مجلة بحوث الإدارة والاقتصاد
Management & Economics Research Journal
ISSN 2710-8856 (Online)
ISSN 2676-184X (Print)

مجلة بحوث الإدارة والاقتصاد، مجلد 2 عدد 3 (2020)، ص 1-23
Management & Economics Research Journal, Vol. 2 No. 4 (2020), pp. 1-23
https://doi.org/10.48100/merj.v2i3.107
Check for updates

دور عمليات إدارة الموارد البشرية في تحقيق الأمن المعلوماتي: دراسة تطبيقية على الجامعات الحكومية السعودية

معاذ يوسف الذنيبات [1]♦، عدنان عواد الشوابكة [2] خيرو خلف البقور [3]
[1] دكتوراه نظم المعلومات الإدارية، أستاذ مشارك، جامعة الطائف (السعودية)
muath@tu.edu.sa
[2] دكتوراه نظم المعلومات الإدارية، أستاذ مشارك، جامعة الطائف (السعودية)
a_alshawabkeh@yahoo.com
[3] دكتوراه نظم المعلومات الإدارية، أستاذ مشارك، جامعة الطائف (السعودية)
khair15@yahoo.com

تاريخ الاستلام: 2020-03-26 تاريخ القبول: 2020-05-18 تاريخ النشر: 2020-06-21

ملخص:

تهدف هذه الدراسة إلى الكشف واقع مساهمة وحدات إدارة الموارد البشرية في تحقيق الأمن المعلوماتي في الجامعات الحكومية السعودية من خلال فحص مدى التزامها بضوابط المواصفة العالمية لنظام إدارة أمن المعلومات (ISO/IEC 27002:2013).

اعتمدت الدراسة على طرق البحث النوعي، حيث تم تصميم قائمة فحص لجمع البيانات اللازمة للدراسة، باستخدام أسلوب المقابلات شبه المهيكلة، والملاحظة المباشرة، وفحص والوثائق المستخدمة بوحدات إدارة الموارد البشرية، كما تم استخدام أسلوب تحليل الفجوات لتحليل البيانات وفهم مدى امتثال وحدات إدارة الموارد البشرية في الجامعات التي شاركت في الدراسة لضوابط أمن المعلومات التي نصت عليها المواصفة (ISO/IEC 27002:2013).

توصلت الدراسة إلى عدد من النتائج كان من أهمها التزام الجامعات المشاركة في الدراسة بنسب متفاوتة تراوحت بين المتوسط والمرتفع في تطبيق بنود المواصفة العالمية (ISO/IEC 27002:2013) فيما يتعلق بعمليات إدارة الموارد البشرية (قبل التوظيف، واثناء التوظيف، وعمليات ترك الخدمة أو تغير الوظيفة).

في ضوء تلك النتائج قدمت الدراسة عدد من التوصيات التي ترشد الجامعات نحو الالتزام الكامل بمتطلبات تلك المواصفة بهدف رفع مستوى مساهمة عمليات إدارة الموارد البشرية في تحقيق الامن المعلوماتي.

الكلمات المفتاحية: إدارة الموارد البشرية، أمن المعلومات، المواصفة الدولية: ISO/IEC 27002:2013.

تصنيف جال: M15.

♦**المؤلف المراسل:** [Muath@tu.edu.sa]

1. مقدمة

يُنظر إلى الأمن المعلوماتي على أنه التحدي الأبرز الذي يواجه معظم منظمات اليوم، خاصة في ظل تزايد الاعتماد على التعاملات الإلكترونية والتحول نحو المجتمعات الافتراضية وبيئة الأعمال الإلكترونية (Singh & Gupta, 2019)، حيث فرضَ هذا التحول على العديد من المنظمات التركيز على كيفية تأمين التعاملات الإلكترونية من التهديدات والمخاطر التي تواجهها، وماهي العوامل المساعدة أو المثبطة لتحقيق هذه الغاية.

ومن هذا المنطلق اتجه الباحثين في مجال نظم المعلومات المحوسبة نحو دراسة قضايا أمن المعلومات من كافة الجوانب الإدارية والتقنية والتنظيمية والبشرية.. الخ، مستفيدين من التطور التقني والعلمي في هذا المجال وآخذين بعين الاعتبار نتائج البحوث والدراسات التي سبقتهم (Li & S, 2011).

من جانب آخر، يعتبر تحقيق الأمن المعلوماتي في المنظمات مسؤولية مشتركة تشمل جميع المتعاملين مع المنظمة والعاملين والوحدات التنظيمية في المنظمة على اختلاف مستوياتها الإدارية وموقعها في الهيكل التنظيمي، حيث أن كل وحدة تنظيمية تتحمل جزءاً من المسؤولية في تحقيق الأمن المعلوماتي من خلال التزامها بتطبيق بنود سياسة أمن المعلومات في المنظمة والتزامها بتطبيق بنود المعايير الدولية لأمن المعلومات عند تنفيذ عملياتها وإجراءاتها لأداء المهام المطلوبة منها (Ma, Schmidth, & Pearson, 2009).

إدارة الموارد البشرية إحدى الوحدات التنظيمية التي نجدها في كل منظمة بغض النظر عن حجم هذه الوحدة أو موقعها في الهيكل التنظيمي، وقد حظيت بأهمية بارزة نتيجة لأهمية الوظائف والعمليات الادارية التي تمارسها وتأثيرها على باقي وظائف وعمليات المنظمة، فاستقطاب وتأهيل وتدريب وإدامة الموارد البشرية الكفؤة سوف يدعم تحقيق جلَّ أهداف المنظمة الاستراتيجية والتكتيكية والتشغيلية، كما أن عمليات إدارة الموارد البشرية تسعى لحفظ حقوق كل من العاملين والمنظمة بما في ذلك المحافظة على أمن المعلومات(Ansen, 2014).

وانطلاقاً مما سبق، وبسبب نجاح العديد من الهجمات الإلكترونية في التغلب على حلول الأمن التقنية من خلال استغلال نقاط الضعف للعوامل البشرية المرتبطة بالمعرفة والمهارات الأمنية(Daniel, 2019)، فإنه يقع على عاتق إدارة الموارد البشرية مسؤولية مباشرة تجاه تحقيق أمن المعلومات، فقد أشارت دراسة مؤخراً إلى أن 67% من مديري الموارد البشرية في أستراليا يلعبون دورًا في تحديد سياسات الوصول للمعلومات ومنح الصلاحيات للمستخدمين استنادًا إلى أدوار الموظفين، كما أن قسم الموارد البشرية يلعب دورًا رئيسيًا في ضمان تنفيذ سياسات الوصول بشكل صحيح ومنح المستخدمين النهائيين مستوى من التعليم والتدريب بشكل يدعم التزامهم بنود سياسة أمن المعلومات في المنظمة(Kehoe, 2016).

إضافة إلى ذلك فقد أثبتت دراسة (Stewart, 2017) أن الموظفين يلعبون دورًا رئيسيًا في إدارة أمن المعلومات، وبالتالي يجب الانتباه إلى هذا الدور وجعله إيجابياً خاصة في المنظمات التي تعد فيها البيانات قيّمة.

ومن خلال هذا الدور الاستراتيجي لإدارة الموارد البشرية فإنها تلتزم بضمان أن جميع العاملين في المنظمة والمتعاقدين معها على علم ودراية تامة بالمسؤوليات الأمنية المناطة بهم بموجب السياسة الأمنية المطبقة في المنظمة وتعهدهم بالالتزام بكافة بنود تلك السياسة، وكذلك أن يكونوا على علم بالإجراءات التأديبية المتبعة في حال مخالفة بنود سياسة أمن المعلومات من قبل أي من العاملين أو المتعاقدين(Wipawayangkool, 2010).

حيث أثبتت الدراسات أن العاملين الذين لديهم دراية ووعي بسياسة أمن المعلومات المطبقة في المنظمة لديهم مستوى أعلى من ثقافة أمن المعلومات مقارنة مع العاملين الذين ليس لديهم وعي

ومعرفة بسياسة أمن المعلومات، وهذا بحد ذاته يؤثر في تحقيق الأمن المعلوماتي على مستوى المنظمة(Da Veiga, 2016).

ومن جهة أخرى، أثبت الدراسات أهمية تبني المنظمات -بما فيها الجامعات - لمواصفات ومعايير إدارة أمن المعلومات العالمية لتحقيق الأمن المعلوماتي، وعليها أن تلتزم بما أسند لها من واجبات ومسؤوليات أمنية بدقة متناهية تلافياً لإحداث الثغرات الأمنية التي تُستغل للاعتداء على أمنية المعلومات فيها خاصة في ظل العدد المتزايد من الانتهاكات الأمنية التي تعرضت لها مؤسسات التعليم العالي في السنوات الأخيرة (Bongiovanni, 2019).

وبالرغم من ذلك، مازال هنالك الكثير من المنظمات لا تعي أهمية تطبيق هذه المواصفات في منظومتها الأمنية مما تسبب بوجود فجوة أمنية في المنظمة وفي مجالات مختلفة(Tsohou, 2010).

ومن هنا تهدف هذه الدراسة للتحقق من مدى قيام إدارات الموارد البشرية في الجامعات السعودية قيد الدراسة بالمسؤولية المناطة بها تجاه تحقيق الأمن المعلوماتي في تلك الجامعات بما يتوافق مع المواصفة العالمية (ISO/IEC 27002:2013).

2. الخلفية النظرية

يقصد بأمن المعلومات مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو المادي للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال، نلاحظ من هذا التعريف أن عناصر الامن المعلوماتي متعددة، فبالإضافة إلى الجانب التقني يوجد جوانب بشرية وبيئية وتنظيمية وتشريعية تؤثر إلى حد كبير في أمن التعاملات الإلكترونية(Alshehri, Drew, & Alfarraj, 2012).

ومن هذا المنطلق تلجأ المنظمات إلى اتباع عدد من الأساليب والطرق والاستراتيجيات التي تعزز موقفها في مجال الأمن المعلوماتي وسلامة التعاملات الإلكترونية فيها، ومن أهم هذه السبل قيام المنظمة بوضع سياسة موثقة لأمن المعلومات، ثم تطبيق هذه السياسة بشكل فعال وإلزام كافة الموظفين والمتعاملين بالامتثال لها لما لذلك من أهمية في نشر الوعي الأمني وتحقيق الامن المعلوماتي(Hina & & Dominic, 2016).

تستخدم المنظمات نظام لإدارة أمن المعلومات يتوافق مع المواصفات القياسية العالمية في مجال أمن المعلومات، ومن أهم هذه المواصفات تلك التي قدمتها المنظمة العالمية للمعايير (International Organization for Standardization) (ISO)، بالإضافة إلى معايير COBIT، ومعيار ITIL، وهي عبارة عن إرشادات وممارسات مثلى لإدارة وتنظيم أمن المعلومات في التعاملات الإلكترونية. (Sewuster, 2012)

قدمت (ISO) العديد من المواصفات المعيارية في مجال إدارة أمن المعلومات مثل المواصفة (ISO/IEC 27001) المتعلقة بإدارة أمن المعلومات، والمواصفة (ISO/IEC 27002) المتعلقة بقواعد الممارسة لنظام إدارة أمن المعلومات، والمواصفة (ISO/IEC 27003) التي تضمنت عدد من التوجيهات لتنفيذ المواصفة (ISO/IEC 27001).. الخ.

المواصفة (ISO/IEC 27001) تتضمن طرق تطبيق نظام إدارة أمن المعلومات والتحكم بها، وتركز على تقييم المخاطر وتحليلها، وإدارة الأصول والموارد، وإدارة الحوادث الطارئة(Susanto, Almunawar, & Tuan, 2011).

أما المواصفة العالمية (ISO/IEC 27002) فهي عبارة عن مجموعة من القواعد العامة والإرشادات حول الممارسة الأفضل في مجال نظم إدارة أمن المعلومات، تساعد المنظمات على تحقيق الأمن المعلوماتي، خصوصا بعد ارتفاع وتيرة الهجمات الإلكترونية، وقد عرفت هذه

المواصفة بتسميتين في السابق، أولها (BS7799 Part 1) ثم تلتها (ISO/IEC 17799) وقد تم تحديثها في عام 2005 ، ثم تعديل رمزها في تموز/يوليو 2007 بحيث أصبح يعرف ISO/IEC (27002:2005) ، ثم بعد ذلك تم تنقيح هذه النسخة لتصدر في عام 2014 النسخة المنقحة (ISO/IEC 27002:2013).

يمكن اعتماد المواصفة (ISO/IEC 27002:2013) كمرجع عند إعداد السياسة المتعلقة بالأمن المعلوماتي، فهي تقترح قواعد لممارسة إدارة الأمن، ومربع تحكم لتحليل المخاطر والتدقيق في مسألة ضمان الأمن، وتكمن أهمية هذه المواصفة في اشتمالها على جميع عناصر المنظومة الأمنية بما فيها الجوانب التنظيمية والبشرية والقانونية والتقنية. (ISO/IEC,2013)

من الجوانب الهامة التي تناولتها هذه المواصفة، ما يتعلق بأمن الموارد البشرية، والمقصود هنا مدى مراعاة العمليات الإدارية التي تمارسها وحدات إدارة الموارد البشرية في المنظمات للجوانب الأمنية، بحيث تساهم في تحقيق الأمن المعلوماتي من خلال ضمان معرفة ووعي العاملين والمتعاقدين من الخارج بنصوص سياسة أمن المعلومات المتبعة في المنظمة، ومدى التزامهم بها عند تنفيذ المهام المطلوبة منهم (ISO/IEC 27002:2013).

ومما لا شك فيه أن تطبيق هذه المعايير أو المواصفات يفيد في توعية العاملين في المؤسسات، ورفع مستوى التزامهم بتحمل مسؤولياتهم تجاه أمن المعلومات، وهذا الأمر يعزز من الأمن المعلوماتي على مستوى المنظمة. (Calder. & Watkins, 2008)

1.2 أمن الموارد البشرية في ضوء المواصفة الدولية (ISO/IEC 27002:2013)

نصت المواصفة الدولية (ISO/IEC 27002:2013) في البند رقم (7) على ضوابط أمن الموارد البشرية حيث تم تصنيفها إلى ثلاثة أقسام وهي قبل التوظيف، أثناء التوظيف، بعد التوظيف، وكانت هذه الضوابط على النحو التالي: (ISO/IEC 27002:2013)

1.1.2 قبل التوظيف: لضمان أن الموظفين والمقاولين الخارجيين (المتعاقدين من الخارج) قد فهموا المسؤوليات التي تقع عليهم وأن هذه المسؤوليات مناسبة للمهام المطلوبة منهم، وشملت الضوابط في هذا القسم ما يلي:

- التحري أو الفحص؛
- شروط وأحكام التوظيف.

2.1.2 أثناء التوظيف: التأكد من أن العاملين والمتعاقدين من الخارج على علم ووعي بأدوارهم ومسؤولياتهم تجاه أمن المعلومات ووفائهم بها، لضمان فهمهم لتهديدات أمن المعلومات وضمان حصولهم على المعرفة اللازمة للتخفيف من هذه التهديدات، وشملت الضوابط في هذا القسم ما يلي:

- إدارة المسؤوليات؛
- التوعية بأمن المعلومات والتدريب والتعليم؛
- الإجراءات التأديبية.

3.1.2 إنهاء العمل وتغيره: لحماية مصالح المنظمة كجزء من عملية تغيير أو إنهاء العمل، بهدف توفير نظام محدد لعملية ترك العمل وإنهاء الخدمة في المنظمة بشكل يضمن إزالة صلاحيات الوصول لهؤلاء الموظفين الذين يملكون حق الوصول إلى معلومات المنظمة وقد تركوا العمل أو تم إنهاء خدماتهم او تم تغيير عملهم، وكذلك ضمان إعادتهم لكافة الأصول التي بحوزتهم وتعود ملكيتها للمنظمة. وشملت الضوابط في هذا القسم:

- مسؤوليات ترك أو تغيير العمل؛
- إعادة الأصول؛
- إزالة إذن الوصول.

2.2 الدراسات السابقة

في الوقت الحاضر، يلقى موضوع أمن المعلومات عموماً اهتماما بحثيا بالغاً على المستوى العالمي، حيث تعددت الدراسات التي تناولت البحث في كيفية تحقيق الأمن المعلوماتي والعوامل المؤثرة والمخاطر المحتملة، ومن بين هذه الدراسات دراسة (Shaaban, 2014) حول تعزيز حوكمة أمن المعلومات في الدول النامية دراسة حالة زنجبار، حيث اهتمت هذه الدراسة بالنظر إلى أمن المعلومات من منظور متكامل واعتمدت على حجة مفادها أنه من أجل تحقيق استراتيجية فعالة لإدارة أمن المعلومات، من الضروري النظر إلى أمن المعلومات في سياق اجتماعي تقني، أي النظر في الأبعاد الثقافية والأخلاقية والقانونية والتنظيمية لأمن المعلومات بالإضافة الى الأدوات، والأجهزة والتقنيات ذات العلاقة، حيث يعتبر هذا البحث محاولة لتعزيز ثقافة أمن المعلومات في زنجبار من خلال دمج القضايا الاجتماعية والتقنية على حد سواء.

كما جاءت دراسة(Malekolkalami, 2014) بهدف تقييم حالة نظام إدارة أمن المعلومات في المكتبات المركزية في الجامعات الحكومية في طهران، من خلال انسجام وتوافق هذا النظام مع المواصفة العالمية لإدارة أمن المعلومات (ISO / IEC 27002)، حيث اجريت الدراسة باستخدام البحث الوصفي واستخدمت الاستبانة لجمع المعلومات من عينة الدراسة وتمثلت وحدة المعاينة بمدراء المكتبات المركزية ، وتوصلت الدراسة إلى عدد من النتائج الهامة من بينها أن المتوسط العام لتوافق نظام إدارة أمن المعلومات في المكتبات التي شملتها الدراسة مع بنود المواصفة القياسية (ISO / IEC 27002)،كان 4 من 5، وأن متوسط توافق نظام إدارة أمن المعلومات مع بند أمن الموارد البشرية كان 4.

هدفت دراسة (العربي, 2015)إلى الكشف عن مدى التزام مواقع أفضل الجامعات العربية (حسب تصنيف ويبومتركس لتقييم الجامعات والمعاهد) بما نصت عليه المواصفة العالمية (ISO/IEC 27002) ، وتم الاعتماد على قائمة مراجعة تضم عناصر معايير تقييم أمن المعلومات لتطبيقها على المواقع الإلكترونية قيد الدراسة، وتوصلت الدراسة إلى عدد من النتائج كان من أهمها أن جميع الجامعات التي شملتها الدراسة حرصت على تطبيق معايير فرعية من بنود المواصفة القياسية موضوع الدراسة وبنسبة 28% من تلك المعايير، وكانت الجامعات السعودية الثلاثة التي شملتها الدراسة (الملك فهد للبترول والمعادن، الملك عبدالعزيز، أم القرى) من أعلى الجامعات التزاما ببنود المواصفة، وكان من بين البنود التي التزمت الجامعات بتطبيق بعض معاييرها بند أمن الموارد البشرية حيث أن جميع الجامعات قيد الدراسة اهتمت بهذا البند حيث بلغت نسبة التزام الجامعات بمعايير هذا البند 74%.

كما بحثت دراسة (Kumah, Winfred, & Charles, 2018) في تحديد الممارسات الرئيسية لإدارة الموارد البشرية (HRM) اللازمة لتحسين أداء أمن المعلومات من منظور متخصصي تكنولوجيا المعلومات، وأثبتت الدراسة أهمية التدريب على أمن المعلومات، والتحقق من الخلفية للمتقدمين للوظائف، والرقابة على الموظفين باعتبارها ممارسات هامة للغاية في إدارة الموارد البشرية يمكن أن تحسن أداء أمن المعلومات التنظيمية.

إضافة إلى ذلك هدفت دراسة (Kumah, Yaokumah, & Okai, 2019) إلى تقييم مدى تطبيق ضوابط أمن الموارد البشرية قبل وأثناء وبعد التوظيف في المنظمات لإدارة مخاطر أمن المعلومات، حيث استخدمت الدراسة المنهج المقارن وتم جمع البيانات بواسطة الاستبيان، وتمثلت عينة الدراسة بمتخصصين في تكنولوجيا المعلومات والموارد البشرية الذين يعملون في خمس قطاعات رئيسية مختلفة في غانا ، وبينت الدراسة أن القطاع الصحي يتفوق على القطاعات الأخرى في إدارة الأمن بعد التوظيف، وكان أداء المؤسسات الحكومية هو الأسوأ بين جميع المنظمات.

وبهدف اقتراح مبادئ توجيهية مرتبطة بالسلوك الأمني للموظفين ويمكن دمجها مع المعايير العالمية ذات الانتشار الواسع مثل معايير (ISO/IEC 27002) قامت دراسة (Topa & Karyda, 2019) بمراجعة الأدبيات السابقة المتعلقة بموضوع إدارة امن المعلومات، ومن خلال نتائج هذه الدراسات توصلت الدراسة إلى أن أهم العوامل المؤثرة في السلوك الأمني للموظفين والتي ترتبط بشكل كلي أو جزئي بمعايير (ISO/IEC 27001, 27002, 27003 2,7005) هي دعم الإدارة العليا، خصائص الأفراد، الثقافة، تشجيع الموظفين على الامتثال للسياسة الأمنية.

3. الطرق والأدوات

تم تنفيذ الدراسة باستخدام منهجية البحث الوصفي وباستخدام طرق البحث النوعي وذلك وفقاً للإجراءات التالية:

- لجمع البيانات الثانوية التي تخدم هذه الدراسة، تم إجراء مسح الكتروني من خلال محرك البحث (google)، واستخدام قواعد البيانات العالمية مثل (Scopus, Emerald, Research Gate) للوصول إلى الأدبيات السابقة في مجال ممارسات أمن المعلومات والمعايير الدولية المتعلقة به، مع التركيز على أمن عمليات إدارة الموارد البشرية لمراجعتها والاطلاع على نتائجها، ومعرفة أهم العمليات التي تمارسها إدارة الموارد البشرية المؤثرة في تحقيق الأمن المعلوماتي. حيث تم الوقوف عند أهم الدراسات السابقة، التي تشكل رافداً حيوياً في هذه الدراسة.
- بناء على ما سبق، صممت قائمة فحص تشمل العمليات الإدارية المهمة التي تمارسها إدارة الموارد البشرية ووردت في المواصفة العالمية27002:2013 ISO/IEC كعوامل مؤثرة في الأمن المعلوماتي، حيث تضمن قائمة الفحص (25) فقرة مقسمة إلى قسمين، القسم الأول يتعلق بسياسة أمن المعلومات المطبقة في الجامعة وخصص لها (6) فقرات، أما القسم الثاني فهو ممارسات أمن عمليات إدارة الموارد البشرية وقد خصص لها (19) فقرة شملت ثلاث مجالات: ممارسات ما قبل التوظيف، ممارسات أثناء التوظيف، ممارسات إنهاء العمل وتغيره، كما تضمنت قائمة الفحص بيانات تعريفية عن الجامعة والوحدات التنظيمية ذات العلاقة.
- تم التحقق من صدق المحتوى لقائمة الفحص باستخدام طريقة رأي الخبراء حيث أنها من الطرق المناسبة لمثل هذا النوع من الدراسات، ووفقا لما جاء في دراسة (Beirami, Modiri, & Eshlaghi, 2016) فقد تم إرسالها إلى 10 خبراء متخصصين في مجال أمن المعلومات وأخذ رأيهم بخصوص الفقرات من حيث (الملائمة، الوضوح، البساطة، الأهمية) وذلك على مقياس ليكرت من 1-4، بعد ذلك تم استبعاد الفقرات التي حصلت على تقييم أقل من 3.
- تم اختيار جامعتين من الجامعات الحكومية في السعودية وهي جامعة الجوف، جامعة تبوك، لغايات تطبيق الدراسة وذلك بعد الحصول على الموافقات اللازمة لتطبيق الدراسة.
- باستخدام طرق البحث النوعي تم جمع البيانات الأولية الواردة في قائمة الفحص، حيث استخدمت المقابلات المهيكلة بشكل رئيسي مع مدراء ومختصي الموارد البشرية ومختصي أمن المعلومات في الجامعات قيد الدراسة، وكذلك تم إجراء مراجعة شاملة لكافة الوثائق المستخدمة مثل عقود العمل وقرارات انهاء الخدمة وأدلة الإجراءات التي توضح سير العمل وتأدية المهام في وحدات إدارة الموارد البشرية قيد الدراسة، كما تم جمع بعض البيانات من خلال الملاحظة المباشرة لكيفية تنفيذ العمليات والإجراءات في وحدات الموارد البشرية في الجامعات قيد الدراسة.

- بعد جمع بيانات الدراسة، تم تحليلها باستخدام أسلوب تحليل الفجوات والوصول للنتائج التي تبين مدى التزام وحدات الموارد البشرية في الجامعات بمعايير أمن المعلومات وفقاً لقائمة الفحص المصممة لهذه الدراسة.
- بعد استخراج النتائج النهائية، تم إجراء الدراسة المقارنة للتعرف على الفروقات بين الجامعات التي تشملها الدراسة فيما يتعلق بمدى الالتزام في تطبيق معايير أمن الموارد البشرية.

4. النتائج والمناقشة

في هذا الجزء من الدراسة سيتم عرض نتائج جمع وتحليل البيانات التي تم جمعها باستخدام طرق البحث النوعي للجامعات الثلاث وذلك على النحو التالي:

1.4 جامعة تبوك

أنشأت جامعة تبوك في عام 1427هـ، 2006م في مدينة تبوك التابعة لمنطقة تبوك التي تقع في الشمال الغربي للمملكة، يضم الهيكل التنظيمي للجامعة 11 كلية جامعية متخصصة تقع في الفرع الرئيسي للجامعة في مدينة تبوك، كما يضم (5) كليات جامعية في الفروع التابع للجامعة في المدن الأخرى التابعة لمنطقة تبوك، إضافة إلى ذلك، يضم الهيكل التنظيمي للجامعة (11) عمادة متخصصة ومركزين للأبحاث ومعهد لتعليم اللغات.

يلغ عدد منسوبي الجامعة قرابة (3057) منهم 1900عضو هيئة تدريس، و1100 موظف إداري، 50موظفاً يعملون في الوظائف الصحية، بالإضافة إلى 7 موظفين يعملون في الوظائف التعليمية من غير أعضاء هيئة التدريس.

تتولى عمادة الموارد البشرية الإشراف على إدارة الموارد البشرية في الجامعة، ويتبع لها عدد من الوحدات التنظيمية الفرعية المتخصصة من أهمها إدارة عمليات الموارد البشرية التي تعنى بممارسة عمليات الموارد البشرية وفقاً للأنظمة واللوائح المرعية، بالإضافة إلى التوجيهات والقرارات الإدارية التي تتخذها الإدارة العليا في سبيل تنفيذ سياسة الموارد البشرية في الجامعة.

كما تتولى عمادة تقنية المعلومات الاشراف على موارد تقنية المعلومات في الجامعة، ويتبع لها عدد من الوحدات التنظيمية الفرعية المتخصصة من بينها إدارة أمن المعلومات التي تتولى الاشراف على وإدارة أمن المعلومات في الجامعة.

1.1.4 سياسة أمن المعلومات في جامعة تبوك

تم جمع البيانات المطلوبة في قائمة الفحص باستخدام طرق البحث النوعي (المقابلات المهيكلة، تفحص الوثائق) وكانت النتائج كما يلي:

جدول رقم (3): واقع امتثال جامعة تبوك للمواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بسياسة أمن المعلومات

	الفقرة	نعم	لا	لا ينطبق	المعززات
1	يتوفر لدى الجامعة سياسة أمن معلومات موثقة	نعم			يوجد خمسة وثائق لسياسات أمن المعلومات
2	وثيقة سياسة أمن المعلومات معتمدة من الإدارة	نعم			خطاب اعتماد الوثيقة
3	وثيقة سياسة أمن المعلومات منشورة للعاملين	نعم			تم نشر وثائق سياسات أمن المعلومات الخمسة على الموقع الإلكتروني للجامعة بالإضافة إلى أرسلها بالبريد الإلكتروني لجميع منسوبي الجامعة

4	تخضع سياسة أمن المعلومات للمراجعة الدورية	نعم			خطابات إدارية تتضمن التوجيه بمراجعة وثائق سياسات أمن المعلومات انسجاما من التوجيهات الحكومية
5	تخضع سياسة أمن المعلومات للمراجعة عند حدوث التغييرات	نعم			وفقاً لما نصت عليه وثيقة تكليف لجنة أمن المعلومات بمراجعة سياسات أمن المعلومات في ضوء قرار مجلس الوزراء رقم 555 تاريخ 2019/5/28
6	حددت سياسة أمن المعلومات دور ومسؤوليات المنسوبين تجاه أمن المعلومات	نعم			وفقاً لما نصت عليه وثيقة سياسة تصنيف البيانات، وثيقة سياسة ضبط الدخول، ووثيقة سياسة الاتصالات اللاسلكية.، ووثيقة سياسة استخدام البريد الإلكتروني الرسمي.
مؤشر الالتزام		%100			التزام كامل

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي

كشفت الدراسة التطبيقية أن جامعة تبوك تلتزم بنسبة (100%) ببنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بموضوع سياسة أمن المعلومات، حيث تبين وجود خمسة سياسات معتمدة وموثقة ومنشورة تتعلق بأمن المعلومات وهي (سياسة تصنيف البيانات، سياسة ضبط الدخول، سياسة الخصوصية لمتصفحي موقع الجامعة، سياسة الاتصالات اللاسلكية، وسياسة استخدام البريد الإلكتروني) حيث قامت الجامعة بإعداد هذه الوثائق واعتمدها من الإدارة العليا، وكذلك نشرها في الموقع الإلكتروني للجامعة وإرسالها بالبريد الإلكتروني لجميع منسوبي الجامعة، ومن جهة أخرى تم اصدار نشرات توعوية للمنسوبين لتوعيتهم بمسؤوليتهم تجاه أمن المعلومات وتم نشر هذه النشرات على الموقع الإلكتروني وكذلك ارسالها بالبريد الإلكتروني لجميع المنسوبين.

من جانب آخر فإن النتائج بينت أن إدارة أمن المعلومات خصصت لجنة تعنى بمراجعة السياسة الأمنية بشكل دوري مرة واحدة سنوياً على الأقل أو عندما تطرأ تغيرات تستدعي ذلك حيث تمت أخر مراجعة بتاريخ 2019/7/1 بعد صدور قرار مجلس الوزراء المتعلق بضوابط استخدام تقنيات المعلومات والاتصالات في الجهات الحكومية.

2.1.4 أمن الموارد البشرية- إجراءات ما قبل التوظيف في جامعة تبوك

جدول رقم (4): واقع امتثال جامعة تبوك للمواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بأمن الموارد البشرية- إجراءات ما قبل التوظيف

	الفقرة	دائماً	غالبا	أحياناً	اطلاقاً	المعززات/ مصادر التوثيق
7	يتم التحقق من كافة المتقدمين للوظائف وفقاً للأنظمة واللوائح بما يخص أمن المعلومات			★		نتائج مراجعة دليل الإجراءات المتعلقة بالتوظيف والتعاقد، بالإضافة إلى خطابات إدارية للجهات الأمنية المختصة
8	يتم فحص كافة طلبات التوظيف من حيث اكتمال البيانات المطلوبة	★				الملاحظة المباشرة، ونتائج مراجعة دليل الإجراءات المتعلقة بالتوظيف والتعاقد

9	يتم فحص بيانات المتقدمين للوظائف فيما يخص الائتمان والسجل الجرمي		★			نتائج المقابلة مع رئيس وحدة التوظيف، الملاحظة المباشرة، مخاطبات إدارية تتعلق بالموظفين المحليين، وكذلك مخاطبات إدارية تتعلق المتعاقدين
10	يتضمن عقد التوظيف شروط والتزامات الموظف تجاه أمن المعلومات				★	نتائج مراجعة نموذج عقد العمل بالنسبة للمتعاقدين، ونموذج قرار التوظيف بالنسبة للموظفين المحليين
11	تحرص الجامعة على أخذ موافقة الموظف على كافة بنود العقد والتوقيع على ذلك	★				نتائج مراجعة نماذج من عقود العمل بالنسبة للمتعاقدين، ونماذج من قرارات التوظيف بالنسبة للموظفين المحليين
12	ينص العقد على الإجراءات المتخذة بحق الموظف في حال تجاهل متطلبات أمن المعلومات				★	نتائج مراجعة نماذج من عقود العمل بالنسبة للمتعاقدين، ونماذج من قرارات التوظيف بالنسبة للموظفين المحليين
	مؤشر الالتزام	50%	التزام متوسط			

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي

كشفت الدراسة التطبيقية أن جامعة تبوك تلتزم بنسبة (50%) ببنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بإجراءات ما قبل التوظيف، حيث كشفت نتائج مراجعة دليل الإجراءات المتعلقة بالتوظيف والتعاقد عدم وجود أي نص يتعلق بالتحقق من المتقدمين للوظائف وفقاً للأنظمة واللوائح بما يخص أمن المعلومات، إلا أنه لوحظ من مراجعة بعض المخاطبات الإدارية الصادرة عن الجامعة تبين التحقق من مدى وجود جرائم معلوماتية مسجلة بحق المرشحين للتعين في وظائف تتعلق بتقنية المعلومات.

كما ان وحدة التوظيف في الجامعة تحرص على مراجعة وتدقيق كافة طلبات التوظيف والتعاقد كمرحلة ثانية بعد انتهاء فترة التقديم عبر البوابة الإلكترونية للتوظيف للتحقق من اكتمال كافة البيانات المطلوبة من المتقدمين، كما أن النظام لا يقبل ارسال الطلب دون اكتمال البيانات الالزامية في الطلب ويعتبر الطلب لاغياً في حال عدم توفر الوثائق المطلوبة.

من جهة أخرى، تحرص وحدة التوظيف في أغلب الأحيان على التحقق من حسن السيرة والسلوك للمتقدمين لشغل الوظائف حيث تعتبر شهادة حسن السيرة والسلوك التي تصدرها الجهات المختصة إحدى الوثائق الرئيسية المطلوبة من كافة المتقدمين للوظائف من المواطنين المحليين، أما المتعاقدين من الأجانب فيقتصر الأمر على رعايا بعض الدول التي تشترط اللوائح حصولهم على موافقات أمنية قبل التعاقد معهم من قبل الجهات الحكومية.

بالإضافة إلى ذلك، وبعد مراجعة نموذج عقد التوظيف ونموذج قرار التوظيف المعتمد في الجامعة، فقد توصلت الدراسة إلى أن الجامعة تحرص دائماً على أخذ موافقة الموظف على كافة بنود العقد والتوقيع على ذلك.

أخيرا، لم يرد في عقد التوظيف أي إشارة إلى الإجراءات المتخذة بحق الموظف في حال تجاهل متطلبات أمن المعلومات.

3.1.4 أمن الموارد البشرية- إجراءات أثناء التوظيف في جامعة تبوك

جدول رقم (5): واقع امتثال جامعة تبوك للمواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بأمن الموارد البشرية- إجراءات أثناء التوظيف

	الفقرة	دائماً	غالبا	أحياناً	اطلاقاً	المعززات/ مصادر التوثيق
13	تحرص الجامعة على توقيع الموظف على نموذج خاص يتعهد بموجبه بعدم افشاء المعلومات الخاصة بالعمل أو الكشف عنها لأشخاص غير مصرح لهم، أو اساءة استخدامها من قبل من يملك اذن الوصول		★			نتائج المقابلة مع رئيس وحدة التوظيف، الملاحظة المباشرة، نماذج موقعه من بعض الموظفين الإداريين
14	تقوم الجامعة بتحديد مسؤوليات المنسوبين المتعاملين مع مرافق معالجة المعلومات بشكل موثق في الوصف الوظيفي	★				الملاحظة المباشرة، ونتائج مراجعة بطاقات الوصف الوظيفي للوظائف المتعلقة بتقنية المعلومات
15	تحرص الجامعة على تعريف وإبلاغ الموظف بمسؤولياته الأمنية قبل تكليفهم بالمهام التي تمس أمن المعلومات		★			عينة من رسائل البريد الإلكتروني المرسلة للمنسوبين، نماذج خاصة
16	تحرص الجامعة على تذكير المنسوبين باستمرار على ضرورة الالتزام بمتطلبات أمن المعلومات	★				عينة من رسائل البريد الإلكتروني المرسلة للمنسوبين
17	تحرص الجامعة على تحفيز المنسوبين الملتزمين بمتطلبات امن المعلومات				★	نتائج المقابلة مع مدير إدارة أمن المعلومات، ومدير إدارة عمليات الموارد البشرية
18	تحرص الجامعة على استقطاب الأشخاص المتخصصين في أمن المعلومات للاستفادة من خبراتهم			★		نتائج المقابلة مع مدير إدارة أمن المعلومات
19	تحرص الجامعة على توعية المنسوبين ونشر ثقافة أمن المعلومات	★				عينة من رسائل البريد الإلكتروني المرسلة للمنسوبين، نشرة توعية بأمن المعلومات منشورة على الموقع الإلكتروني للجامعة
20	تحرص الجامعة على تدريب المنسوبين ومن في حكمهم على مسائل أمن المعلومات			★		نتائج المقابلة مع مدير إدارة أمن المعلومات، مراجعة ملفات موظفي عمادة تقنية المعلومات

21	يوجد إجراءات تأديبية واضحة ومحددة تتخذ بحق المنسوبين المتسببين في الخروقات الأمنية	★				مراجعة وثائق سياسات أمن المعلومات، نظام الجرائم الإلكترونية، قرارات إدارية صادرة بحق منسوبين في الجامعة.
	مؤشر الالتزام	%67				التزام متوسط

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي

كشفت الدراسة التطبيقية أن جامعة تبوك تلتزم بنسبة (67%) ببنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بإجراءات أثناء التوظيف، حيث تبين من خلال البيانات التي تم الوصول إليها حرص الجامعة في معظم الأحيان على توقيع المنسوبين على نموذج خاص يتعهد بموجبه بعدم افشاء المعلومات الخاصة بالعمل أو الكشف عنها لأشخاص غير مصرح لهم، أو اساءة استخدامها من قبل من يملك اذن الوصول.

كما حرصت الجامعة على تحديد مسؤوليات المنسوبين المتعاملين مع مرافق معالجة المعلومات بشكل موثق في بطاقات الوصف الوظيفي لجميع وظائف عمادة تقنية المعلومات.

وكذلك تحرص الجامعة على تعريف وإبلاغ الموظف بمسؤولياته الأمنية قبل تكليفهم بالمهام التي تمس أمن المعلومات، حيث تم تصنيف وظائف المنسوبين إلى عدة مجموعات وتحديد مسؤولية أمن المعلومات لكل مجموعة منها واعداد نموذج خاص لكل مجموعة يتضمن المسؤولية الأمنية التي تقع على عاتق أعضاء هذه المجموعة يتم ارساله للمنسوبين وأخذ توقيعه عليه، كما تحرص الجامعة على تذكير المنسوبين باستمرار على ضرورة الالتزام بمتطلبات أمن المعلومات من خلال ارسال رسائل توعوية بالبريد الإلكتروني للمنسوبين.

من جهة أخرى، أشارت النتائج إلى أن الجامعة لم تهتم بتحفيز المنسوبين الملتزمين بضوابط امن المعلومات فلم تتوصل الدراسة إلى أي قرار تحفيز من هذا النوع وفقاً لما أكدته المقابلات مع المعنيين بهذا الخصوص.

أيضا تبين من خلال البحث النوعي أن الجامعة حرصت في فترة معينة على استقطاب كفاءات متخصصة في أمن المعلومات للعمل لديها وذلك من قبيل الاستفادة من خبراتهم ومهاراتهم في تحقيق الأمن المعلوماتي.

بالإضافة إلى ما سبق، فقد حرصت الجامعة على توعية المنسوبين بقضايا أمن المعلومات وذلك من خلال الرسائل التذكيرية التي يتم ارسالها إلى المنسوبين عبر البريد الإلكتروني، وكذلك من خلال النشرات التوعوية في مجال أمن المعلومات التي تنشرها الجامعة على موقعها الإلكتروني.

أما فيما يتعلق بجانب التدريب، فإن اهتمام الجامعة به كان متواضعاً حيث اقتصر التدريب في مجال أمن المعلومات على بعض موظفي عمادة تقنية المعلومات دون باقي المنسوبين.

أخيراً نصت سياسات أمن المعلومات على الإجراءات التأديبية المتخذة بحق المنسوبين المخالفين لضوابط امن المعلومات وكذلك نشرت الجامعة على موقعها الإلكتروني نظام مكافحة الجرائم المعلوماتية لبيان العقوبات التي ستتخذ حيال أي جريمة معلوماتية ممكن أن تقع على الموارد المعلوماتية التابعة لها، كما تبين من خلال مراجعة بعض القرارات الإدارية بهذا الشأن ان الجامعة لا تتهاون في تطبيق النظام ومحاسبة المتسببين بأي خروقات لأمن المعلومات.

4.1.4 أمن الموارد البشرية- إجراءات تغير أو ترك العمل في جامعة تبوك

جدول رقم (6): واقع امتثال جامعة تبوك للمواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بأمن الموارد البشرية- إجراءات ترك العمل

	الفقرة	دائماً	غالبا	أحياناً	اطلاقاً	المعززات/ مصادر التوثيق
22	يتوفر في الجامعة الإجراءات المحددة التي تخص أمن المعلومات عند ممارسة انهاء خدمات أحد المنسوبين ومن في حكمهم	★				نتائج مراجعة وثائق إنهاء الخدمة وإخلاء الطرف للموظفين المحليين ومن في حكمهم وكذلك نماذج انهاء الخدمة وإخلاء الطرف للمتعاقدين.
23	تطبق الجامعة إجراءات واضحة ومحددة لإزالة حق الوصول للمعلومات للمنسوبين المنتهية خدماتهم	★				الملاحظة المباشرة لآلية تنفيذ قرار انهاء الخدمات من خلال نظام معلومات المنسوبين ونظام الصلاحيات
24	تطبق الجامعة إجراءات واضحة ومحددة لتعديل صلاحيات المنسوبين في الوصول للمعلومات عند النقل أو تغيير مهامهم		★			الملاحظة المباشرة لآلية تنفيذ قرارات النقل والانتداب من خلال نظام معلومات المنسوبين ونظام الصلاحيات
25	تطبق الجامعة إجراءات واضحة ومحددة لإعادة الأصول المتعلقة بمعالجة المعلومات من المنسوبين المنتهية خدماتهم	★				نتائج مراجعة وثائق إنهاء الخدمة وإخلاء الطرف للموظفين المحليين ومن في حكمهم وكذلك نماذج انهاء الخدمة وإخلاء الطرف للمتعاقدين.
	مؤشر الالتزام	%92				التزام مرتفع

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي

كشفت الدراسة التطبيقية أن جامعة تبوك تلتزم بنسبة (92%) ببنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بإجراءات تغيير أو ترك العمل، حيث تبين أن الجامعة ألزمت كل من تنتهي خدمته أن يخلي طرفه من عمادة تقنية المعلومات، وتبين من خلال تفحص الإجراءات الإدارية لإخلاء الطرف في عمادة تقنية المعلومات أن ذلك يشمل كل ما يتعلق بأمن المعلومات مثل إزالة حق الوصول لمرافق المعلومات، واغلاق الحسابات الخاصة بمن تنتهي خدماته.

بالإضافة الإجراءات الإدارية في إخلاء الطرف فهناك أيضاً إجراءات فنية ينفذها النظام بصورة آلية بمجرد إدخال بيانات قرار انهاء الخدمات للموظف ومن في حكمه، فإن النظام يقوم بإزالة حق الوصول للمعلومات الذي كان لدى الموظف قبل انتهاء خدماته.

ومن جانب آخر فإن الجامعة في أغلب الأحيان تقوم بتعديل صلاحيات المنسوبين الذين يتم نقلهم أو تغيير وظائفهم حسب الوضع الجديد، حيث تبين ذلك من خلال الملاحظة المباشرة لآلية تنفيذ قرارات النقل والانتداب من خلال نظام معلومات المنسوبين ونظام الصلاحيات المعتمد لدى عمادة تقنية المعلومات وعمادة الموارد البشرية، حيث يتم تنفيذ ذلك آلياً من خلال النظام بمجرد ادخال بيانات قرار النقل تتوقف صلاحيات الوصول للمعلومات الممنوحة للموظف بسبب وظيفته السابقة، ومنحه صلاحيات الوصول للمعلومات حسب وظيفته الجديدة، وبالرغم من ذلك إلا أن ذلك لا ينطبق

على جميع الحالات بسبب مشاكل فنية في النظام مما يتطلب تنفيذ هذا الإجراء بصورة يدوية على نظام الصلاحيات مباشرة.

أخيراً، تشتمل إجراء ات إخلاء الطرف من عمادة تقنية المعلومات وإدارة المستودعات على إلزام الموظف المنتهية خدماته بتسليم كافة الأجهزة والبرمجيات التي حصل عليها أثناء خدمته في الجامعة.

2.4 جامعة الجوف

أنشأت جامعة الجوف في عام 1426هـ، 2005م في مدينة سكاكا التابعة لمنطقة الجوف التي تقع في شمال المملكة، يضم الهيكل التنظيمي للجامعة 12 كلية جامعية متخصصة تقع في الفرع الرئيسي للجامعة في مدينة سكاكا، كما يضم (5) كليات جامعية في الفروع التابع للجامعة في المدن الأخرى التابعة لمنطقة الجوف، إضافة إلى ذلك، يضم الهيكل التنظيمي للجامعة (10) عمادة متخصصة ومعهداً للبحوث والدراسات الاستشارية، بالإضافة إلى عدد من الوحدات الإدارية التنفيذية المساندة.

بلغ عدد منسوبي الجامعة قرابة (2709) منهم 1778عضو هيئة تدريس، و931 موظف. تتولى عمادة شؤون أعضاء هيئة التدريس والموظفين الإشراف على إدارة الموارد البشرية في الجامعة، ويتبع لها عدد من الوحدات التنظيمية الفرعية المتخصصة من أهمها إدارة شؤون أعضاء هيئة التدريس، وإدارة شؤون الموظفين، التي تعنى بممارسة عمليات الموارد البشرية وفقاً للأنظمة واللوائح المرعية.

كما تتولى الإدارة العامة لتقنية المعلومات والاتصالات الاشراف على موارد تقنية المعلومات في الجامعة، ويتبع لها عدد من الوحدات التنظيمية الفرعية المتخصصة من بينها إدارة الجودة وأمن المعلومات التي تتولى الاشراف على وإدارة أمن المعلومات في الجامعة.

1.2.4 سياسة أمن المعلومات في جامعة الجوف

تم جمع البيانات المطلوبة في قائمة الفحص باستخدام طرق البحث النوعي (المقابلات المهيكلة، تفحص الوثائق) وكانت النتائج كما يلي:

جدول رقم (7): واقع امتثال جامعة الجوف للمواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بسياسة أمن المعلومات

	الفقرة	نعم	لا	لا ينطبق	المعززات
1	يتوفر لدى الجامعة سياسة أمن معلومات موثقة	★			وثيقة سياسة أمن المعلومات الإصدار الأول والثاني والثالث
2	وثيقة سياسة أمن المعلومات معتمدة من الإدارة	★			خطاب اعتماد الوثيقة من الإدارة العليا
3	وثيقة سياسة أمن المعلومات منشورة للعاملين	★			تم نشر وثيقة سياسة أمن المعلومات على الموقع الإلكتروني للإدارة العامة لتقنية المعلومات والاتصالات بالإضافة إلى تعميمها على كافة الوحدات التنظيمية في الجامعة بموجب رسالة إدارية
4	تخضع سياسة أمن المعلومات للمراجعة الدورية	★			بموجب قرارات إدارية موثق تم مراجعة وثيقة سياسة أمن المعلومات بشكل دوري ثلاث مرات
5	تخضع سياسة أمن المعلومات للمراجعة عند حدوث التغييرات		★		لا يوجد نص في وثيقة سياسة أمن المعلومات المعتمدة يوجه بمراجعة هذه الوثيقة عند حدوث تغييرات، ولم يحصل أنه تم مراجعتها لحدوث

					تغييرات معينة وانما اقتصر الأمر على المراجعة الدورية.
6	حددت سياسة أمن المعلومات دور ومسؤوليات المنسوبين تجاه أمن المعلومات	★			وفقاً لما نصت عليه وثيقة سياسة أمن المعلومات الإصدار الأول والثاني والثالث.
مؤشر الالتزام		%83			التزام مرتفع

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي

كشفت الدراسة التطبيقية أن جامعة الجوف تلتزم بنسبة (83%) ببنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بموضوع سياسة أمن المعلومات، حيث تبين وجود وثيقة السياسات العامة لأمن المعلومات معتمدة ومنشورة، وكذلك يتم بشكل دوري توعية المنسوبين بمسؤولياتهم تجاه أمن المعلومات من خلال الرسائل التي ترسلها إدارة الجودة وأمن المعلومات بالبريد الإلكتروني لكافة المنسوبين والطلبة.

من جانب آخر فإن النتائج بينت أن إدارة الجودة وأمن المعلومات قامت بمراجعة السياسة الأمنية بشكل دوري فقد تم اصدار النسخة الأولى بتاريخ 2015/5/11 وخضعت للمراجعة الدورية بتاريخ 2016/8/3، وتمت آخر مراجعة للسياسات العامة لأمن المعلومات بتاريخ 2019/8/20.

بالرغم من ذلك إلا أن وثيقة السياسات العامة لأمن المعلومات الإصدار الثالث وكذلك الإصدارات التي سبقته لم تنص صراحة على ضرورة مراجعة هذه الوثيقة عند حدوث أي تغيرات، ولم يتم التوصل من خلال هذه الدراسة إلى أي وثيقة أو رسالة إدارية توجه بمراجعة وثيقة السياسات العامة لأمن المعلومات نتيجة حدوث تغييرات محددة.

أخيراً، حددت وثيقة السياسات العامة لأمن المعلومات بنص صريح مسؤولية كل من الوحدات التنظيمية في الجامعة وكذلك المنسوبين والطلاب والمتعاقدين من الخارج تجاه أمن المعلومات.

2.2.4 أمن الموارد البشرية- إجراءات ما قبل التوظيف في جامعة الجوف

جدول رقم (8): واقع امتثال جامعة الجوف للمواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بأمن الموارد البشرية- إجراءات ما قبل التوظيف

	الفقرة	دائماً	غالبا	أحياناً	اطلاقاً	المعززات/ مصادر التوثيق
7	يتم التحقق من كافة المتقدمين للوظائف وفقاً للأنظمة واللوائح بما يخص أمن المعلومات				★	نتائج مراجعة دليل الإجراءات المتعلقة بالتوظيف والتعاقد، بالإضافة إلى نتائج المقابلة
8	يتم فحص كافة طلبات التوظيف من حيث اكتمال البيانات المطلوبة	★				الملاحظة المباشرة، ونتائج مراجعة دليل الإجراءات المتعلقة بالتوظيف والتعاقد
9	يتم فحص بيانات المتقدمين للوظائف فيما يخص الائتمان والسجل الجرمي	★				نتائج المقابلة مع مدير إدارة عمليات الموارد البشرية، الملاحظة المباشرة، مخاطبات إدارية تتعلق بالموظفين المحليين،

						وكـذلك مخاطبـات إداريـة تتعلق المتعاقدين
10	يتضـمن عقـد التوظيـف شـروط والتزامـات الموظـف تجـاه أمـن المعلومات				★	نتائج مراجعة نموذج عقد العمـل بالنسـبة للمتعاقـدين، ونمـوذج قـرار التوظيـف بالنسبة للموظفين المحليين
11	تحرص الجامعة على أخذ موافقة الموظـف علـى كافـة بنـود العقـد والتوقيع على ذلك	★				نتائج مراجعـة نمـاذج مـن عقـــود العمـــل بالنســـبة للمتعاقـدين، ونمـــاذج مـــن قـرارات التوظيـف بالنسـبة للموظفين المحليين
12	يـنص العقـد علـى الإجـراءات المتخذة بحق الموظـف فـي حـال تجاهل متطلبات أمن المعلومات				★	نتـائج مراجعـة نمـاذج مـن عقـــود العمـــل بالنســـبة للمتعاقـدين، ونمـــاذج مـــن قـرارات التوظيـف بالنسـبة للموظفين المحليين
	مؤشر الالتزام	%50				التزام متوسط

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي

كشفت الدراسة التطبيقية أن جامعة الجوف تلتزم بنسبة (50%) ببنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بإجراءات ما قبل التوظيف، حيث كشفت نتائج مراجعة دليل الإجراءات المتعلقة بالتوظيف والتعاقد عدم وجود أي نص يتعلق بالتحقق من المتقدمين للوظائف وفقاً للأنظمة واللوائح بما يخص أمن المعلومات.

كما ان إدارة عمليات الموارد البشرية في الجامعة تحرص على مراجعة وتدقيق كافة طلبات التوظيف والتعاقد كمرحلة ثانية بعد انتهاء فترة التقديم سواء كان طلب التوظيف ورقي أو الكتروني فقد تم تضمينه بجزء يتعلق بفحص اكتمال بيانات الطلب.

من جهة أخرى، تحرص إدارة عمليات الموارد البشرية على التحقق من حسن السيرة والسلوك للمتقدمين لشغل الوظائف حيث تعتبر شهادة حسن السيرة والسلوك التي تصدرها الجهات المختصة إحدى الوثائق الرئيسية المطلوبة من كافة المتقدمين للوظائف من المواطنين المحليين، أما المتعاقدين من الأجانب فيطلب منهم ارفاق وثيقة صادرة عن الجهات المعنية في دولهم تثبت حسن السيرة والسلوك وعدم قيامهم بأفعال جرمية.

بالإضافة إلى ذلك، وبعد مراجعة نموذج عقد التوظيف ونموذج قرار التوظيف المعتمد في الجامعة، فقد توصلت الدراسة إلى أن الجامعة تحرص دائماً على أخذ موافقة الموظف على كافة بنود العقد والتوقيع على ذلك.

أخيرا، لم يرد في عقد التوظيف أي إشارة إلى الإجراءات المتخذة بحق الموظف في حال تجاهل متطلبات أمن المعلومات.

3.2.4 أمن الموارد البشرية- إجراءات أثناء التوظيف في جامعة الجوف

جدول رقم (9): واقع امتثال جامعة الجوف للمواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بأمن الموارد البشرية- إجراءات أثناء التوظيف

	الفقرة	دائماً	غالبا	أحياناً	اطلاقاً	المعززات/ مصادر التوثيق
13	تحرص الجامعة على توقيع الموظف على نموذج خاص يتعهد بموجبه بعدم افشاء المعلومات الخاصة بالعمل أو الكشف عنها لأشخاص غير مصرح لهم، أو اساءة استخدامها من قبل من يملك اذن الوصول	★				نماذج تم التوقيع عليها الموظفين الإداريين
14	تقوم الجامعة بتحديد مسؤوليات المنسوبين المتعاملين مع مرافق معالجة المعلومات بشكل موثق في الوصف الوظيفي	★				بطاقات الوصف الوظيفي للوظائف المتعلقة بتقنية المعلومات
15	تحرص الجامعة على تعريف وإبلاغ الموظف بمسؤولياته الأمنية قبل تكليفهم بالمهام التي تمس أمن المعلومات			★		نتائج المقابلة مع رئيس وحدة أمن المعلومات
16	تحرص الجامعة على تذكير المنسوبين باستمرار على ضرورة الالتزام بمتطلبات أمن المعلومات			★		لم تحصل الدراسة على أي رسالة بريد الكتروني أو مخاطبة إدارية بهذا الخصوص، وتم الاكتفاء بالتوجيهات الشفوية على مستوى إدارة تقنية المعلومات
17	تحرص الجامعة على تحفيز المنسوبين الملتزمين بمتطلبات امن المعلومات				★	نتائج المقابلة مع مدير إدارة شؤون الموظفين، ومدير إدارة شؤون أعضاء هيئة التدريس
18	تحرص الجامعة على استقطاب الأشخاص المتخصصين في أمن المعلومات للاستفادة من خبراتهم		★			نتائج المقابلة مع رئيس وحدة أمن المعلومات
19	تحرص الجامعة على توعية المنسوبين ونشر ثقافة أمن المعلومات	★				عينة من رسائل البريد الإلكتروني المرسلة للمنسوبين
20	تحرص الجامعة على تدريب المنسوبين ومن في حكمهم على مسائل أمن المعلومات			★		نتائج المقابلة مع رئيس وحدة أمن المعلومات، فقط بعض من منسوبي إدارة تقنية المعلومات حصلوا على تدريب في هذا المجال

21	يوجد إجراءات تأديبية واضحة ومحددة تتخذ بحق المنسوبين المتسببين في الخروقات الأمنية	★				نص وثيقة سياسة أمن المعلومات، نظام الجرائم الإلكترونية
	مؤشر الالتزام	%63				التزام متوسط

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي

كشفت الدراسة التطبيقية أن جامعة الجوف تلتزم بنسبة (63%) ببنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بإجراءات أثناء التوظيف، حيث تبين النتائج حرص الجامعة دوماً على توقيع المنسوبين (موظفين وأعضاء هيئة تدريس) على نموذج خاص يتعهد بموجبه بعدم افشاء المعلومات الخاصة بالعمل أو الكشف عنها لأشخاص غير مصرح لهم، أو اساءة استخدامها من قبل من يملك اذن الوصول.

كما تحرص الجامعة دوماً على تحديد مسؤوليات المنسوبين المتعاملين مع مرافق معالجة المعلومات بشكل موثق في بطاقات الوصف الوظيفي لجميع وظائف إدارة تقنية المعلومات.

وبينت الدراسة أن اهتمام الجامعة بتعريف وإبلاغ الموظف بمسؤولياته الأمنية قبل تكليفهم بالمهام التي تمس أمن المعلومات كان منخفضاً، حيث لم يتم الوصول إلى أي مخاطبة إدارية بهذا الخصوص، وكذلك لم تحصل الدراسة على أي رسالة بريد الكتروني أو مخاطبة إدارية تعكس اهتمام الجامعة بتذكير المنسوبين بضرورة الالتزام بمتطلبات أمن المعلومات وانما تم الاكتفاء بالتوجيهات الشفوية لموظفي إدارة تقنية المعلومات.

من جهة أخرى، أشارت النتائج إلى أن الجامعة لم تهتم بتحفيز المنسوبين الملتزمين بضوابط امن المعلومات فلم تتوصل الدراسة إلى أي قرار تحفيز من هذا النوع وفقاً لما أكدته المقابلات مع المعنيين بهذا الخصوص.

أيضا كشفت نتائج المقابلات أن الجامعة حرصت على استقطاب كفاءات متخصصة في أمن المعلومات للعمل لديها وذلك من قبيل الاستفادة من خبراتهم ومهاراتهم في تحقيق الأمن المعلوماتي.

بالإضافة إلى ما سبق، تحرص الجامعة وباستمرار على توعية المنسوبين بقضايا أمن المعلومات وذلك من خلال الرسائل التذكيرية التي يتم ارسالها إلى المنسوبين عبر البريد الإلكتروني.

أما فيما يتعلق بجانب التدريب، فقد كشفت نتائج المقابلات انخفاض مستوى اهتمام الجامعة بتدريب المنسوبين على قضايا امن المعلومات، حيث اقتصر التدريب في مجال أمن المعلومات على بعض منسوبي إدارة تقنية المعلومات دون باقي المنسوبين.

أخيراً نصت سياسة أمن المعلومات التي اعتمدتها الجامعة ونشرتها على موقعها الإلكتروني على الإجراءات التأديبية المتخذة بحق المنسوبين المخالفين لضوابط امن المعلومات وكذلك نشرت الجامعة على موقعها الإلكتروني نظام مكافحة الجرائم المعلوماتية لبيان العقوبات التي ستتخذ حيال أي جريمة معلوماتية ممكن أن تقع على الموارد المعلوماتية التابعة لها.

4.2.4 أمن الموارد البشرية- إجراءات تغير أو ترك العمل في جامعة الجوف

جدول رقم (10) واقع امتثال جامعة الجوف للمواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بأمن الموارد البشرية- إجراءات ترك العمل

	الفقرة	دائماً	غالباً	أحياناً	اطلاقاً	المعززات/ مصادر التوثيق
22	يتوفر في الجامعة الإجراءات المحددة التي تخص أمن المعلومات عند ممارسة انهاء خدمات أحد المنسوبين ومن في حكمهم	★				نتائج مراجعة وثائق إنهاء الخدمة وإخلاء الطرف للموظفين وأعضاء هيئة التدريس
23	تطبق الجامعة إجراءات واضحة ومحددة لإزالة حق الوصول للمعلومات للمنسوبين المنتهية خدماتهم	★				الملاحظة المباشرة لعمل نظام الصلاحيات آلياً
24	تطبق الجامعة إجراءات واضحة ومحددة لتعديل صلاحيات المنسوبين في الوصول للمعلومات عند النقل أو تغيير مهامهم	★				الملاحظة المباشرة لعمل نظام الصلاحيات آلياً
25	تطبق الجامعة إجراءات واضحة ومحددة لإعادة الأصول المتعلقة بمعالجة المعلومات من المنسوبين المنتهية خدماتهم	★				نتائج مراجعة وثائق إنهاء الخدمة وإخلاء الطرف للموظفين وأعضاء هيئة التدريس
	مؤشر الالتزام	%100				التزام مرتفع

المصدر: من إعداد الباحثين بالاعتماد على نتائج التحليل الإحصائي

كشفت الدراسة التطبيقية أن جامعة الجوف تلتزم بنسبة (100%) ببنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بإجراءات تغيير أو ترك العمل، حيث تبين أن الجامعة ألزمت كل من تنتهي خدمته أن يخلي طرفه من إدارة تقنية المعلومات، تبين من خلال ملاحظة عمل نظام الصلاحيات أنه يتم إزالة حق الوصول لمرافق المعلومات، واغلاق الحسابات الخاصة بالموظف أو عضو هيئة التدريس الذي تنتهي خدماته.

بالإضافة إلى ذلك، فإن نظام شؤون الموظفين وأعضاء هيئة التدريس المحوسب المتوفر في الجامعة مرتبط بنظام الصلاحية فبمجرد إدخال بيانات فرار النقل أو تغيير الوظيفة فإن النظام لن ينفذ هذا التغيير إلى إذا تم تعديل مجموعة الموظف في نظام الصلاحيات وبالتالي إزالة حق الوصول للمعلومات التي كانت لدى الموظف قبل قرار النقل أو الانتداب أو تغيير الوظيفة.

أخيراً، تشتمل إجراء ات إخلاء الطرف من إدارة تقنية المعلومات وإدارة المستودعات على إلزام الموظف المنتهية خدماته بتسليم كافة الأجهزة والبرمجيات التي حصل عليها أثناء خدمته في الجامعة.

5. الخلاصة

في ظل تحليل البيانات النوعية التي جمعتها الدراسة التطبيقية، وفي ضوء الأهداف التي تسعى هذه الدراسة لتحقيقها، فقد تم التوصل إلى النتائج التالية:

- كشف الدراسة عن وجود سياسة أمن المعلومات موثقة ومعتمدة من الإدارة العليا ومنشورة للعاملين في جامعة تبوك وجامعة الجوف، حيث أن جامعة تبوك الأكثر التزاما ببنود المواصفة الدولية (ISO 27001:2013) فيما يتعلق ببند سياسة أمن المعلومات فقد التزمت بشكل كامل في هذا المعيار الدولي الهام لتحقيق أمن المعلومات.
- بينت الدراسة ان كلا الجامعتين تطبق معايير أمن المعلومات المتعلقة بإجراءات قبل التوظيف بمستوى متوسط وبنسب متساوية بلغت (50%)، حيث تجاهلت الجامعتين تضمين عقد التوظيف بأي شروط تلزم الموظف بالالتزام بمتطلبات أمن المعلومات، وكذلك لم ينص عقد التوظيف على أي إجراءات تتخذ بحق الموظف في حال تجاهل متطلبات الامن، بالإضافة إلى ذلك لم تلتزم الجامعتين بالقيام بالتحقق من أهلية المتقدمين للوظائف فيما يتعلق بقضايا أمن المعلومات، حيث لم تصل الدراسة الى ما يشير بأن جامعة الجوف اهتمت بهذا البند، أما جامعة تبوك فتوصلت الدراسة الى اهتمامها بهذا البند بمستوى منخفض.
- كشفت الدراسة عن التزام الجامعتين بمستوى متوسط بتطبيق بنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بإجراءات أثناء التوظيف وبنسب متقاربة، وكانت الجامعتين قد أهملت الالتزام بشكل كامل موضوع تحفيز الموظفين الملتزمين بمتطلبات أمن المعلومات، وكذلك كان هنالك تقصير فيما يتعلق بتعريف الموظف بمسؤولياته الأمنية قبل تكليفهم بالمهام التي تمس بأمن المعلومات، وكذلك قصرت كلا الجامعتين بموضوع تدريب الموظفين على مسائل أمن المعلومات.، وفي المقابل تبين وجود إجراءات نظامية واضحة ومحددة تتخذ بحق المتسببين بالخروقات الأمنية ومصدر هذه الإجراءات نظام الجرائم الإلكترونية الذي أصدرته الحكومة. وكذلك تحرص كلا الجامعتين على توعية منسوبيها فيما يتعلق بمسائل أمن المعلومات وتذكرهم باستمرار بواجباتهم تجاه هذا الموضوع، ويتم توقيع الموظف على نموذج خاص يتعهد بموجبه بالمحافظة على سرية المعلومات وعدم كشفها لغير المصرح لهم.
- بينت الدراسة ان كلا الجامعتين ملتزمة بمستوى مرتفع في تطبيق بنود المواصفة العالمية ISO/IEC 27002:2013 فيما يتعلق بإجراءات تغيير أو ترك العمل، حيث التزمت جامعة الجوف التزاماً كاملا بهذا المعيار، كذلك بالنسبة لجامعة تبوك فقد حرصت على تنفيذ معظم بنود هذا المعيار.

في ضوء النتائج التي توصلت إليها الدراسة فإنها توصي بما يلي:

- أن تقوم كلا الجامعتين برفع مستوى التزامها ببنود المواصفة ISO/IEC 27002:2013 فيما يتعلق بإجراءات ما قبل التوظيف خاصة فيما يتعلق بالتحقق من المتقدمين للوظائف من حيث سلوكهم في مجال أمن المعلومات قبل أن يتم توظيفهم، وكذلك يجب عليها تضمين عقد التوظيف بشروط تلزم الموظف بالالتزام بمتطلبات أمن المعلومات، وأن ينص عقد التوظيف على الإجراءات التي تتخذ بحق الموظف في حال تجاهل متطلبات الامن المعلوماتي والمسؤوليات الأمنية المنصوص عليها في وثيقة سياسة أمن المعلومات.
- كما توصي الدراسة بضرورة رفع مستوى التزام كلا الجامعتين ببنود المواصفة ISO/IEC 27002:2013 فيما يتعلق بإجراءات أثناء التوظيف وعليها أن تحدد حوافز لكل الملتزمين بمتطلبات امن المعلومات وفق معايير واضحة تضمن التزام المنسوبين بالمتطلبات الأمنية، بالإضافة إلى ضرورة أن تحدد الإجراءات كيفية تعريف الموظف بمسؤولياته تجاه امن المعلومات قبل تكليفه بالمهام التي تمس أمن المعلومات، وعليها أيضاً أن تحدد برامج تدريسية واضحة ضمن المسار التدريبي للموظف تتعلق بأمن المعلومات.

- أخيرا، توصي الدراسة بإجراء المزيد من الدراسات التي تهتم بدور عمليات إدارة الموارد البشرية في تحقيق الأمن المعلوماتي في الجامعات والمنظمات الحكومية الأخرى استنادا إلى المنهجية التي استخدمتها هذه الدراسة، بالإضافة إلى اجراء دراسة تقدم اطاراً مقترحاً وآلية عمل واضحة ومحددة تساعد الجامعات والمنظمات الحكومية الأخرى على ضمان أن تكون عمليات إدارة الموارد البشرية تساهم في تحقيق الأمن المعلوماتي في ضوء نتائج هذه الدراسة ومنهجيتها.

الشكر

تم تمويل هذه الدراسة برعاية عمادة البحث العلمي، جامعة الطائف، المملكة العربية السعودية لذا أتقدم لهم بوافر الشكر وعظيم الامتنان.

المراجع (References)

Al-Arabi, A. O., Miayar almunadhama adwliya litawhid alkiassi ISO 27002: lisyasat amn almaaloumat dirassa wasfiua tahliliya limawaki aljamiaat alarabiya. Majalat jamiat taiba lioulom w aladab, 7, 661-738. [In Arabic]

Alshehri, M., Drew, S., & Alfarraj, O. (2012). A Comprehensive Analysis of E-government services adoption in Saudi Arabia: Obstacles and Challenges. (IJACSA) International Journal of Advanced Computer Science and Applications, 3(2), 1-6.

Ansen, J. B. (2014). Information Security Management in a Human Resource Information System of a Selected University of Technology. (master), Cape Peninsula University of Technology of South Africa,

Beirami, N., Modiri, N., & Eshlaghi, A. T. (2016). Reviewing the Implementation of Information Security Management System

Requirements in Hospitals in Tabriz in East Azarbaijan. Journal of Management and Accounting Studies, 4(1), 74-80.

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350-357.

Calder., A., & Watkins. (2008). IT Governance – A Manager's Guide to Data Security and ISO 27001 and ISO 27002 (4th edition. ed.): Kogan Page.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. Information & Computer Security, 24(2), 139-151. https://doi.org/10.1108/ICS-12-2015-0048

Daniel, A. U. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and

Information Technology, 21(1), 2-35. https://doi.org/10.1108/JSIT-02-2018-0028

Hina, S., & Dominic, D. D. (2016). Information security policies: Investigation of compliance in universities. Paper presented at the 2016 3rd International Conference on Computer and Information Sciences.

Kehoe, D. (2016). The Role of Human Resources in Managing Cybersecurity. Retrieved from https://www.telstra.com.au/content/dam/tcom/business-enterprise/campaigns/workforce-of-the-future/the-role-of-human-resources%20in-managing-cybersecruity.pdf

Kumah, P., Winfred, Y., & Charles, B.-A. (2018). Identifying HRM Practices for Improving Information Security Performance: An Importance-Performance Map Analysis. International Journal of Human Capital and Information Technology Professionals (IJHCITP), 9(4), 23-43. https://doi.org/10.4018/IJHCITP.2018100102

Kumah, P., Yaokumah, W., & Okai, E. (2019). A conceptual model and empirical assessment of HR security risk management. information and Computer Security, 27(3), 411-433. https://doi-org.sdl.idm.oclc.org/10.1108/ICS-05-2018-0057

Li, Y., & S, S., M. (2011). A Call for Research on Home Users' Information Security Behavior. Paper presented at the Pacific Asia Conference on Information Systems, Brisbane, Queensland, Australia.

Ma, Q., Schmidth, M. B., & Pearson, J. M. (2009). An integrated framework of information security management. Review of Business, 30(1), 58–69.

Malekolkalami, K. (2014). Evaluation of the central libraries information security management at governmental universities located in Tehran, according to the international standard ISO/IEC 27002 Journal of Information Processing and Management, 28(4), 895-916.

Sewuster, P. (2012). Information security in practice: The practice of using ISO 27002 in the public sector (Master thesis), University of Nijmegen,

Shaaban, H. K. (2014). Enhancing The Governance Of Information Security In Developing Countries: The Case Of Zanzibar, (PhD thesis), University of Bedfordshire, UK.

Singh, A.N, & Gupta, M. P. (2019). Information Security Management Practices: Case Studies from India. Global Business Review, 20(1), 253-271.

Stewart, H. (2017). Information security management and the human aspect in organizations. Information & Computer Security, 25(5), 494-534. https://doi.org/10.1108/ICS-07-2016-0054

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences, 11(5), 23-29.

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. Information & Computer Security, 27(3), 326-342. https://doi.org/10.1108/ICS-09-2018-0108

Tsohou, A. (2010). A security standards' framework to facilitate best practices' awareness and conformity. Information Management & Computer Security, 18(5), 350-365. https://doi.org/10.1108/09685221011095263

Wipawayangkool, K. (2010, 12-15 August). Strategic Role of Human Resource Management in Information Security Management. Paper presented at the Sixteenth Americas Conference on Information Systems, Lima, Peru.

The Role of Human Resource Management Processes in Achieving Information Security: An Applied Study on Saudi Government Universities

Mo'ath Y. Al-Thunaibat♦[1], Adnan A . Al-shawabkeh [2], Khiro K . Al-baqor [3]

Received: 26-03-2020 Accepted: 18-05-2020 Published: 21-06-2020

Abstract:

This study aims to reveal the reality of the Human Resources Management Units' contribution to achieving information security at Saudi government universities by examining their compliance with the international standard of the Information Security Management System (ISO/IEC 27002:2013). The study was based on qualitative research methods. A checklist was designed to collect the data needed for the study, using semi-structured interviews, direct observation, and document examination used in Human Resources management units. The gap analysis method has also been used to analyse data to determine the range of compliance of the university's Human Resources Management Units to the information security controls provided by the international standard (ISO/IEC 27002:2013). The study reached several results, the most important of which was the commitment of the participating universities in different rates ranging from medium to high in the application of the international standard (ISO/IEC 27002:2013) controls concerning human resources management processes (before employment, during employment, termination or change of employment). In light of those findings, the study made several recommendations that guide universities towards full compliance with controls of that international standard to raise the level of the contribution of human resources management processes to achieve complete information security.

Keywords: Human Resource Management, Information Security, International Standard: ISO/IEC 27002:2013.

JEL Classification: M15.

How to Cite: Al-Thunaibat, M. Y., Al-shawabkeh, A. A. ., & Al-baqor, K. K. . (2020). The Role of Human Resource Management Processes in Achieving Information Security: An Applied Study on Saudi Government Universities. *Management & Economics Research Journal*, *2*(3), 1-23. https://doi.org/10.48100/merj.v2i3.107 [In Arabic]

[1]♦ PhD in Management Information System Associate Professor: Taif University (kingdom of Saudi Arabia). [✉ muath@tu.edu.sa]

[2] PhD in Management Information System Associate Professor: Taif University (kingdom of Saudi Arabia). [✉ a_sahawabkeh@yahoo.com]

[3] PhD in Management Information System Associate Professor: Taif University (kingdom of Saudi Arabia).. [✉ khir15@yahoo.com]