشي (القرشي، 2011)معيار مؤسسة المواصفات العالمية ISO 27004 لقياس كفاءة وفاعلية سياسات امن نظم المعلومات. وقد خلصت دراسته الى عدم وجود طريقة منهجية لقياس سياسات أمن نظم المعلومات في الشركة وعدم وجود رضا تام من الموظفين تجاه التدريبات اللازمة في مجال امن المعلومات. وقد اعتمد على عدد من المعايير لقياس قلة كفاءة سياسات أمن المعلومات التي من ضمنها قلة الوعي بأمن المعلومات وضعف التدريب والإرشاد.

و قد قام قدور مقراني (مقراني، 2016) بدراسة وتقييم مدى مساهمة أمن نظم المعلومات الإلكتروني في الحد من مخاطر نظم

المعلومات بدراسة حالة مؤسسة اتصالات الجزائر. حيث تطرق الباحث إلى المخاطر المحيطة بنظام المعلومات وطرق التخفيف منها. وقد توصل الباحث إلى أن السياسات الأمنية داخل المؤسسة من شأنها ضمان استمرارية عمل نظام المعلومات في ظروف طبيعية مع ضرورة إشراك المستخدمين في تقييم وتعديل هذه السياسات.

دراسات اجنبية

في دراسته لإلتزام الموظفين بسياسات أمن نظم المعلومات في قطاع التجزئة كدراسة حالة موظفي المتاجر (Muhire, 2012)، قام الباحث بدراسة تأثير مستوى التعليم على التزام الموظفين بسياسات أمن نظم المعلومات وهل يؤثر المستوى العلمي على الوعي بالسياسات الأمنية وبالتالي على التزام الموظفين بتلك السياسات. وقد استخدم الباحث المنهج الوصفي والاستبانة كأداة لجمع البيانات. وقد خلصت الدراسة إلى وجود علاقة إيجابية قوية بين المستوى العلمي والوعي بسياسات أمن نظم المعلومات. كما اشارت الدراسة إلى أن مستوى التعليم له أثر إيجابي على نية الموظفين للإلتزام بسياسات أمن نظم المعلومات.

و قد اجرى Burcu وآخرون (Bulgurcu, Cavusoglu, & Benbasat, 2010) دراسة تجريبية حول الإلتزام بسياسات أمن نظم المعلومات. وقد هدفت الدراسة إلى تقسيم الموظفين حسب تقييمهم العام لسياسات أمن نظم المعلومات. كما هدفت أيضا إلى تعرُّف معتقداتهم حول مخرجات الإلتزام بسياسات أمن المعلومات وتبعاتها، وإلى تعرُّف دور التوعية في مجال أمن المعلومات على معتقدات الالتزام بسياسات أمن نظم المعلومات. وقد استخدم الباحثون عدة أدوات للبحث من ضمنها الاختبار القبلي والبعدي. وقد خلصت الدراسة إلى أن إيجاد بيئة معرفية بأمن المعلومات في داخل المؤسسات ستعزز الإلتزام بسياسات أمن المعلومات وبالتالي رفع مستوى أمن المعلومات في المؤسسة. كما أوضحت الدراسة بان المكافآت المادية لا تؤثر على نحو كبير على الإلتزام بسياسات أمن نظم المعلومات إذ أن الموظفين يُعَدّوا المكافآت مرتبطة بأعمال غير الزامية. وقد أوصى الباحثون بضرورة توفير جزء من أوقات العمل للقيام بإجراءات سياسات أمن نظم المعلومات، كما اوصوا بضرورة توفير برامج تدريبية من جهات خارجية لرفع ثقة الموظفين بهذه التدريبات وبالتالي الإهتمام بالإلتزام بسياسات الأمان في المؤسسة.

قام Nader وآخرون (Safa, Solms, & Furnell, 2016) بتطوير نموذج يوضح كيف يؤدي الالتزام بسياسات أمن نظم المعلومات في المؤسسات إلى التخفيف من المخاطر المرتبطة بسلوكات الموظفين والمستخدمين. حيث قام الباحثون بدراسة ما يقارب 462 موظف يعملون في 4 شركات ماليزية جرى اختيارها من الشركات التي لديها سياسات أمن نظم معلومات، حيث استخدم الباحثون نموذج معادلة الهيكلة لتحديد العلاقة بين المتغيرات الكامنة والمتغيرات الملحوظة. ووجد الباحثون أن مشاركة المعلومات الخاصة بأمن نظام المعلومات والتعاون في مجال أمن المعلومات والتدخلات من قبل ذوي الخبرة لها تأثيرات إيجابية على أمن نظام المعلومات في المؤسسات. كما أشارت الدراسة إلى أن الإنضباط والسلوك الشخصي لهما أثر كبير في الإلتزام بسياسات أمن المعلومات في المؤسسات.

و في دراسة أخرى، قام Knapp وآخرون بدراسة تأثير التوعية وإلزام التنفيذ، والمراجعة والتحديث المستمرين لسياسات أمن نظم المعلومات على كفاءة أمن نظم المعلومات. حيث قام الباحثون بتجميع البيانات من مختصي أمن نظم المعلومات الحاصلين على شهادات في هذا المجال ممن يعملون في عدة مجالات منها الحكومية والمصرفية والصحية وغيرها. وقد خلصت الدراسة بأهمية هذه العوامل الثلاث (التوعية والزام التنفيذ والمراجعة الدورية) في رفع مستوى الإلتزام بسياسات أمن نظم المعلومات. حيث كان للتوعية الجزء الأكثر فاعلية يليها إجبار التنفيذ ومن ثَم المراجعة والتحديث المستمرين لسياسات أمن نظم المعلومات.

هدفت دراسة Jorro (Jorro, 2011) إلى تعرُّف مدى استعداد مؤسسات وهيئات الحكومة الاثيوبية لمراجعة أمن نظم المعلومات لديها للحيلولة دون تفاقم مشكلة أمن المعلومات والتخفيف من تبعاتها؛ حيث حاول الباحث تعرُّف مشاكل أمن نظم المعلومات التي تحول دون تطبيق خدمات الحكومة الإلكترونية، وتحليلها بهدف وضع سياسات وإجراءات تنظيمية لحل هذه المشاكل. وخلص الباحث إلى أن مؤسسات الحكومة الاثيوبية في مستوى منخفض من الجهوزية تجاه قضايا أمن نظم المعلومات، وأن تلك المؤسسات تفتقد إلى توافر السياسات والإجراءات اللازمة لعمل مراجعات لأمن المعلومات. ونوهت الدراسة أيضا إلى إفتقار تلك المؤسسات للكفاءات المدربة في مجال أمن نظم المعلومات.

و قد استفدنا من الدراسات السابقة في تحديد الجوانب الرئيسية الواجب فحصها لمعرفة واقع سياسات الأمان في مؤسسات التعليم العالي الفلسطينية، حيث أسهمت تلك الدراسات وعلى نحو كبير في مساعدتنا على تصميم الإستبانة وتحديد المحاور الرئيسية والمعلومات الديمغرافية اللازمة.

و قد امتازت هذه الدراسة عن الدراسات السابقة بتغطيتها لمجتمع دراسة مغاير لمجتمعات الدراسات الأخرى، كما ستقوم هذه الدراسة بتقديم نتائج وتوصيات مستقبلية في بيئة مغايرة لبيئة الدراسات الأخرى –مؤسسات التعليم العالي الفلسطينية– التي تُعَدّ بيئة مهمة للدراسة في ظل التطور التكنولوجي والحاجة الماسة لتأمين عملية التعليم الإلكتروني وخصوصا بعد جائحة كورونا.

الطريقة والإجراءات

مقدمة:

تناول هذا الجزء من الدراسة وصفًا كاملًا ومفصلًا لطريقة وإجراءات الدراسة التي قام بها الباحث لتنفيذ هذه الدراسة وشمل وصف منهج الدراسة، مجتمع الدراسة، وعينة الدراسة، أداة الدراسة، صدق الأداة، ثبات الأداة، إجراءات الدراسة، والتحليل الإحصائي.

منهج الدراسة:

استخدم الباحث المنهج الوصفي التحليلي وهو طريقة في البحث عن الحاضر، وتهدف إلى تجهيز بيانات لإثبات فروض معينة تمهيدًا للإجابة عن تساؤلات محددة– سلفًا– بدقة تتعلق بالظواهر الحالية والأحداث الراهنة التي يمكن جمع المعلومات عنها في زمان إجراء البحث وذلك باستخدام أدوات مناسبة.

مجتمع الدراسة:

تكون مجتمع الدراسة من جميع الموظفين في جامعة الخليل للعام الأكاديمي (2019–2020م) والبالغ عددهم (650) موظفا وموظفة.

عينة الدراسة:

طبقت الدراسة على عينة مكونة من (110) موظف وموظفة من العاملين في جامعة الخليل، اختيروا بطريقة العينة العشوائية الطبقية، وبعد جمع الاستبانات، بلغ عدد الاستبانات المستردة (104) استبانة، والجدول التالي يوضح خصائص أفراد العينة الديموغرافية:

الجدول (1): خصائص أفراد العينة الديموغرافية

المتغير	مستويات المتغير	العدد	النسبة %
الجنس	ذكر	85	81.7
	أنثى	19	18.3
	المجموع	104	100.0
المؤهل العلمي	دبلوم فأقل	8	7.7
	بكالوريوس	65	62.5
	ماجستير	15	14.4
	دكتوراة	16	15.4
	المجموع	104	100.0
الخبرة العملية	أقل من 5 سنوات	47	45.2
	من 5–9 سنوات	18	17.3
	من 10–14 سنة	27	26.0
	من 15–19 سنة	12	11.5
	المجموع	104	100.0
الفئة العمرية	18-30سنة	51	49.0
	31-45سنة	39	37.5
	46-60سنة	14	13.5
	المجموع	104	100.0

أداة الدراسة:

1- صدق المقياس:

أ- صدق المحكمين (الصدق الظاهري):

للتحقق من الصدق الظاهري للأداة قام الباحث بعرض الأداة على (3) محكمين من العاملين في الجامعات الفلسطينية ومن ذوي الاختصاص والخبرة، وفي ضوء آراء المحكمين تم حذف بعض الفقرات وتعديل بعضها، وبعد التعديلات أصبحت الأداة مكونة من (20) فقرة تتوزع على (3) محاور، المحور الأول: المعرفة في أمن نظم المعلومات ويتكون من (6) فقرات، والمحور الثاني: واقع سياسات أمن نظم المعلومات ويتكون من (9) فقرات، والمحور الثالث: مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة ويتكون من (5) فقرات.

ب- صدق الاتساق الداخلي:

تم التحقق من صدق الأداة بحساب معامل ارتباط بيرسون (Pearson Correlation) لكل فقرة من فقرات المجال الذي تنتمي إليه مع الدرجة الكلية للمجال، وذلك كما هو واضح في الجدول (2)

الجدول (2): نتائج معامل الارتباط بيرسون (Pearson correlation) لمصفوفة ارتباط كل فقرة من فقرات المجال مع الدرجة الكلية للمجال.

رقم الفقرة	الفقرات	معامل ارتباط بيرسون (ر)	القيمة الاحتمالية (Sig.)
أولًا: المعرفة في أمن نظم المعلومات			
.1	ادرك تماما المخاطر الأمنية المرتبطة بسوء استخدام نظم المعلومات.	0.53**	0.00
.2	على دراية تامة بمخاطر مشاركة كلمات المرور الخاصة بي وامتنع عن مشاركتها مع الاخرين.	0.70**	0.00
.3	على وعي تام بمخاطر تسريب أو مشاركة البيانات الخاصة بالمؤسسات مع جهات خارجية دون اذن او تصريح من الجهات ذات العلاقة.	0.73**	0.00
.4	من واجبي الإبلاغ عن أي حدث ذو علاقة بنظم المعلومات مثل هجمة فيروسية أو تسريب بيانات أو حجب خدمة أو غيرها من المخاطر.	0.71**	0.00
.5	أقوم بإستخدام كلمات مرور قوية صعبة التخمين وأقوم بتغييرها على نحو دوري كل 6 شهور على الأقل.	0.73**	0.00
.6	أقوم بالخدمات المخولة لي حسب صلاحياتي المتاحة لي من مدير النظام ولا أحاول التعدي على صلاحيات الغير باستخدام كلمات مرورهم أو اجهزتهم الخاصة.	0.73**	0.00
ثانيًا: واقع سياسات أمن نظم المعلومات			
.7	يوجد سياسات متبعة عند تزويد الموظف باسم المستخدم وكلمة المرور تتم من خلال دائرة شؤون الموظفين ودائرة نظم المعلومات.	0.65**	0.00
.8	يمنع الموظف من تعديل أو تنزيل البرامج على جهازه المكتبي أو المحمول دون الرجوع لدائرة تكنولوجيا المعلومات	0.77**	0.00
.9	هناك تعليمات واضحة لإستخدام الإنترنت السلكي واللاسلكي في أثناء العمل.	0.66**	0.00
.10	هناك تعليمات واضحة لإستخدام مواقع التواصل الإجتماعي والبريد الإلكتروني الخاص بالمؤسسة.	0.80**	0.00
.11	يتم توزيع التعليمات والسياسات الخاصة بأمن نظم المعلومات على نحو دوري حسب الإجراءات المعتمدة في المؤسسة بحيث يعرف كل موظف هذه السياسات.	0.68**	0.00
.12	يوجد نظام عقوبات خاص بمخالفة سياسات الأمان في المؤسسة بحيث يعرف كل موظف العقوبة حسب المخالفة التي ارتكبها.	0.79**	0.00
.13	تمنع المؤسسة استخدام البرمجيات المقرصنة على أجهزتها.	0.64**	0.00
.14	توظف المؤسسة التقنيات اللازمة لحماية نظم المعلومات من خلال برامج مضادة للفيروسات وحماية الشبكة وكشف التسلل.	0.76**	0.00

رقم الفقرة	الفقرات	معامل ارتباط بيرسون (ر)	القيمة الاحتمالية (Sig.)
.15	توفر المؤسسة تدريب وتوعية للموظفين حول سياسات المؤسسة الخاصة بأمن المعلومات من خلال ورش عمل ودورات تدريبية.	0.71**	0.00
ثالثًا: مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة			
.16	بالنسبة إلي فان الإلتزام بسياسات امن المعلومات هو ضروري ومفيد لي وللمؤسسة.	0.74**	0.00
.17	لدي النية بالالتزام بسياسات المؤسسة في مجال أمن المعلومات	0.55**	0.00
.18	لدى النية للحفاظ على مصادر المؤسسة الإلكترونية حسب ما هو موضح في سياسات امن نظم المعلومات.	0.79**	0.00
.19	لدي العزم على تحمل مسؤولياتي تجاه سياسات أمن نظم المعلومات في المؤسسة والعمل على تطويرها في المستقبل	0.69**	0.00
.20	لدي قناعة تامة بان عدم التزامي بسياسات أمن المعلومات في المؤسسة سيعرضني للمسؤولية بناء على ما هو موضح في تلك السياسات.	0.69**	0.00

** دالة إحصائيًا عند ($\alpha \leq 0.01$)، * دالة إحصائيًا عند ($\alpha \leq 0.05$)

تشير المعطيات الواردة في الجدول (2) إلى أن جميع قيم مصفوفة ارتباط فقرات المجال مع الدرجة الكلية للمجال دالة إحصائيًا، مما يشير إلى قوة الاتساق الداخلي لفقرات الأداة، وهذا بالتالي يعبر عن صدق فقرات الأداة في قياس ما صيغت من أجل قياسه.

وللتحقق من صدق الاتساق الداخلي للمجالات قام الباحث بحساب معاملات الارتباط بين درجة كل مجال من مجالات الأداة مع الدرجة الكلية للأداة والجدول (3) يوضح ذلك.

الجدول (3): مصفوفة معاملات ارتباط درجة كل مجال من مجالات الأداة مع الدرجة الكلية للأداة.

المتغيرات	معامل ارتباط بيرسون (ر)	القيمة الاحتمالية (Sig.)
المعرفة في أمن نظم المعلومات * الدرجة الكلية	0.79**	0.00
واقع سياسات أمن نظم المعلومات * الدرجة الكلية	0.94**	0.00
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة* الدرجة الكلية	0.81**	0.00

** دالة إحصائيًا عند ($\alpha \leq 0.01$)، * دالة إحصائيًا عند ($\alpha \leq 0.05$)

يتضح من خلال البيانات الواردة في الجدول (3) أن جميع المجالات ترتبط بالدرجة الكلية للأداة ارتباطًا ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.01$)، حيث أن معامل ارتباط بيرسون للعلاقة بين درجة كل مجال والدرجة الكلية للأداة كان قويًا، مما يشير إلى قوة الاتساق الداخلي لفقرات الأداة وأنها تشترك معا في قياس التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل.

2- الثبات:

قام الباحث بحساب الثبات بطريقة الاتساق الداخلي وبحساب معادلة الثبات كرونباخ ألفا، وكذلك تم حساب الثبات بطريقة التجزئة النصفية، وذلك كما هو موضح في الجدول (4).

الجدول (4): معاملات الثبات

المتغيرات	عدد الفقرات	كرونباخ ألفا معامل الثبات
المعرفة في أمن نظم المعلومات	6	0.78
واقع سياسات أمن نظم المعلومات	9	0.90
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	5	0.79
الدرجة الكلية	20	0.89

تشير المعطيات الواردة في الجدول (4) أن قيمة معامل ثبات كرونباخ ألفا لجميع مجالات الأداة وللدرجة الكلية للأداة كانت جيدة، حيث تراوحت قيم معامل ثبات كرونباخ ألفا لمجالات الأداة ما بين (0.78 – 0.90)، وبلغ معامل ثبات كرونباخ ألفا للدرجة الكلية للأداة (0.89)، مما يشير إلى أن الأداة تتمتع بدرجة مرتفعة من الثبات، مما يعطى الباحث درجة من الثقة عند استخدام الأداة في البحث الحالي، ويعد مؤشرًا على أن الأداة يمكن أن تعطي النتائج نفسها إذا ما أعيد تطبيقها على العينة نفسها وفى ظروف التطبيق نفسها.

تصحيح الأداة:

وزعت درجات الإجابة عن فقرات المقياس بطريقة ليكرت Likert حيث يحصل المستجيب على 5 درجات عندما يجيب (أوافق بشدة)، 4 درجات عندما يجيب (أوافق)، 3 درجات عندما يجيب (محايد)، ودرجتان عندما يجيب (لا أوافق)، ودرجة واحدة عندما يجيب (لا أوافق بشدة).

وقد تم تقسيم طول السلم الخماسي إلى ثلاث فئات لمعرفة درجة موافقة أفراد عينة الدراسة على مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل، وتم حساب فئات المقياس الخماسي كما يلي:

مدى المقياس = الحد الأعلى للمقياس– الحد الأدنى للمقياس = (5–1) = 4

عدد الفئات = 3

طول الفئة = مدى المقياس ÷ عدد الفئات

= 4 ÷ 3 = 1.33

بإضافة طول الفئة (1.33) للحد الأدنى لكل فئة نحصل على فئات المتوسطات الحسابية كما هو موضح في الجدول (5):

الجدول (5): فئات المتوسطات الحسابية لتحديد درجة الموافقة لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل

فئات المتوسط الحسابي	مدى الالتزام درجة الموافقة
2.33–1.00	قليلة
3.67–2.34	متوسطة
5.00–3.68	كبيرة

متغيرات الدراسة:

المتغيرات المستقلة: الجنس، المؤهل العلمي، الخبرة العلمية، الفئة العمرية.

المتغير التابع: التزام الموظفين بسياسات امن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل.

إجراءات الدراسة:

- من خلال الرجوع إلى ما أتيح من الأدب التربوي، المرتبط بمتغيرات الدراسة، الذي ساعد الباحث على تكوين خلفية علمية لموضوع الدراسة.

- بالرجوع إلى بعض الدراسات والأبحاث المحلية والعربية والعالمية ذات العلاقة بمتغيرات الدراسة للإفادة منها في بناء أداة الدراسة.
- قام الباحث بتجهيز الأداة التي استخدمتها لجمع البيانات. وذلك بعد الحصول على الموافقات الخاصة ببدء تنفيذ توزيعها، ومن ثَم جرى جمعها وإجراء المعالجات الإحصائية اللازمة.

الأساليب الإحصائية:

اعتمد الباحث في تحليل بيانات دراسته بعد تطبيق الأدوات على أفراد عينة الدراسة، حزمة البرامج الاحصائية للعلوم الإجتماعية،

SPSS: Statistical Package for the Social Sciences, Version (26)

وجرى استخدام الاختبارات الإحصائية التالية:

- التكرارات والأوزان النسبية.
- المتوسطات الحسابية، الانحرافات المعيارية.
- اختبار كرونباخ ألفا لمعرفة ثبات فقرات الاستبانة.
- معامل الارتباط بيرسون (Pearson Correlation) لمعرفة صدق فقرات الاستبانة.
- اختبار (ت) (Independent samples T Test)، لمعرفة الفروق بين متوسطات عينتين مستقلتين.
- اختبار تحليل التباين الأحادي (One-Way Analysis of Variance) للمقارنة بين المتوسطات أو التوصل إلى قرار يتعلق بوجود أو عدم وجود فروق بين المتوسطات.
- اختبار شيفيه (Scheffe) للمقارنات الثنائية البعدية لإيجاد مصدر الفروق.

نتائج الدراسة:

يتضمن هذا الجزء من الدراسة، تحليلًا إحصائيًا للبيانات الناتجة عن الدراسة، وذلك من أجل الإجابة عن أسئلة الدراسة، وفحص فرضياتها.

السؤال الرئيس: ما مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل؟

للإجابة عن السؤال الرئيس، جرى استخراج المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل. وذلك كما هو في الجدول (6).

الجدول (6): المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لمدى التزام الموظفين بسياسات امن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل مرتبة تنازليًا

ترتيب المجال في الاستبانة	المجال	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي %	الترتيب	درجة الموافقة
1	المعرفة في أمن نظم المعلومات	4.55	0.37	91.0	1	كبيرة
3	مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	4.50	0.47	90.0	2	كبيرة
2	واقع سياسات أمن نظم المعلومات	3.70	0.80	74.0	3	كبيرة
الدرجة الكلية		4.25	0.55	85.0		كبيرة

تشير البيانات الواردة في الجدول (6) أن مدى التزام الموظفين بسياسات امن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل كان بدرجة كبيرة، إذ بلغ المتوسط الحسابي للدرجة الكلية لمدى التزام الموظفين (4.25)، وبنسبة مئوية بلغت (85.0%).

وقد جاء مجال "المعرفة في أمن نظم المعلومات" في المركز الأول، بمتوسط حسابي بلغ (4.55)، ونسبة مئوية بلغت (91.0%)، وجاء مجال "مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة" في المركز الثاني، بمتوسط حسابي بلغ (4.50)، ونسبة مئوية بلغت (90.0%)، وجاء مجال " واقع سياسات أمن نظم المعلومات" في المركز الثالث، بمتوسط حسابي بلغ (3.70)، ونسبة مئوية بلغت (74.0%).

أما فيما يتعلق بمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة لكل مجال من مجالاته، فقد استخرجت المتوسّطات الحسابيّة والانحرافات المعيارية والأوزان النسبية لكل مجال على النحو الآتي:

أولًا: المعرفة في أمن نظم المعلومات، ويبينها الجدول (7):

الجدول (7): المتوسطات الحسابية والانحرافات المعيارية والأوزان لمدى المعرفة في أمن نظم المعلومات، مرتبة تنازليًا

رقم الفقرة في الاستبانة	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي %	الترتيب	درجة الموافقة
2	على دراية تامة بمخاطر مشاركة كلمات المرور الخاصة بي وامتنع عن مشاركتها مع الآخرين.	4.85	0.41	97.0	1	كبيرة
3	على وعي تام بمخاطر تسريب أو مشاركة البيانات الخاصة بالمؤسسات مع جهات خارجية دون إذن أو تصريح من الجهات ذات العلاقة.	4.68	0.60	93.6	2	كبيرة
1	ادرك تماما المخاطر الأمنية المرتبطة بسوء استخدام نظم المعلومات.	4.63	0.59	92.6	3	كبيرة
4	من واجبي الإبلاغ عن أي حدث ذو علاقة بنظم المعلومات مثل هجمة فيروسية أو تسريب بيانات أو حجب خدمة أو غيرها من المخاطر.	4.56	0.64	91.2	4	كبيرة
6	اقوم بالخدمات المخولة لي حسب صلاحياتي المتاحة لي من مدير النظام ولا أحاول التعدي على صلاحيات الغير باستخدام كلمات مرورهم أو أجهزتهم الخاصة.	4.48	0.64	89.6	5	كبيرة
5	اقوم باستخدام كلمات مرور قوية صعبة التخمين واقوم بتغييرها على نحو دوري كل 6 شهور على الأقل.	4.12	0.80	82.4	6	كبيرة
الدرجة الكلية للمعرفة بأمن نظم المعلومات		4.55	0.61	91.0	كبيرة	

تشير المعطيات الواردة في الجدول (7) أن درجة المعرفة بأمن نظم المعلومات لدى أفراد عينة الدراسة كان بدرجة كبيرة، إذ بلغ المتوسط الحسابي للدرجة الكلية للمعرفة بأمن نظم المعلومات (4.55) ونسبة مئوية (91.0%). وقد تراوحت المتوسطات الحسابية ما بين (4.12–4.85).

ويتضح من الجدول (7) أن الفقرة (على دراية تامة بمخاطر مشاركة كلمات المرور الخاصة بي وامتنع عن مشاركتها مع الاخرين) قد حصلت على أعلى درجة موافقة بالنسبة للمعرفة بأمن نظم المعلومات، وقد جاءت بدرجة موافقة كبيرة.

في حين أن الفقرة (أقوم باستخدام كلمات مرور قوية صعبة التخمين وأقوم بتغييرها على نحو دوري كل 6 شهور على الاقل) قد حصلت على أقل درجة موافقة بالنسبة للمعرفة بأمن نظم المعلومات، وقد جاءت بدرجة موافقة كبيرة.

و قد اتفقت هذه الدراسة مع دراسة (يونس، 2017) و(عبد الواحد، 2015) بإدراك العاملين في الجامعات الفلسطينية بأهمية سياسات أمن نظم المعلومات وفاعليتها، حيث أشارت الدراسة هنا إلى أن معرفة العاملين في جامعة الخليل بسياسات أمن المعلومات كبيرة. وهذا لا ينفي الحاجة إلى تطوير المعرفة في بعض الجوانب من خلال التدريب والمتابعة. وتعزى هذه النتيجة من وجهة نظر الباحث إلى الإجراءات التي اتبعتها جامعة الخليل في السنوات العشر الأخيرة والمتمثلة بالاعتماد الكبير على التكنولوجيا في التعليم. حيث قامت الجامعة بتطوير بيئة الكترونية مساندة للتعليم الوجاهي وقامت بعمل دورات تدريبية مكثفة

للموظفين للإفادة القصوى من هذه التكنولوجيا. (Hasasneh & Moreb , 2013)

ثانيًا: واقع سياسات أمن نظم المعلومات، ويبينها الجدول (8):

الجدول (8): المتوسطات الحسابية والانحرافات المعيارية والأوزان لواقع سياسات أمن نظم المعلومات، مرتبة تنازليًا

رقم الفقرة في الاستبانة	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي %	الترتيب	درجة الموافقة
1	يوجد سياسات متبعة عند تزويد الموظف بإسم المستخدم وكلمة المرور تتم من خلال دائرة شؤون الموظفين ودائرة نظم المعلومات.	4.03	0.93	80.6	1	كبيرة
8	توظف المؤسسة التقنيات اللازمة لحماية نظم المعلومات من خلال برامج مضادة للفيروسات وحماية الشبكة وكشف التسلل.	4.02	0.97	80.4	2	كبيرة
7	تمنع المؤسسة استخدام البرمجيات المقرصنة على أجهزتها.	3.71	1.26	74.2	3	كبيرة
4	هناك تعليمات واضحة باستخدام مواقع التواصل الاجتماعي والبريد الالكتروني الخاص بالمؤسسة.	3.66	0.97	73.2	4	متوسطة
9	توفر المؤسسة تدريب وتوعية للموظفين حول سياسات المؤسسة الخاصة بأمن المعلومات من خلال ورش عمل ودورات تدريبية.	3.66	1.04	73.2	5	متوسطة
2	يمنع الموظف من تعديل أو تنزيل البرامج على جهازه المكتبي أو المحمول دون الرجوع لدائرة تكنولوجيا المعلومات.	3.63	1.14	72.6	6	متوسطة
3	هناك تعليمات واضحة لإستخدام الإنترنت السلكي واللاسلكي في أثناء العمل.	3.61	1.12	72.2	7	متوسطة
5	يتم توزيع التعليمات والسياسات الخاصة بأمن نظم المعلومات على نحو دوري حسب الإجراءات المعتمدة في المؤسسة بحيث يعرف كل موظف هذه السياسات.	3.60	1.07	72.0	8	متوسطة
6	يوجد نظام عقوبات خاص بمخالفة سياسات الأمان في المؤسسة بحيث يعرف كل موظف العقوبة حسب المخالفة التي ارتكبها.	3.41	1.15	68.2	9	متوسطة
الدرجة الكلية لواقع سياسات أمن نظم المعلومات		3.70	1.07	74.0	كبيرة	

تشير المعطيات الواردة في الجدول (8) أن واقع سياسات أمن نظم المعلومات لدى أفراد عينة الدراسة كان إيجابيا بدرجة كبيرة، إذ بلغ المتوسط الحسابي للدرجة الكلية واقع سياسات أمن نظم المعلومات (3.70) ونسبة مئوية (74.0%). وقد تراوحت المتوسطات الحسابية ما بين (3.41-4.03).

ويتضح من الجدول (8) أن الفقرة (يوجد سياسات متبعة عند تزويد الموظف باسم المستخدم وكلمة المرور تتم من خلال دائرة شؤون الموظفين ودائرة نظم المعلومات) قد حصلت على أعلى درجة موافقة بالنسبة لواقع سياسات أمن نظم المعلومات، وقد جاءت بدرجة موافقة كبيرة.

في حين أن الفقرة (يوجد نظام عقوبات خاص بمخالفة سياسات الامان في المؤسسة بحيث يعرف كل موظف العقوبة حسب المخالفة التي ارتكبها) قد حصلت على أقل درجة موافقة بالنسبة لواقع سياسات أمن نظم المعلومات، وقد جاءت بدرجة موافقة متوسطة.

و قد اتفقت هذه الدراسة مع (يونس، 2017) من ناحية التأكيد على أهمية وجود سياسات أمن نظم المعلومات في المؤسسات السورية، مع التأكيد على أن واقع سياسات أمن نظم المعلومات في جامعة الخليل أفضل مما اشارت اليه الدراسة في المؤسسات

السورية. وقد اختلفت هذه الدراسة مع دراسة (Jorro, 2011) التي يشير فيها الى تدني تطبيق سياسات أمن نظم المعلومات في مؤسسات الحكومة الاثيوبية. وتعزى هذه النتيجة إلى الإعتمادية الكبيرة على نظام التعليم الالكتروني في جامعة الخليل التي تستوجب تأمين كافة العمليات وخاصة الحساسة منها مثل نظام العلامات والدفع الإلكتروني. كما أن وجود قسم أمن وحماية شبكات الحاسوب ضمن كلية تكنولوجيا المعلومات في جامعة الخليل كان له الأثر الكبير في إلقاء الضوء على تأمين الإجراءات الإلكترونية بما فيها وضع وتطبيق سياسات الأمان لنظم المعلومات المستخدمة.

ثالثًا: مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة، ويبينها الجدول (9):

الجدول (9): المتوسطات الحسابية والانحرافات المعيارية والأوزان لمدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة، مرتبة تنازليًا

رقم الفقرة في الاستبانة	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي %	الترتيب	درجة الموافقة
1	بالنسبة الي فإن الالتزام بسياسات أمن المعلومات هو ضروري ومفيد لي وللمؤسسة.	4.60	0.63	92.0	1	كبيرة
2	لدي النية بالإلتزام بسياسات المؤسسة في مجال أمن المعلومات.	4.59	0.53	91.8	2	كبيرة
3	لدى النية للحفاظ على مصادر المؤسسة الإلكترونية حسب ما هو موضح في سياسات أمن نظم المعلومات.	4.52	0.62	90.4	3	كبيرة
4	لدي العزم على تحمل مسؤولياتي تجاه سياسات أمن نظم المعلومات في المؤسسة والعمل على تطويرها في المستقبل.	4.45	0.68	89.0	4	كبيرة
5	لدي قناعة تامة بأن عدم التزامي بسياسات أمن المعلومات في المؤسسة سيعرضني للمسؤولية بناء على ما هو موضح في تلك السياسات.	4.36	0.74	87.2	5	كبيرة
الدرجة الكلية مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة		4.50	0.64	90.0	كبيرة	

تشير المعطيات الواردة في الجدول (9) أن مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة لدى أفراد عينة الدراسة كان بدرجة كبيرة، إذ بلغ المتوسط الحسابي للدرجة الكلية لمدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة (4.50) ونسبة مئوية (90.0%). وقد تراوحت المتوسطات الحسابية ما بين (4.36-4.60).

ويتضح من الجدول (9) أن الفقرة (بالنسبة الي فان الالتزام بسياسات امن المعلومات هو ضروري ومفيد لي وللمؤسسة) قد حصلت على أعلى درجة موافقة بالنسبة لمدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة، وقد جاءت بدرجة موافقة كبيرة.

في حين أن الفقرة (لدي قناعة تامة بان عدم التزامي بسياسات امن المعلومات في المؤسسة سيعرضني للمسؤولية بناء على ما هو موضح في تلك السياسات) قد حصلت على أقل درجة موافقة بالنسبة لمدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة، وقد جاءت بدرجة موافقة كبيرة.

و هذه النتائج تتفق ودراسة (نبي، مرزا، و الغثبر، 2010) التي تشير الى ان غالبية المؤسسات في المملكة العربية السعودية تمتلك سياسات امن نظم معلومات وتقوم بعمل مراجعة دورية لها. وهو ما يتفق مع توصية (الصاحب، 2013) حول سياسات أمن نظم المعلومات في جامعة بوليتكنك فلسطين والإجراءات الواجب اتباعها لإعتماد وتطبيق تلك السياسات. وتعزى هذه النتيجة إلى اهتمام الإدارة العليا بجامعة الخليل في الإستثمار في تكنولوجيا المعلومات وتوفير التكنولوجيا الآمنة لتنفيذ العمليات المختلفة. من هنا فقد قامت الإدارة باتخاذ خطوات متدرجة اشتملت على توفير التدريبات اللازمة لكافة الموظفين ضمن برنامج تدريبي، وقد تخلل البرنامج عقد ندوات ومحاضرات وورش عمل توعية في مجال أمن نظم المعلومات. بعدها تم تعميم السياسات على

الموظفين مع المتابعة المستمرة لتطبيق تلك السياسات.

من الجدير ذكره بان هذه النتائج لا تتفق مع نتائج (Jorro، 2011) التي تشير إلى إنخفاض مستوى الجهوزية لدى المؤسسات الاثيوبية تجاه قضايا أمن نظم المعلومات. وقد يعزى هذه الإختلاف إلى سياسات الحكومة الفلسطينية بتبني الحلول التكنولوجية المتقدمة في تقديم الخدمات للجمهور وتشجيع كافة القطاعات للإستثمار في مجال التكنولوجيا وحمايتها من خلال سياسات أمن نظم المعلومات.

السؤال الثاني: هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغيرات (الجنس، والمؤهل العلمي، والخبرات العلمية، والفئة العمرية)؟

وانبثق عنه الفرضيات الصفرية من (1–4) الآتية:

الفرضية الصفرية الأولى: لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الجنس.

لفحص الفرضية الصفرية الأولى، استخدم اختبار (ت) للعينات المستقلة (Independent-Sample t-test) لإيجاد الفروق بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الجنس.

الجدول (10) نتائج اختبار (ت) (Independent- Sample t-test) لتعرُّف الفروق بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الجنس.

المتغير	الجنس	التكرارات	المتوسط الحسابي	الانحراف المعياري	قيمة ت المحسوبة	الدلالة الإحصائية
المعرفة في أمن نظم المعلومات	ذكر	85	4.54	0.40	0.90	0.37
	أنثى	19	4.62	0.25		
واقع سياسات أمن نظم المعلومات	ذكر	85	3.67	0.85	1.05	0.30
	أنثى	19	3.88	0.50		
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	ذكر	85	4.48	0.49	0.89	0.38
	أنثى	19	4.59	0.40		
الدرجة الكلية	ذكر	85	4.13	0.53	1.19	0.24
	أنثى	19	4.28	0.24		

* *دالة إحصائيًا عند مستوى دلالة (0.01)، * دالة إحصائيًا عند مستوى دلالة (0.05)، درجات الحرية = 98

تشير النتائج كما هو موضح في الجدول (10) إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الجنس في الدرجة الكلية وفي جميع مجالات الاستبانة، حيث كانت جميع قيم الدلالة الإحصائية المحسوبة للدرجة الكلية وللمجالات أكبر من (0.05). وبهذه النتيجة تقبل الفرضية الصفرية الأولى.

الفرضية الصفرية الثانية: لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي.

لفحص الفرضية الصفرية الثانية، تم إيجاد المتوسطات الحسابية والانحرافات المعيارية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي، وذلك كما هو موضح في الجدول (11).

الجدول (11): الأعداد والمتوسطات الحسابية والانحرافات المعيارية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي

المتغير	المؤهل العلمي	العدد	المتوسط الحسابي	الانحراف المعياري
المعرفة في أمن نظم المعلومات	دبلوم فأقل	8	4.69	0.19
	بكالوريوس	65	4.59	0.38
	ماجستير	15	4.47	0.39
	دكتوراة	16	4.43	0.39
	المجموع	104	4.55	0.37
واقع سياسات أمن نظم المعلومات	دبلوم فأقل	8	4.13	0.56
	بكالوريوس	65	3.86	0.72
	ماجستير	15	3.54	0.97
	دكتوراة	16	3.03	0.65
	المجموع	104	3.70	0.80
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	دبلوم فأقل	8	4.73	0.28
	بكالوريوس	65	4.48	0.48
	ماجستير	15	4.63	0.49
	دكتوراة	16	4.35	0.49
	المجموع	104	4.50	0.47
الدرجة الكلية	دبلوم فأقل	8	4.44	0.31
	بكالوريوس	65	4.23	0.47
	ماجستير	15	4.09	0.54
	دكتوراة	16	3.78	0.44
	المجموع	104	4.16	0.49

يتضح من الجدول (11) وجود فروق ظاهرية بين المتوسطات الحسابية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي. وللتحقق من دلالة الفروق استخدم اختبار تحليل التباين الأحادي (One Way Anova)، كما هو موضح في الجدول (12):

الجدول (12) نتائج اختبار تحليل التباين الأحادي (One Way Anova) لتعرُّف الفروق في مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي

المتغير	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف المحسوبة	مستوى الدلالة الإحصائية
المعرفة في أمن نظم المعلومات	بين المجموعات	0.59	3	0.20	1.41	0.24
	داخل المجموعات	13.87	100	0.14		
	المجموع	14.46	103	------		
واقع سياسات أمن نظم المعلومات	بين المجموعات	10.64	3	3.55	6.47**	0.00
	داخل المجموعات	54.80	100	0.55		
	المجموع	65.45	103	------		
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	بين المجموعات	1.02	3	0.34	1.54	0.21
	داخل المجموعات	22.18	100	0.22		
	المجموع	23.20	103	------		
الدرجة الكلية	بين المجموعات	3.39	3	1.13	5.25**	0.00
	داخل المجموعات	21.53	100	0.22		
	المجموع	24.92	103	------		

** دالة إحصائيًا عند مستوى دلالة (0.01). * دالة إحصائيًا عند مستوى دلالة (0.05)

يتضح من البيانات الموضحة في الجدول (12) وجود فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05\geq\alpha$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي، حيث كانت قيمة الدلالة الإحصائية للدرجة الكلية (0.00) وهي أصغر من (0.05) ودالة إحصائيًا. كذلك ظهرت فروق دالة إحصائيًا في مجال واقع سياسات أمن نظم المعلومات.

بينما لم تظهر فروق دالة إحصائيًا في متوسطات مجال المعرفة في أمن نظم المعلومات، ومجال مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة.

ولإيجاد مصدر الفروق، استخدم اختبار شيفيه (Scheffe) للمقارنات الثنائية البعدية للفروق بين متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي، وذلك كما هو واضح من خلال الجدول (13).

الجدول (13): نتائج اختبار شيفيه (Scheffe) للمقارنات الثنائية البعدية للفروق بين متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي

المجال	المقارنات	المتوسط الحسابي	بكالوريوس	ماجستير	دكتوراة
واقع سياسات أمن نظم المعلومات	دبلوم فأقل	4.13	------	------	1.10*
	بكالوريوس	3.86		------	0.83*
	ماجستير	3.54	------		0.51*
	دكتوراة	3.03	------	------	
الدرجة الكلية	دبلوم فأقل	4.44		------	0.67*
	بكالوريوس	4.23		------	0.45*
	ماجستير	4.09	------		0.31*
	دكتوراة	3.78	------	------	

* الفرق في المتوسطات دال إحصائيًا عند (0.05)

تشير المقارنات الثنائية البعدية وفق الجدول (13) إلى أن الفروق في متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل، ظهرت بين الذين مؤهلهم العلمي دبلوم فأقل، وبكالوريوس وماجستير من جهة وبين الذين مؤهلهم العلمي دكتوراة من جهة أخرى، وكانت الفروق لصالح أصحاب المؤهلات العلمية دبلوم فأقل، وبكالوريوس وماجستير الذين كان التزامهم بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية أعلى.

و تتعارض هذه النتيجة مع دراسة (Muhire، 2012) التي تشير إلى أن المستوى العلمي له أثر إيجابي على التزام الموظفين بسياسات أمن نظم المعلومات في المؤسسات، حيث أشارت إلى أثر المستوى العلمي في رفع الوعي تجاه أمن المعلومات وبالتالي الإلتزام بسياسات أمن نظم المعلومات. وقد يعزى التعارض إلى أن معظم موظفي جامعة الخليل من حملة شهادة الماجستير فما دون هم حديثي التخرج، ما يعني أن غالبيتهم من مستخدمي التكنولوجيا على نحو كبير؛ الأمر الذي أدى إلى رفع مستوى الوعي لديهم حول أمن المعلومات والسياسات المتبعة.

الفرضية الصفرية الثالثة: لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05\geq\alpha$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الخبرة العملية.

لفحص الفرضية الصفرية الثالثة، تم إيجاد المتوسطات الحسابية والانحرافات المعيارية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الخبرة العملية، وذلك كما هو موضح في الجدول (14).

الجدول (14): الأعداد والمتوسطات الحسابية والانحرافات المعيارية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير المؤهل العلمي

المتغير	الخبرة العلمية	العدد	المتوسط الحسابي	الانحراف المعياري
المعرفة في أمن نظم المعلومات	أقل من 5 سنوات	47	4.60	0.34
	من 5–9 سنوات	18	4.43	0.46
	من 10–14 سنة	27	4.53	0.35
	من 15–19 سنة	12	4.63	0.40
	المجموع	104	4.55	0.37
واقع سياسات أمن نظم المعلومات	أقل من 5 سنوات	47	3.95	0.57
	من 5–9 سنوات	18	3.45	0.91
	من 10–14 سنة	27	3.39	0.94
	من 15–19 سنة	12	3.84	0.77
	المجموع	104	3.70	0.80
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	أقل من 5 سنوات	47	4.50	0.47
	من 5–9 سنوات	18	4.54	0.57
	من 10–14 سنة	27	4.45	0.49
	من 15–19 سنة	12	4.55	0.30
	المجموع	104	4.50	0.47
الدرجة الكلية	أقل من 5 سنوات	47	4.28	0.39
	من 5–9 سنوات	18	4.02	0.58
	من 10–14 سنة	27	4.00	0.57
	من 15–19 سنة	12	4.25	0.42
	المجموع	104	4.16	0.49

يتضح من الجدول (14) وجود فروق ظاهرية بين المتوسطات الحسابية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الخبرة العلمية. وللتحقق من دلالة الفروق استخدم اختبار تحليل التباين الأحادي (One Way Anova)، كما هو موضح في الجدول (15):

الجدول (15) نتائج اختبار تحليل التباين الأحادي (One Way Anova) لتعرُّف الفروق في مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الخبرة العلمية

المتغير	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف المحسوبة	مستوى الدلالة الإحصائية
المعرفة في أمن نظم المعلومات	بين المجموعات	0.45	3	0.15	1.08	0.36
	داخل المجموعات	14.01	100	0.14		
	المجموع	14.46	103	------		
واقع سياسات أمن نظم المعلومات	بين المجموعات	6.90	3	2.30	3.93**	0.01
	داخل المجموعات	58.55	100	0.59		
	المجموع	65.45	103	------		
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	بين المجموعات	0.13	3	0.04	0.18	0.91
	داخل المجموعات	23.07	100	0.23		
	المجموع	23.20	103	------		
الدرجة الكلية	بين المجموعات	1.89	3	0.63	2.73*	0.04
	داخل المجموعات	23.03	100	0.23		
	المجموع	24.92	103	------		

** دالة إحصائيًا عند مستوى دلالة (0.01). * دالة إحصائيًا عند مستوى دلالة (0.05)

يتضح من البيانات الموضحة في الجدول (15) وجود فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05\geq\alpha$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الخبرة العلمية، حيث كانت قيمة الدلالة الإحصائية للدرجة الكلية (0.04) وهي أصغر من (0.05) ودالة إحصائيًا. كذلك ظهرت فروق دالة إحصائيًا في مجال واقع سياسات أمن نظم المعلومات.

بينما لم تظهر فروق دالة إحصائيًا في متوسطات مجال المعرفة في أمن نظم المعلومات، ومجال مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة.

ولإيجاد مصدر الفروق، استخدم اختبار شيفيه (Scheffe) للمقارنات الثنائية البعدية للفروق بين متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الخبرة العلمية، وذلك كما هو واضح من خلال الجدول (16).

الجدول (16): نتائج اختبار شيفيه (Scheffe) للمقارنات الثنائية البعدية للفروق بين متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الخبرة العلمية

المجال	المقارنات	المتوسط الحسابي	من 5–9 سنوات	من 10–14 سنة	من 15–19 سنة
واقع سياسات أمن نظم المعلومات	أقل من 5 سنوات	3.95	0.50*	*0.56	------
	من 5–9 سنوات	3.45		------	------
	من 10–14 سنة	3.39	------		------
	من 15–19 سنة	3.84	------	------	
الدرجة الكلية	أقل من 5 سنوات	4.28	0.26*	0.28*	------
	من 5–9 سنوات	4.02		------	------
	من 10–14 سنة	4.00	------		------
	من 15–19 سنة	4.25	------	------	

* الفرق في المتوسطات دال إحصائيًا عند (0.05)

تشير المقارنات الثنائية البعدية وفق الجدول (16) إلى أن الفروق في متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الخبرة العملية، ظهرت بين الذين خبرتهم العملية أقل من 5 سنوات من جهة وبين الذين خبرتهم العملية (من 5–9) و(من 10–14) سنة جهة أخرى، وكانت الفروق لصالح أصحاب الخبرة العلمية الأقل من 5 سنوات الذين كان التزامهم بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية أعلى.

و يعزى السبب بذلك إلى أن معظم الموظفين ذوي الخبرة العملية المتدنية (5 سنوات فاقل) هي من حديثي التخرج الذين استخدموا التكنولوجيا على نحو كبير في حياتهم العملية، ما دفعهم إلى تعرُّف مخاطر التكنولوجيا وبالتالي الالتزام بسياسات أمن نظم المعلومات للتقليل من المخاطر المرتبطة بها.

الفرضية الصفرية الرابعة: لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05\geq\alpha$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية.

لفحص الفرضية الصفرية الرابعة، تم إيجاد المتوسطات الحسابية والانحرافات المعيارية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية، وذلك كما هو موضح في الجدول (17).

الجدول (17): الأعداد والمتوسطات الحسابية والانحرافات المعيارية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية

المتغير	الفئة العمرية	العدد	المتوسط الحسابي	الانحراف المعياري
المعرفة في أمن نظم المعلومات	30-18سنة	51	4.58	0.36
	45-31سنة	39	4.57	0.36
	46 سنة فأكبر	14	4.39	0.44
	المجموع	104	4.55	0.37
واقع سياسات أمن نظم المعلومات	30-18سنة	51	3.91	0.65
	45-31سنة	39	3.62	0.90
	46 سنة فأكبر	14	3.19	0.75
	المجموع	104	3.70	0.80
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	30-18سنة	51	4.50	0.49
	45-31 سنة	39	4.53	0.51
	46 سنة فأكبر	14	4.44	0.33
	المجموع	104	4.50	0.47
الدرجة الكلية	30-18سنة	51	4.26	0.43
	45-31سنة	39	4.13	0.55
	46 سنة فأكبر	14	3.86	0.43
	المجموع	104	4.16	0.49

يتضح من الجدول (17) وجود فروق ظاهرية بين المتوسطات الحسابية لمدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية. وللتحقق من دلالة الفروق استخدم اختبار تحليل التباين الأحادي (One Way Anova)، كما هو موضح في الجدول (18):

الجدول (18) نتائج اختبار تحليل التباين الأحادي (One Way Anova) لتعرُّف الفروق في مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية

المتغير	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف المحسوبة	مستوى الدلالة الإحصائية
المعرفة في أمن نظم المعلومات	بين المجموعات	0.42	2	0.21	1.50	0.23
	داخل المجموعات	14.04	101	0.14		
	المجموع	14.46	103	------		
واقع سياسات أمن نظم المعلومات	بين المجموعات	6.03	2	3.01	5.12**	0.01
	داخل المجموعات	59.42	101	0.59		
	المجموع	65.45	103	------		
مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة	بين المجموعات	0.08	2	0.04	0.17	0.85
	داخل المجموعات	23.12	101	0.23		
	المجموع	23.20	103	------		
الدرجة الكلية	بين المجموعات	1.73	2	0.86	3.76*	0.03
	داخل المجموعات	23.19	101	0.23		
	المجموع	24.92	103	------		

** دالة إحصائيًا عند مستوى دلالة (0.01). * دالة إحصائيًا عند مستوى دلالة (0.05)

يتضح من البيانات الموضحة في الجدول (18) وجود فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطات التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية، حيث كانت قيمة الدلالة الإحصائية للدرجة الكلية (0.03) وهي أصغر من (0.05) ودالة إحصائيًا. كذلك ظهرت فروق دالة إحصائيًا في مجال واقع سياسات أمن نظم المعلومات.

بينما لم تظهر فروق دالة إحصائيًا في متوسطات مجال المعرفة في أمن نظم المعلومات، ومجال مدى التزام الموظف بسياسات أمن المعلومات داخل المؤسسة.

ولإيجاد مصدر الفروق، استخدم اختبار شيفيه (Scheffe) للمقارنات الثنائية البعدية للفروق بين متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية، وذلك كما هو واضح من خلال الجدول (19).

الجدول (19): نتائج اختبار شيفيه (Scheffe) للمقارنات الثنائية البعدية للفروق بين متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية

المجال	المقارنات	المتوسط الحسابي	31-45سنة	46 سنة فأكبر
واقع سياسات أمن نظم المعلومات	18-30سنة	3.91	------	*0.72
	31-45سنة	3.62		0.42*
	46 سنة فأكبر	3.19	------	
الدرجة الكلية	18-30سنة	4.26	------	0.39*
	31-45سنة	4.13		0.27*
	46 سنة فأكبر	3.86	------	

* الفرق في المتوسطات دال إحصائيًا عند (0.05)

تشير المقارنات الثنائية البعدية وفق الجدول (19) إلى أن الفروق في متوسطات مدى التزام الموظفين بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية – دراسة حالة جامعة الخليل تبعًا لمتغير الفئة العمرية، ظهرت بين الفئات العمرية (18–30) و(31–45) من جهة وبين الفئة العمرية (46 سنة فأكثر) من جهة أخرى، وكانت الفروق لصالح الفئات العمرية (18–30) و(31–45) الذين كان التزامهم بسياسات أمن المعلومات في مؤسسات التعليم العالي الفلسطينية أعلى.

و تعزى أسباب هذا الإختلاف إلى أن الموظفين من ذوي الفئات العمرية العالية هم من الذين تخرجوا قديما ولم يستخدموا التكنولوجيا على نحو واسع مقارنة مع ذوي الفئات العمرية القليلة، وبالتالي يميل هؤلاء إلى الإبتعاد عن استخدام التكنولوجيا وبالتالي يؤثر سلبا على مدى التزامهم بسياسات أمن نظم المعلومات.

التوصيات

في ضوء ما تم عرضه من نتائج الدراسة، التي يمكن تلخيصها في النقاط التالية:

1) معرفة موظفي جامعة الخليل بتكنولوجيا المعلومات عالية، مع وجود حاجة الى تطوير المعرفة المستمر من خلال التدريب والمتابعة.
2) واقع سياسات أمن نظم المعلومات في جامعة الخليل متقدم، مع الحاجة إلى التقييم الدوري والتعديل بناء على التقييم.
3) أبدى موظفو جامعة الخليل أهمية كبيرة تجاه الإلتزام بسياسات أمن نظم المعلومات في جامعة الخليل

فان الباحث يوصي بما يلي:

1) ضرورة إشراك كافة الموظفين في برامج تعليمية ودورات تدريبية حول تكنولوجيا وأمن المعلومات، ليكونوا على اطلاع دائم بوسائل التكنولوجيا وطرق الإستخدام الآمن لها.
2) ضرورة عمل تقييم دوري لسياسات أمن نظم المعلومات للتحقق من ملائمتها للتطور التكنولوجي والعمل على تحديثها

عند اللزوم.

3) ضرورة متابعة التزام الموظفين بتطبيق سياسات أمن نظم المعلومات وتفعيل نظام العقوبات في حال عدم الإلتزام، مع ضرورة توفير نسخة الكترونية لسياسات أمن المعلومات تكون متاحة لكافة الموظفين، ليتسنى لهم مراجعتها والعمل بموجبها.

و من خلال معرفة الباحث في مجال أمن نظم المعلومات فإننا نوصي أيضا بما يلي:

1) ضرورة توفير موظف دعم تقني للإجابة عن استفسارات الموظفين بخصوص سياسات أمن المعلومات وتوفير الارشاد لهم.

2) توفير آلية للتعاون المشترك بين كافة مؤسسات التعليم العالي الفلسطينية لتبادل الخبرات حول سياسات أمن نظم المعلومات وسبل تطبيقها وتطويرها.

3) إعتماد مرجعية عالمية متخصصة في مجال سياسات أمن نظم المعلومات والعمل على تحسين واقع سياسات نظم المعلومات بناءًا على المعايير العالمية المتبعة.

4) توفير آلية للتعاون مع جامعات عالمية ذات خبرة واسعة وتجارب عريقة في هذا المجال للإفادة من تجاربهم.

المصادر والمراجع

بيت المال، حمزة. (2014) الإعلام ودوره في التوعية بالجرائم عبر وسائل التواصل الاجتماعي. ملتقى: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، 1 – 22.

حسن الشهري. (2009). نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية. المجلة العربية للدراسات الأمنية والتدريب – جامعة نايف العربية للعلوم الأمنية، 513 – 526.

بحر، عبد الرحمن (1999). معوقات التحقيق في جرائم الانترنت. جامعة نايف العربية للعلوم الأمنية. الرياض: المكتبة الأمنية.

عوض، احمد، & خلف، امير. (2003). مقدمة في نظم التشفير وأمنية المعلومات. الخرطوم: منشورات مركز الدراسات الاستراتيجية.

عرفان نبي، عبد الرحمن مزرا، خالد الغثبر. (2008) رسالة عملية حول امن المعلومات في المنظمات السعودية، المملكة العربية السعودية: جامعة الملك سعود، مركز التميز لامان المعلومات.

محمد عبيد الكعبي. (2009). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت. القاهرة: دار النهضة العربية.

ذياب موسى البداينة. (2014). الجرائم الالكترونية: المفهوم والأسباب. الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، (الصفحات 3 – 28). Amman.

تركي المويشير. (2012). بناء نموذجي امني لمكافحة الجرائم الإلكترونية وقياس فاعليته. الرياض: مركز البحوث والدراسات – جامعة نايف العربية للعلوم الأمنية.

موسى، مصطفى. (2008). التحقيق الجنائي في الجرائم الالكترونية. ط1، . القاهرة: دار النهضة العربية.

داود، حسن. (2004). امن شبكات المعلومات. الرياض: معهد الإدارة العامة – مركز البحوث.

يونس، رؤي. (2017). دراسة واقع إدارة أمن نظم المعلومات في المؤسسات السورية. مجلة جامعة البعث المجلد 93 العدد 3، 61-90.

الأمم المتحدة. (1992). تنمية القدرات التكنولوجية الذاتية:دور المؤسسات المالية المتخصصة. (ا. المتحدة، Ed.) القاهرة، جمهورية مصر العربية: الاسكوا.

هروال، نبيلة. (2007). الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات. الإسكندرية: دار الفكر الجامعي.

شهوان، وسيم. (2018). دور المؤسسة الأمنية في الحد من الجرائم المستحدثة في الضفة الغربية من وجهة نظر ذوي الاختصاص. جامعة القدس ، عمادة الدراسات العليا. القدس: مجلة جامعة القدس.

غيطاس، جمال.(2007). عصر المعلومات: القادم مذهل اكثر. القاهرة: مركز الخبرات المهنية.

الدنف، ايمن.(2013). واقع ادارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها. رسالة ماجستير. فلسطين، غزة: الجامعة الاسلامية.

ياسين، سعد. (2009). اساسيات نظم المعلومات الادارية وتكنولوجيا المعلومات. عمان: دار المناهج.

مصطفى، شعيب. (1998). أثر المعرفة التقانية والسلوك الأبداعي في مستوى أداء بعض المنظمات الصناعية العراقية. جامعة الموصل
عبدالملك، عماد. (2012). جرائم الكمبيوتر والانترنت. الإسكندرية: دار المطبوعات الجامعية.
الجهاز المركزي للاحصاء الفلسطيني. (08 08، 2019). تاريخ الاسترداد 17 10، 2019، من ItemID=3529&http://www.pcbs.gov.ps/postar.aspx?lang=ar.
الشرطة الفلسطينية. (31 03، 2019). تاريخ الاسترداد 17 10، 2019، من http://www.palpolice.ps: http://www.palpolice.ps/ar/content/726833.html
الصاحب، محمود. (2013). سياسة امن المعلومات في الجامعات – حالة دراسية. Journal Cybrarians عدد 33.
الشبلي، هيثم. (2009). إدارة مخاطر الاحتيال في قطاع الاتصالات. عمان: دار صفاء للنشر والتوزيع.
بسيوني، عبد الحميد. (2007). حماية الحاسبات والشبكات من فيروسات الكمبيوتر والتجسس والملوثات. القاهرة: دار الكتب العلمية للنشر والتوزيع.
الواحد، آن. (2015). سياسات أمن المعلومات وعلاقتها بفاعلية نظم المعلومات الإداايية ي الجامعات الفلسطينية – قطاع غزة. رسالة ماجستير. غزة: جامعة الازهر.
الغثبر، خالد.، & القحطاني، محمد. (2009). امن المعلومات بلغة ميسرة. الرياض: مركز التميز لامن المعلومات– جامعة الملك سعود.
مقراني، قدور. (2016). تقييم مدى مساهمة أمن نظم المعلومات الالكتروني في الحد من مخاطر نظم المعلومات – دراسة حالة مؤسسة اتصالات الجزائر. رسالة ماجستير. الجزائر: جامعة قاصدي ومرباح ورقلة.
القرشي، محمد. (2011). قياس كفاءة سياسات أمن المعلومات – دراسة حالة على شركة في االامارات العربية المتحدة. رسالة ماجستير. ستوكهولم، السويد: جامعة ستوكهولم.
المومني، نهلا. (2010). جرائم المعلومات. عمان: دار الثقافة للنشر والتوزيع.
إبراهيم، خالد.(2009). الجرائم المعلوماتية. الإسكندرية: دار الفكر الجامعي.
العتيبي، سليمان.(2016). دور البحث الجنائي في الكشف عن الجرائم المعلوماتية. أطروحة دكتوراة، جامعة نايف العربية للعلوم الأمنية، قسم الدراسات الأمنية، الرياض.
القحطاني، عبدالله. (2014). تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية. جامعة نايف العربية للعلوم الأمنية. الرياض: المكتبة الأمنية.
الزهراني، سعيد. (2014). أنظمة الجرائم المعلوماتية في دول مجلس التعاون الخليجي، ، الرياض). الرياض: جامعة نايف العربية للعلوم الأمنية.
(2001). الاتفاقية المتعلقة بالجريمة الإلكترونية. بودابست: The Council of Europe.
المشهداني، سرحان. (2001). امن الحاسوب والمعلومات. عمان: دار وائل للطباعة والنشر

References

Al-Janabi, S., & AlShourbaji, I. (2016, 02). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information & Knowledge Management, 15(1), 30.

Andress, J. (2014). The Basics of Information Security. Syngress.

Bourgeois, D., & Bourgeois, D. T. (2014). Information Systems for Business and Beyond. Creative Commons.

Bruijn, H. d., & Janssen, M. (2017, 1). Building cybersecurity awareness: The need for evidence-based framing strategies. (A. Kankanhalli, G. K. Tayi, & A. Zuiderwijk, Eds.) Government Information Quarterly , 34(1), 1 - 7.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness1. MIS Quarterly - Vol:24 , No: 3, 523-548.

Claude, B. (2008). la traduction juridique fondement et méthode. Bruxelles: De Boeck Université.

Dulany, K. M. (2002). security is not just technical. GSEC Practical Assignments - SANS Institute, 1-4.

Easttom, C. (2019). Computer Security Fundamentals. USA: Pearson.

Hare, C. (2001). Information Security Policies, Procedures, and Standards: Establishing an Essential Code of Conduct. USA: Auerbach Publications - CRC Press LLC.

Hasan, M. S., Rahman, R. A., Farah, S., Binti, H., Abdillah, T., & Omar, N. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. Journal of Social Sciences, 11(4), 395 - 404.

Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment. (2020, January 9). Retrieved from ISO - International Standard Organization: https://www.iso.org/standard/61347.html

Hornby. (1974). Oxford Advanced Learns, Dictionary of English. London: Oxford University Press.

Jorro, Y. (2011). Information System Security Audit Readiness Case study: Ethiopian Government Organizations. Master thesis. Stockholm, Sweden: Stockholm University.

Kumar, S., Benigni, M., & Carley, K. M. (2016). The impact of US cyber policies on cyber-attacks trend. 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 1228-1239). Tucson, USA: IEEE.

Loudon, K., & Loudon, J. (2010). Management Information Systems. Managing the Digital Firm. New Jersey: Prentice-Hall inc.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013). Comprehensive Study on Cybercrime. UNITED NATIONS, UNITED NATIONS OFFICE ON DRUGS AND CRIME. New York: UNITED NATIONS OFFICE ON DRUGS AND CRIME.

Maynard, S., Ruighaver, A., & Sandow-Quick, M. (2002). Redefining the Information System Security Policy". IS One World Conference. Las Vegas.

Moallem, A. (2018). Cyber Security Awareness Among College Students. International Conference on Applied Human Factors and Ergonomics. 782, pp. 79 - 87. Orlando, Florida: Springer.

Muhire, B. (2012, 1 5). Employee Compliance with Information Systems Security Policy in Retail Industry. Case: Store Level Employees. Honors Thesis Program in the college of management. Boston, USA: University of Massachusetts Boston.

Pescatore, J. (2019). SANS Top New Attacks and Threat Report. SANS Institute.

Reynolds, G. W. (2014). Ethics in Information Technology. Cengage Learning.

Safa, N. S., Solms, R. V., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers and securoty, Vol: 56, 1-13.

SANS. (2019). Security Awareness Report: The Rising Era of Awareness Training. Retrieved 10 17, 2019, from https://www.sans.org/security-awareness-training/reports/2019-security-awareness-report

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness amongcollege students in

Tamil Nadu. IOP Conference Series: Materials Science and Engineering. 263. IOP Publishing.

Stair, R., & Reynolds, G. (2012). Principles of Information Systems. Boston, USA: CENAGE Learning.

UK Government. (2016). NATIONAL CYBER SECURITY STRATEGY 2016 - 2021. London: Cabinet Office and National security and intelligence.

Whitman, M. E., & Mattord, H. J. (2012). Principles of Information security. Boston, USA: CENAGE learning Inc.

Hasasneh, Nabil and. Moreb ,mohammed. (2013). E-Learning at Hebron University -- A Case Study. 2013 Fourth International Conference on e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity", Manama,.

Amro, Belal. (2018). Cybercrime as a Matter of the Art in Palestine and its Effect on Individuals. International Journal of Wireless and Microwave Technologies(IJWMT), 19 - 26.

The reality and motives for adherence to information security policies in Palestinian higher education institutions – A case study of Hebron University

*Belal Amro**

ABSTRACT

Information systems security is a core factor in the development and using of computer information systems which provides security for the data and privacy for users; and humans are one of the major key players in this field. Some of human behaviors that leads to security breaches in computer information systems include Ignorance, negligence, indifference, and lack of awareness in information security. In this research, we are spotting the light on the importance of information system security policies in higher educational institutions in Palestine – Hebron University case study. The importance of this research lies in knowing the reality of information systems security policies in Palestinian universities and knowing the factors affecting adherence to information security policies such as knowledge of information security, experience, and educational level. The study concluded that the degree of knowledge about the security of information systems and their adherence by the staff of Hebron University was high. The study also concluded that there are statistically significant differences for related to the staff adherence to information systems security policies according to the educational level and experience. The study has recommended the necessity of following up the implementation of information systems security policies, and updating and reviewing them in line with the requirements of the next phase and the tremendous technological development the world is witnessing.

Keywords: Information systems security; security policies; higher education.

* Hebron University, Palestine.

Received on 10/6/2020 and Accepted for Publication on 22/9/2020.