Contents lists available at https://digitalcommons.aaru.edu.jo/huj_nas/.

Hadhramout University Journal of Natural & Applied Science

Article

Digital Object Identifier:
Received 10 May 2025,
Accepted 1 June 2025,
Available online 25 July 2025

Analyzing the Security of Student Data and Results in the Student Affairs System at Hadhramout University: Toward Enhancing Protection with Modern Technologies

Naziha Mohammed Ali Al-Aidroos

Department of Mathematics, Faculty of Education, Hadhramout University, Mukalla-Yemen

Email: naz.moh@hu.edu.ye

Abstract: This study aims to examine the current state of data and student results security in the Student Affairs System at Hadhramout University. It identifies the main security challenges facing the system and explores the potential for enhancing data protection through the adoption of modern technologies such as encryption, local storage, multi-factor authentication, and blockchain.

The study was guided by key research questions addressing the current level of data security, potential threats and risks, the extent of policy compliance, staff awareness, and the feasibility of applying modern technical solutions to strengthen data protection.

A descriptive analytical methodology was adopted. Data was collected through a structured questionnaire distributed to a sample of 27 employees working directly in the Student Affairs administration, in addition to conducting interviews with system administrators and technical personnel.

The findings revealed that while the system has an acceptable technical infrastructure and a generally sound access control mechanism, there are notable gaps in security training, weak policy enforcement, and inconsistencies in employees' awareness of existing risks and procedures. Moreover, staff confidence in system security does not always reflect an institutional reality supported by clear policies and structured training.

Recommendations were developed based on the analysis of both the questionnaire and interviews. Key proposals include: appointing a designated data protection officer, implementing encryption and multi-factor authentication, improving incident reporting procedures, enhancing monitoring and compliance, and adopting emerging technologies such as blockchain to ensure data integrity and prevent manipulation.

This research highlights the urgent need for a comprehensive data security strategy in academic institutions and serves as a foundational reference for improving security policies and system performance in Yemeni universities.

Keywords: *Data Security, Student Affairs System, Hadhramout University, Data Protection, Information Security in Universities.*

تحليل أمن بيانات ونتائج الطلاب في نظام شؤون الطلاب بجامعة حضرموت: نحو تعزيز الحماية بالتقنيات الحديثة

نزيهة محمد علي العيد روس

قسم معلم مجال رياضيات/حاسوب، كلية التربية، جامعة حضرموت، المكلا–اليمن.

الملخص: يستهدف هذا البحث دراسة واقع أمن بيانات ونتائج الطلاب في نظام شؤون الطلاب بجامعة حضرموت، وتحديد أبرز التحديات الأمنية التي تواجه هذا النظام، مع استكشاف إمكانية تعزيز حماية البيانات من خلال توظيف التقنيات الحديثة مثل التشفير، التخزين المحلي، التحقق متعدد العوامل، وتقنية البلوك تشين.

انطلقت الدراسة من تساؤلات رئيسية تناولت مستوى أمن البيانات الحالي، والمخاطر والتهديدات المحتملة، ودرجة الالتزام بالسياسات الأمنية، ووعي الموظفين، إضافة إلى مدى قابلية تطبيق تقنيات حديثة لتعزيز حماية البيانات.

أُستخدم المنهج الوصفي التحليلي، وتم جمع البيانات باستخدام استبيانه موجهة إلى عينة من الموظفين المختصين في نيابة شؤون الطلاب، شملت 27 مشاركًا، إضافة إلى إجراء مقابلات مباشرة مع عدد من المسؤولين والفنيين ذوي العلاقة المباشرة بإدارة النظام.

كشفت النتائج عن وجود بنية تقنية مقبولة وتوزيع جيد للصلاحيات، ووعي نظري عام بأهمية حماية البيانات، إلا أن الدراسة بيّنت وجود فجوات واضحة في التدريب الأمني، وضعفًا في تفعيل السياسات الأمنية وتوثيقها، وتفاوتًا في وعي الموظفين بالإجراءات الأمنية والمخاطر المحتملة. كما أظهرت النتائج أن ثقة الموظفين بإجراءات الأمان لا تعكس دائمًا واقعًا مؤسسيًا مدعومًا بسياسات واضحة أو تدريب منتظم.

بُنيت التوصيات على تحليل نتائج الاستبيانة والمقابلات، ومن أبرزها: تعيين مسؤول رسمي لحماية البيانات، تطبيق التشفير وتقنيات التحقق المتعدد، تطوير آلية الإبلاغ، تفعيل الرقابة، وتبني تقنيات ناشئة مثل البلوك تشين لضمان سلامة البيانات ومنع التلاعب بها.

يسهم هذا البحث في تسليط الضوء على الحاجة إلى استراتيجية شاملة لأمن البيانات الأكاديمية، ويُعدّ أساسًا يمكن البناء عليه لتطوير السياسات الأمنية وتحسين جودة الأنظمة التقنية في الجامعات اليمنية.

الكلمات المفتاحية: *أمن البيانات، نظام شؤون الطلاب، جامعة حضرموت، حماية البيانات، أمن المعلومات في الجامعات.*

المقدمة:

تعد البيانات الأكاديمية للطلاب أحد الأصول الحيوية التي تعتمد عليها مؤسسات التعليم العالي في تقديم خدماتها التعليمية والإدارية. ومع التوسع في استخدام الأنظمة الإلكترونية لإدارة شؤون الطلاب، مثل أنظمة التسجيل الإلكتروني، وإدارة النتائج، والسجلات الأكاديمية، تزايدت الحاجة الملحة إلى حماية هذه البيانات من المخاطر المتعددة التي تهدد سلامتها وسريتها.

وفي ظل التطور السريع للتقنيات الحديثة، أصبحت التهديدات الإلكترونية أكثر تعقيدًا، مما يجعل أنظمة شؤون الطلاب عرضة للاختراقات، أو التسريب، أو التلاعب بالمعلومات الحساسة. من هنا تنبع أهمية تعزيز إجراءات أمن البيانات، وتطوير حلول تقنية متقدمة لضمان حماية المعلومات الطلابية وضمان نزاهة العمليات الإدارية المرتبطة بها.

يأتي هذا البحث ليسلط الضوء على واقع أمن بيانات ونتائج الطلاب في نظام شؤون الطلاب بجامعة حضرموت، متناولًا التحديات الأمنية القائمة، ومستعرضًا فرص تعزيز الحماية عبر دمج أحدث التقنيات، بما يسهم في بناء بيئة تعليمية أكثر أمانًا وموثوقية.

مشكلة البحث:

في ظل الاعتماد المتزايد على الأنظمة الإلكترونية في إدارة شؤون الطلاب بجامعة حضرموت، تبرز مشكلة أساسية تتمثل في:

"مدى كفاية إجراءات حماية بيانات ونتائج الطلاب في ضمن نظام شؤون الطلاب، ومقدار الحاجة إلى تطويرها باستخدام تقنيات حديثة لضمان أمن وسرية المعلومات الأكاديمية وسريتها".

وتنطوي هذه المشكلة على عدة تساؤلات فرعية، من أبرزها:

1- ما مستوى أمن البيانات الحالي في نظام شؤون الطلاب بجامعة حضرموت؟

2- ما أبرز المخاطر الأمنية والتهديدات المحتملة التي تواجه بيانات الطلاب في ضمن هذا النظام؟

3- إلى أي مدى يتم الالتزام بتطبيق السياسات والمعايير الأمنية المتعلقة بحماية بيانات الطلاب؟

4- كيف يمكن توظيف التقنيات الحديثة، مثل التشفير، التخزين المحلي، والبلوك تشين، لتعزيز حماية بيانات الطلاب؟

5- ما درجة وعي موظفي نظام شؤون الطلاب بمبادئ أمن المعلومات؟

6- ما المقترحات الممكنة لتعزيز حماية بيانات الطلاب باستخدام حلول تقنية حديثة؟

أهداف البحث:

يستهدف هذا البحث:

1- تحليل واقع أمن بيانات ونتائج الطلاب في نظام شؤون الطلاب بجامعة حضرموت.

2- رصد أبرز التهديدات والمخاطر الأمنية التي تواجه النظام الحالي.

3- تقييم مدى التزام النظام بالمعايير والسياسات الأمنية الخاصة بحماية المعلومات.

4- استكشاف فرص تعزيز الحماية عبر تبني تقنيات حديثة مناسبة.

5- تقديم توصيات عملية لتحسين أمن البيانات وضمان استمرارية العمليات الأكاديمية بأمان وموثوقية.

أهمية البحث:

تنبع أهمية هذا البحث من عدة جوانب رئيسية:

- **أكاديميًا:** يسد فجوة معرفية حول واقع حماية بيانات الطلاب في البيئة الجامعية المحلية، ويوفر أساسًا علميًا للدراسات المستقبلية.
- **عمليًا:** يقدم مقترحات عملية قابلة للتطبيق لتحسين مستوى الأمان المعلوماتي في نظام شؤون الطلاب.
- **مؤسسيًا:** يدعم جهود جامعة حضرموت في تعزيز أمن معلوماتها، مما ينعكس إيجابًا على جودة الخدمات الأكاديمية والإدارية المقدمة للطلاب.
- **اجتماعيًا:** يسهم في حماية حقوق الطلاب المتعلقة بالخصوصية وسرية المعلومات، بما يتماشى مع المعايير الأخلاقية والقانونية.

1- الإطار النظري والدراسات السابقة:

- مفهوم أمن البيانات (Data Security) :

يُعد أمن البيانات من الركائز الأساسية لحماية المعلومات في العصر الرقمي، ويُعرف بأنه "مجموعة من السياسات والإجراءات والتقنيات المصممة لحماية البيانات من الوصول غير المصرح به، أو التعديل، أو التدمير، أو الفقدان" [1]. وتتمثل الأهداف الرئيسية لأمن البيانات في تحقيق السرية (Confidentiality)، والسلامة أو التكاملية (Integrity)، والإتاحة(Availability)، والتي تُعرف مجتمعة بمثلث أمن المعلومات (CIA). [2]

- **السرية:** تعني ضمان عدم اطلاع الأشخاص غير المخولين على المعلومات.
- **التكاملية:** تشير إلى حماية البيانات من التعديل أو التلف غير المصرح به.
- **الإتاحة** تعني ضمان إمكانية الوصول إلى المعلومات عند الحاجة دون تأخير أو تعطل.

وتتزايد أهمية أمن البيانات بشكل خاص في المؤسسات التعليمية مثل الجامعات، حيث تتعامل مع كميات ضخمة من البيانات الحساسة المرتبطة بالطلاب، بما في ذلك المعلومات الشخصية، والسجلات الأكاديمية، والبيانات المالية. وقد أظهرت العديد من الدراسات الحديثة

أن المؤسسات التعليمية أصبحت أهدافًا رئيسية للهجمات السيبرانية نظرًا لقيمة هذه المعلومات وحساسيتها. [3]

وفي هذا السياق، يُعد نظام شؤون الطلاب من أكثر الأنظمة عرضة للمخاطر نظراً لطبيعة البيانات التي يديرها، والتي تشمل عمليات التسجيل، الدرجات، الحضور، والملفات الشخصية للطلاب. لذلك، من الضروري أن تعتمد الجامعات أنظمة حماية متقدمة لنظام شؤون الطلاب، تشمل استخدام تقنيات التشفير، تطبيق سياسات التحكم في الوصول، تدريب الموظفين على معايير أمن المعلومات، وتحديث الأنظمة بشكل دوري. ووفقًا لدراسة Price [4]، فإن وجود التزام مؤسسي قوي بسياسات أمن البيانات يُعد عاملًا حاسمًا في تقليل مخاطر تسريب المعلومات وتعزيز الثقة في النظام الأكاديمي.

ومن ثم، فإن حماية بيانات الطلاب لا تحمي فقط الحقوق الفردية، بل تسهم أيضًا في تعزيز سمعة المؤسسة الأكاديمية وضمان استمرارية عملياتها الإدارية والتعليمية بأمان وكفاية.

– **نظم شؤون الطلاب في الجامعات (Student Information Systems):**

تُعد نظم شؤون الطلاب (Student Information Systems - SIS) من الركائز الأساسية لإدارة المعلومات الأكاديمية والإدارية للطلاب داخل مؤسسات التعليم العالي. يُعرَّف نظام شؤون الطلاب بأنه "نظام معلومات إلكتروني متكامل يُستخدم في المؤسسات التعليمية لجمع وتخزين وإدارة ومعالجة بيانات الطلاب، بما يشمل معلومات القبول والتسجيل، النتائج الأكاديمية، الحضور، والوثائق الرسمية، بهدف دعم العمليات الأكاديمية والإدارية وتحسين جودة الخدمات المقدمة للطلبة".

وقد بيَّن Al-Kharusi [5]، أن هذا النظام يمثل عنصرًا أساسيًا في البنية الإدارية الرقمية للمؤسسات الأكاديمية الحديثة، لما يوفره من كفاية ودقة في إدارة البيانات الطلابية.

تتكون نظم شؤون الطلاب عادةً من عدة مكونات رئيسية تشمل:

- وحدة إدارة بيانات الطلاب الشخصية (مثل الاسم، الهوية الوطنية، العنوان).
- وحدة إدارة التسجيل الأكاديمي (مثل تسجيل المواد الدراسية، تعديل الجداول).
- وحدة إدارة النتائج والتقديرات الأكاديمية.
- وحدة متابعة الحضور والسلوك.
- وحدة الشهادات والتوثيق الرسمي.
- وحدات دعم أخرى مرتبطة بالخدمات المالية والمنح الدراسية.

وتدير هذه الأنظمة مجموعة واسعة من البيانات الحيوية، أبرزها المعلومات الشخصية للطالب، سجله الأكاديمي الكامل، بيانات الحضور والغياب، التحويلات الأكاديمية، درجات الاختبارات والتقييمات، وأحيانًا حتى البيانات الصحية أو الخاصة بالخدمات الاجتماعية.

كما تؤثر نظم شؤون الطلاب تأثيرًا حيويًا في دعم اتخاذ القرار الأكاديمي والإداري داخل الجامعات. فمن خلال التحليل المستمر للبيانات الطلابية، يتمكن صانعو القرار من تحسين التخطيط الأكاديمي، متابعة الأداء الطلابي، تطوير البرامج الدراسية، تخصيص الموارد بشكل أكثر فعالية، وتقديم خدمات مخصصة لدعم احتياجات الطلاب.

مع ذلك، تواجه نظم شؤون الطلاب تحديات متزايدة في مجال حماية البيانات. فقد أشارت دراسات مثل دراسة Samuel [6] إلى أن الاعتماد المتزايد على الأنظمة الإلكترونية يجعل هذه البيانات عرضة لمخاطر الاختراقات الإلكترونية، تسرب المعلومات، وسوء الاستخدام الداخلي. ومن ثم، فإن نجاح نظم شؤون الطلاب لا يتوقف فقط على فعاليتها في إدارة العمليات الأكاديمية، بل يتطلب أيضًا مستوىً عاليًا من الحماية الأمنية لضمان سلامة وسرية بيانات الطلاب، والحفاظ على الثقة المؤسسية.

– **الهيكل التنظيمي لنظام شؤون الطلاب بجامعة حضرموت:**

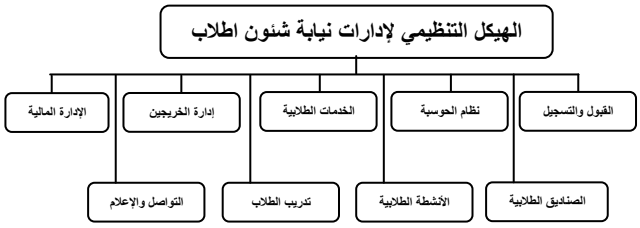
يُعد نظام شؤون الطلاب في جامعة حضرموت أحد الأنظمة الحيوية التي تدير العمليات الأكاديمية والإدارية المتعلقة بالطلاب. يتبع النظام هيكلًا تنظيميًا يشمل عدة إدارات ووحدات (شكل 1)، منها:

- **الإدارة العامة للقبول والتسجيل:** تُعد من الركائز الأساسية في الهيكل الإداري للجامعة، إذ تضطلع بإدارة شؤون الطلاب منذ لحظة قبولهم وحتى تخرجهم. وتشمل مهامها تنظيم إجراءات القبول، تسجيل المقررات الدراسية، إصدار الوثائق الأكاديمية، والإجابة عن استفسارات الطلاب. كما تُسهم في إعداد وتنفيذ اللوائح المتعلقة بالطلاب، وتنسق بشكل وثيق مع الكليات والوحدات الإدارية المختلفة لخدمة العملية التعليمية وضمان سلامة البيانات الأكاديمية.
- **الإدارة العامة لنظام حوسبة شؤون الطلاب:** تتولى تطوير وتشغيل الأنظمة المعلوماتية التقنية الخاصة بإدارة بيانات الطلاب، وتسهيل مهام موظفي القبول والتسجيل في رئاسة الجامعة والكليات. وتشمل مهامها تنظيم إجراءات القبول والتنسيق، دعم الخدمات الطلابية إلكترونيًا، وتقديم المعلومات والبيانات الأكاديمية للجهات المعنية داخل الجامعة وخارجها بدقة وكفاية عالية.
- **الإدارة العامة للخريجين:** تُعنى بمتابعة شؤون خريجي الجامعة وتعزيز التواصل المستمر معهم، بهدف توثيق الروابط بين الجامعة ومخرجاتها. وتشمل مهامها جمع بيانات الخريجين، متابعة مساراتهم المهنية، والتنسيق معهم بصفة سفراء للجامعة، بما يعكس اهتمام الجامعة برأيهم وأثرهم في المجتمع.
- **الإدارة العامة للخدمات الطلابية:** أنشئت لتلبية احتياجات الطلاب المتوافدين من مختلف المحافظات اليمنية والدول العربية والإسلامية. وتتمثل مهام هذه الإدارة في توفير خدمات التسكين

والإيواء، والنقل، والرعاية الصحية والاجتماعية، بما يضمن للطلاب بيئة جامعية مريحة تدعم مسيرتهم التعليمية.

- **الإدارة العامة للأنشطة الطلابية:** تتولى مسؤولية تنظيم وتنسيق مختلف الأنشطة اللاصفية، بما في ذلك الأنشطة الرياضية والثقافية والاجتماعية والتوعوية والكشفية. وتستهدف تنمية شخصية الطالب وتوفير بيئة داعمة تساعده على التكيّف مع الحياة الجامعية، من خلال إعداد برامج تربوية متكاملة تعزز القيم الإسلامية، وتشجع الإبداع، وتبرز المواهب الطلابية عبر فعاليات سنوية تسهم في دمج الجامعة بالمجتمع المحلي وتحفيز الطلبة على التميز.
- **الإدارة العامة لتدريب الطلاب:** تُعنى بتأهيل طلاب الجامعة وخريجيها من خلال تنفيذ برامج تدريبية متخصصة، تستهدف ربط الجانب الأكاديمي بالمهارات العملية المطلوبة في سوق العمل. وتشمل مهامها التنسيق مع الجهات ذات العلاقة داخليًا وخارجيًا لتوفير فرص تدريب ملائمة، وتطوير قدرات الطلاب بما يعزز جاهزيتهم للحياة المهنية بعد التخرج.
- **إدارة التواصل والإعلام:** تضطلع الإدارة العامة للإعلام والتواصل في نيابة شؤون الطلاب بأثر محوري في تعزيز صورة الجامعة داخليًا وخارجيًا، من خلال تنفيذ خطة استراتيجية للتواصل مع الطلاب والخريجين والشركاء والجهات ذات العلاقة. وتشمل مهامها نشر الأخبار والفعاليات عبر الموقع الإلكتروني الرسمي، وتغطية المناسبات الإعلامية، وبناء علاقات تفاعلية تسهم في ترسيخ الصورة الإيجابية للجامعة وتعزيز حضورها الإعلامي في المجتمع.
- **الإدارة المالية:** تتولى مسؤولية تنفيذ كافة العمليات المالية المرتبطة بالنيابة، بما في ذلك صرف الميزانية، وتحصيل الإيرادات، وتوثيقها محاسبيًا وفق اللوائح والأنظمة المعتمدة. كما تقدم خدماتها للجهات الداخلية والخارجية المتعاملة مع الجامعة، وتسعى لإنجاز المعاملات بدقة وسرعة.
- **وحدة الصناديق الطلابية:** وقد أُنشئت بهدف تنسيق عمل الصناديق المخصصة لدعم الطلبة. وتشرف الوحدة على صندوق الرعاية الاجتماعية، الذي يُعنى بتقديم الخدمات الصحية والاجتماعية لطلاب الجامعة، وصندوق تدريب الطلاب، الذي يركز على تطوير مهاراتهم في المجالات العلمية والإبداعية، بما يسهم في دعم مسيرتهم الأكاديمية والمهنية.

من خلال استعراض مهام الإدارات التابعة لنيابة شؤون الطلاب، يُلاحظ أن الإدارات التي تقع في ضمن نطاق البحث بشكل مباشر هي الإدارة العامة للقبول والتسجيل بوصفها الجهة الأساسية المسؤولة عن إدخال ومعالجة بيانات ونتائج الطلاب، إلى جانب الإدارة العامة لنظام حوسبة شؤون الطلاب الجهة الفنية المسؤولة عن تشغيل النظام الإلكتروني، لما لهما من أثر مباشر في إدارة البيانات الأكاديمية الحساسة المرتبطة بالطلاب وسجلاتهم التعليمية.



شكل 1. الهيكل التنظيمي لإدارات نيابة شئون اطلاب.

– لمحة عن نظام شؤون الطلاب الإلكتروني بجامعة حضرموت:

يعتمد نظام شؤون الطلاب الإلكتروني في جامعة حضرموت على منصة حوسبة مركزية داخلية تم تطويرها محليًا بإشراف الإدارة الفنية التابعة لنيابة شؤون الطلاب. يستهدف هذا النظام رقمنة العمليات المتعلقة بالقبول والتسجيل، وإدارة بيانات الطلاب الأكاديمية، وإصدار النتائج، وتنظيم ملفات الخريجين، مما يسهم في تسريع الإجراءات وتقليل الاعتماد على المعاملات الورقية.

آلية الوصول:

- يتم الوصول إلى النظام عبر شبكة الجامعة الداخلية أو بوابة إلكترونية خاصة.
- يُمنح كل مستخدم صلاحيات وصول بحسب المهام الوظيفية (مدخل بيانات، مراجع، مشرف... إلخ).

مستوى الحماية المطبق حاليًا:

- يعتمد النظام حاليًا على حماية أساسية بكلمات مرور خاصة، مع تسجيل دخول مميز لكل مستخدم.
- لا توجد آليات تحقق متعددة العوامل (MFA).
- عمليات النسخ الاحتياطي تُنفذ بشكل دوري.

تشير هذه المعطيات إلى وجود أساس بنية رقمية جيد، لكنه بحاجة إلى تعزيز عبر تقنيات أكثر تطورًا، وهو ما سعت هذه الدراسة إلى تقييمه واقتراح تطويره.

– التهديدات الأمنية لبيانات الطلاب في نظم شؤون الطلاب:

التهديدات الأمنية تشير إلى أية أحداث أو ظروف قد تعرض أمن المعلومات للخطر، سواء كانت تهديدات داخلية ناتجة عن أخطاء

بشرية أو سوء استخدام، أو تهديدات خارجية مثل الهجمات الإلكترونية، أو الأعطال التقنية أو الكوارث الطبيعية.

يُعد نظام شؤون الطلاب أحد أهم الأنظمة الإلكترونية في المؤسسات الجامعية، كونه يحوي قواعد بيانات حساسة تتعلق بمعلومات الطلاب الشخصية، والأكاديمية، والمالية، وغيرها من البيانات ذات الطابع السري. ومع الاعتماد المتزايد على الرقمنة في إدارة شؤون القبول، والتسجيل، وإعلان النتائج، أصبحت هذه النظم هدفًا مباشرًا للتهديدات الأمنية، سواء كانت داخلية ناتجة عن سلوكيات بشرية غير منضبطة، أو خارجية بفعل هجمات إلكترونية منظمة.

وتتمثل أبرز التهديدات التي تواجه نظام شؤون الطلاب في اختراق الحسابات والصلاحيات الإدارية، والتلاعب بالدرجات أو تعديل البيانات دون تفويض، وتسريب المعلومات الخاصة بالطلاب أو استغلالها لأغراض غير مشروعة. كما أن الإهمال في تطبيق سياسات الوصول أو ضعف الوعي الأمني قد يؤدي إلى كوارث تقنية وإدارية يصعب احتواؤها، خاصة إذا لم يكن هناك نسخ احتياطي أو إجراءات استجابة فعالة.

إن تحليل هذه التهديدات لا يكتفي بتتبع مصدرها، بل يتطلب أيضًا فهمًا للسياق المؤسسي والإداري الذي يسمح بحدوثها أو يمنعها، مما يجعل أمن نظام شؤون الطلاب مسألة تقنية وإدارية وسلوكية في آنٍ واحد.

وقد تم تصنيف هذه التهديدات إلى عدة أنواع رئيسية:

1. التهديدات الداخلية وسلوك الموظفين

تُعد التهديدات الداخلية من أخطر التحديات التي تواجه أمن البيانات داخل مؤسسات التعليم العالي، حيث تنبع من داخل المؤسسة ذاتها، عبر موظفين أو مستخدمين يمتلكون صلاحيات واسعة للوصول إلى المعلومات الحساسة، مما يعرض البيانات الطلابية الحساسة لمخاطر كبيرة.

وتشير الدراسات إلى أن سلوك الموظفين والمستخدمين داخل المؤسسة، سواء عن قصد أو بسبب الإهمال، قد يُشكل مصدرًا مباشرًا لاختراق الخصوصية أو تسريب البيانات. فقد بيّنت دراسة Earp و Payton [7] أن ضعف الوعي بسياسات حماية الخصوصية قد يؤدي إلى تصرفات تعرض البيانات الأكاديمية للخطر، مثل مشاركة كلمات المرور أو استخدام أدوات غير مؤمنة.

وتشمل التهديدات الداخلية الشائعة ما يلي:

- **نقص الوعي الأمني:** ويشمل التصرفات الناتجة عن الجهل أو الإهمال، مثل ترك الحواسيب دون حماية، أو تحميل الملفات الحساسة في وسائط غير مؤمّنة.
- **مشاركة بيانات الدخول:** ما يسهل الوصول غير المشروع إلى أنظمة شؤون الطلاب.
- **سوء الاستخدام المتعمد:** كالوصول إلى بيانات الطلاب دون مبرر وظيفي، أو تسريبها لطرف خارجي.
- **الاعتماد على أجهزة غير مؤمنة:** مثل استخدام حواسيب شخصية أو شبكات عامة دون حماية مناسبة.

ويزداد أثر هذه التهديدات في غياب برامج توعية فعّالة أو سياسات رقابية صارمة. وتشير الأبحاث إلى أن تعزيز ثقافة أمنية داخل المؤسسة، من خلال التدريب المستمر والتدقيق المنتظم، يُعد من الوسائل الفعّالة للحد من المخاطر الناجمة عن السلوك البشري داخل النظام.

2. التهديدات التقنية الخارجية

تواجه أنظمة شؤون الطلاب في الجامعات تهديدات تقنية متزايدة، أبرزها:

- **البرمجيات الخبيثة (Malware)**: تُستخدم لاختراق الأنظمة وسرقة البيانات أو تعطيل الخدمات .
- **هجمات الفدية (Ransomware)**: يقوم المهاجمون بتشفير البيانات وطلب فدية لفك التشفير .
- **التصيد الإلكتروني (Phishing)** : تُستخدم لخداع الموظفين للحصول على بيانات الدخول.

تشير الدراسات إلى أن مؤسسات التعليم العالي تُعد أهدافًا رئيسية لهذه الهجمات، حيث أبلغت نسبة كبيرة من الجامعات عن تعرضها لهجمات فدية ناجحة، مما يعرض بيانات الطلاب للخطر ويؤثر في استمرارية الخدمات التعليمية. [8]

1. التهديدات المرتبطة بسوء إدارة النظام

وتحدث هذه التهديدات عندما يُستخدم النظام بطريقة تتجاوز الأذونات أو تخالف السياسات الأمنية. من امثلة هذه التهديدات [9]:

- عدم وجود نسخ احتياطية منتظمة: مما يعرض البيانات للفقدان في حال حدوث خلل.
- غياب سياسات واضحة لإدارة الوصول: مما يسمح بالوصول غير المصرح به للمعلومات الحساسة .
- تحميل بيانات حساسة على منصات غير آمنة.

- نقص التدريب والتوعية: مما يؤدي إلى أخطاء بشرية تؤثر في أمن البيانات .

2. ضعف البنية التحتية والتقنيات القديمة

تعتمد بعض الجامعات على أنظمة معلومات طلابية قديمة تفتقر إلى التحديثات الأمنية اللازمة، مما يجعلها عرضة للاختراقات. غياب التشفير القوي، واستخدام كلمات مرور ضعيفة، وعدم وجود تحكم صارم في الوصول، كلها عوامل تزيد من مخاطر تسريب البيانات. [10]

3. تهديدات ناجمة عن الكوارث الطبيعية أو الأعطال التقنية

رغم أنها ليست هجمات متعمدة، إلا أن الأعطال المفاجئة أو الكوارث الطبيعية (مثل الحرائق أو السيول) قد تؤدي إلى فقدان أو تسريب بيانات الطلاب، خاصة إذا لم تكن هناك خطط نسخ احتياطي واستعادة مناسبة. أوصت دراسة Feng [11] بتطوير خطط شاملة للتعافي من الكوارث لحماية البيانات الأكاديمية .

– التقنيات الحديثة لتعزيز حماية بيانات الطلاب في نظم شؤون الطلاب

مع تصاعد المخاطر المرتبطة بأمن البيانات في المؤسسات التعليمية، تزايدت الحاجة إلى اعتماد تقنيات حديثة تعزز حماية المعلومات، خصوصًا داخل الأنظمة الحساسة مثل نظم شؤون الطلاب، التي تُعد المخزن المركزي لبيانات الطلاب الأكاديمية والشخصية. هذه الأنظمة أصبحت أهدافًا مغرية للهجمات الإلكترونية بسبب ما تحتويه من معلومات ذات طابع حساس، مما يتطلب بنية تقنية متطورة وإجراءات أمان متعددة الطبقات.

1. التشفير (Encryption) :

يُعد التشفير من أهم الأدوات التقنية لحماية البيانات في أثناء التخزين أو النقل. وهو يعتمد على تحويل البيانات إلى صيغة غير قابلة للقراءة دون وجود مفتاح فك التشفير، مما يضمن سرية المعلومات حتى لو تم الوصول إليها بطرائق غير مشروعة. وقد استخدمت Zainudin وآخرون [12] خوارزمية AES في ضمن نظام سحابي لحماية ملفات الطلاب، وأظهرت نتائجهم فعالية التشفير في تقليل احتمالية تسرب البيانات.

2. التخزين المحلي مقابل التخزين السحابي:

تواجه المؤسسات خيارين رئيسيين في تخزين بيانات الطلاب: التخزين السحابي أو المحلي. ورغم أن السحابة تتيح سهولة الوصول والتوسع، إلا أنها تثير مخاوف تتعلق بالخصوصية والسيطرة على البيانات.

3. تقنية البلوك تشين (Blockchain) في حماية بيانات الطلاب:

تُعد تقنية البلوك تشين واحدة من أكثر الابتكارات الواعدة في مجال حماية البيانات، بفضل خصائصها المتمثلة في الشفافية، وعدم قابلية التعديل، وسهولة التتبع. أظهرت دراسة Yang وWang [13] أن دمج البلوك تشين في نظام شؤون الطلاب عزز الأمان بنسبة 87% مقارنةً بالأنظمة التقليدية، ومنع التلاعب بسجلات الدرجات أو السجلات الأكاديمية.

ويمكن للجامعات، ومنها جامعة حضرموت، الاستفادة من هذه التقنية في تأمين عمليات تسجيل النتائج، والتحقق من صحة الشهادات الأكاديمية، ومنع التلاعب بسجلات الطالب الأكاديمية، مما يُمثل نقلة نوعية نحو نظام أكاديمي أكثر موثوقية.

4. التحقق متعدد العوامل (Multi-Factor Authentication) :

أصبح استخدام أنظمة التحقق متعددة العوامل ضرورة لحماية الأنظمة من الدخول غير المصرح به. لا يكفي الاعتماد على اسم المستخدم وكلمة المرور، بل يجب تضمين عناصر تحقق إضافية مثل رموز ترسل للهاتف أو تطبيقات مصادقة، وهو ما يقلل من فرص الاختراق حتى في حال تسريب بيانات الدخول. وقد أوصت دراسة DeLong وآخرون [14] بضرورة تطبيق هذا النوع من التحقق في ضمن الشبكات الجامعية الحساسة .

5. النسخ الاحتياطي وخطط التعافي من الكوارث:

تشكل النسخ الاحتياطية المنتظمة وخطط استعادة البيانات من الكوارث إحدى ركائز الأمن المعلوماتي. أظهرت دراسة [11] Feng أن العديد من الأرشيفات الجامعية عرضة للفقد أو التلف بسبب غياب خطط فعالة للتعافي من الكوارث، وأوصت باستخدام تقنيات حديثة للنسخ الآلي والتخزين خارج الموقع .

إن دمج هذه التقنيات داخل نظم شؤون الطلاب لا يقتصر فقط على حماية المعلومات، بل يسهم في تعزيز ثقة الطلاب والإداريين بالنظام، ويقلل من المخاطر القانونية والمؤسسية المرتبطة بتسريب البيانات أو اختراقها.

– الدراسات السابقة

تناولت العديد من الدراسات قضايا أمن بيانات الطلاب في مؤسسات التعليم العالي، مما يعكس الأهمية المتزايدة لحماية المعلومات الشخصية والأكاديمية في ظل التحول الرقمي والتوسع في استخدام الأنظمة الإلكترونية. وقد اختلفت هذه الدراسات في زوايا معالجتها

للموضوع، بين تطوير الأنظمة الآمنة، وتحليل مستوى الوعي المؤسسي، واستكشاف أثر التقنيات الحديثة في حماية البيانات، وتحليل التهديدات السيبرانية المتنامية في البيئات الجامعية.

فيما يتعلق بتطوير نظم معلومات الطلاب، سعى Samuel [6] إلى بناء نظام آمن لإدارة بيانات الطلاب باستخدام إطار عمل Laravel مزود بميزات حماية متقدمة مثل التشفير وإدارة كلمات المرور والحماية من هجمات حقن SQL ، مما يعزز سلامة البيانات في البيئات الجامعية. كما صمم Ramya و Ranjith [15] نظامًا لإدارة معلومات الطلاب (SIMS) يستهدف تقليل الأخطاء اليدوية وتحسين الشفافية من خلال أتمتة العمليات الأكاديمية. وفي ذات السياق، استكشف Yang و Wang [13] توظيف تقنية البلوك تشين في نظم إدارة معلومات الطلاب، حيث أثبتت الدراسة زيادة أمان النظام بنسبة 87% مقارنة بالأنظمة التقليدية. إضافة إلى ذلك، طور Zainudin وآخرون [12] نظامًا يعتمد على خوارزمية AES لتأمين تخزين الملفات الأكاديمية في بيئات السحابة الإلكترونية، مما عزز من خصوصية وسرية المعلومات.

أما على صعيد الوعي المؤسسي بالمخاطر، فقد تناولت عدة دراسات تصورات الموظفين والتحديات التي تواجه السياسات الأمنية. حلل Earp و Payton [7] تصورات موظفي الجامعات حول خصوصية بيانات الطلاب، وأظهرت النتائج وجود قلق حقيقي بشأن الوصول غير المصرح به للمعلومات، مع الإشارة إلى قصور السياسات الحالية في مواجهة التطورات التقنية السريعة. كما أوضحت دراسة Jones [16] أن بعض الجامعات تستمر في استخدام أرقام الضمان الاجتماعي كمعرفات للطلاب، مما يزيد من احتمالية سرقة الهوية، مؤكدة أهمية تدريب الموظفين على حماية الخصوصية. من جانب آخر، ناقش Stahl وKarger [17] التحديات المتعلقة بخصوصية بيانات الطلاب في بيئات التعلم الرقمية، مع التركيز على خصوصية بيانات الطلاب ذوي الاحتياجات الخاصة، مشيرين إلى التحديات المرتبطة بحماية هذه الفئة الحساسة في بيئات التعلم الرقمية. كذلك، تناولت دراسة Price [4] العلاقة بين الالتزام المؤسسي وسلوكيات حماية البيانات، مؤكدة أن السياسات الرسمية والتدريب المستمر يعززان من وعي الموظفين وقدرتهم على حماية المعلومات الحساسة. وفي إطار أثر خصائص أمن المعلومات في الأداء المؤسسي، بينت دراسة عوض الله [2] أن تحقيق التميز المؤسسي يعتمد بدرجة كبيرة على السرية والتكاملية والإتاحة الفعالة للمعلومات، مما يبرز أهمية تبني معايير صارمة لحماية البيانات داخل الجامعات.

وفيما يتعلق باستخدام التقنيات الحديثة وأثرها في أمن البيانات، ناقش McKelvey [18] المخاطر الناجمة عن استخدام الحوسبة السحابية وتقنيات القياسات الحيوية في الجامعات، مؤكدًا على ضرورة وجود سياسات تحكم صارمة لحماية البيانات الطلابية. كما قدم Amo وآخرون [19] إطار عمل LEDA الذي يركز على أولوية التخزين والمعالجة المحلية للبيانات بدلاً من الاعتماد الكامل على الحوسبة السحابية، مما يقلل من مخاطر تسرب البيانات.

وقد سلطت بعض الدراسات الضوء على التهديدات السيبرانية العامة التي تواجه الجامعات. حيث وثق Ulven وWangen [3] أبرز هذه التهديدات، مثل التصيد الاحتيالي والبرمجيات الخبيثة واستغلال الثغرات الأمنية، مشيرين إلى قصور استراتيجيات الأمن السيبراني في مؤسسات التعليم العالي. كما حلل Li وآخرون [20] العوامل المؤثرة في حوادث خرق البيانات، مؤكدين أن استخدام التخزين السحابي الآمن والتقليل من الإفصاح عن الثغرات يقلل من احتمالية الاختراق. وفي مجال حماية البيانات البحثية، أوضح Peisert [1] أهمية الجمع بين الحلول التقنية والسياسات التنظيمية لتعزيز سرية البيانات. واستعرض DeLong وآخرون [14] تجربة جامعة Duke في إنشاء شبكة محمية لحماية البيانات البحثية الحساسة، مع إبراز أهمية التعاون بين الفنيين والمستخدمين.

وفي سياق أهمية حماية السجلات الأكاديمية التاريخية، ناقش Feng [11] التحديات التي تواجه أرشيف الجامعات في ظل التحول الرقمي، مشددًا على أهمية تطوير خطط نسخ احتياطي واستراتيجيات تعافي من الكوارث لضمان سلامة البيانات وسريتها.

بشكل عام، تعكس هذه الدراسات السابقة مدى تنوع التحديات التي تواجه أمن بيانات الطلاب، سواء على مستوى الأنظمة أو الأفراد أو التقنيات، مما يبرز الحاجة إلى تطوير حلول متكاملة تأخذ في الاعتبار الأبعاد التقنية والتنظيمية والإنسانية لحماية هذه البيانات الحيوية في بيئات التعليم العالي.

3. منهجية الدراسة وأدواتها:

منهج الدراسة

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، لكونه الأنسب لطبيعة البحث الذي يستهدف تقييم مستوى أمن البيانات

في نظام شؤون الطلاب بجامعة حضرموت، والتعرف على واقع الممارسات الأمنية المتبعة، وتحديد أوجه القصور واقتراح حلول تقنية حديثة لتعزيز حماية البيانات.

مجتمع الدراسة

يتكون مجتمع الدراسة من جميع الموظفين العاملين في نيابة شؤون الطلاب بجامعة حضرموت، ممن لديهم صلة مباشرة بإدارة أو إدخال أو معالجة بيانات الطلاب عبر النظام الإلكتروني، وبشكل خاص:

- **الإدارة العامة للقبول والتسجيل**، باعتبارها الجهة المسؤولة عن إدخال وتحديث وتوثيق السجلات الأكاديمية للطلاب، والمرتبطة ارتباطًا وثيقًا بجميع الكليات والبرامج التعليمية.
- **الإدارة العامة لنظام حوسبة شؤون الطلاب**، نظرًا لأثرها المحوري في إدارة النظام الإلكتروني الذي تتم من خلاله جميع عمليات تسجيل الطلاب ومعالجة نتائجهم وحفظ بياناتهم.

تُعد هذه الجهات جوهرية في الدراسة، نظرًا لمسؤوليتها المباشرة عن إدارة البيانات الأكاديمية الحساسة للطلاب، والتي تمثل محور البحث فيما يتعلق بأمن البيانات وإمكانية تعزيز الحماية.

عينة الدراسة

تم اعتماد العينة الكلية لمجتمع الدراسة، نظرًا لمحدودية عدد الأفراد المتعاملين فعليًا مع نظام شؤون الطلاب.

وقد تم توزيع الاستبانة على جميع أفراد المجتمع، وتم الحصول على استجابات فعالة من (27) مشاركًا يمثلون وظائف متنوعة تشمل إداريين، مدخلي بيانات، فنيين، ومشرفين على النظام.

كما تم اختيار عينة قصدية من بعض الموظفين ممن لديهم خبرة مباشرة أو مسؤولية وظيفية فنية/إدارية متقدمة لإجراء مقابلات نوعية معهم، وذلك بهدف تعميق فهم نتائج الاستبانة، واستخلاص التحديات والمقترحات بشكل تفصيلي.

أدوات الدراسة

تم استخدام أداتين رئيسيتين لجمع البيانات:

1. الاستبانة:

أُعدت استبانة مكونة من (6) محاور تغطي الجوانب الآتية: البيانات العامة للمشاركين، البنية التقنية للنظام، السياسات والإجراءات الأمنية، وعي الموظفين بأمن البيانات، التهديدات والمخاطر الفعلية، ومقترحات التحسين. وقد اشتملت على (25) فقرة مغلقة باستخدام مقياس ليكرت الخماسي، بالإضافة إلى سؤال مفتوح في نهاية الاستبانة.

2. المقابلات:

وُجهت إلى عدد من الموظفين المختصين، وتناولت محاور ذات طابع تفسيري أعمق تتعلق بإجراءات الحماية المتبعة، مستوى الالتزام بالسياسات، أبرز التحديات التي يواجهها النظام، والرؤى المستقبلية للتحسين.

صدق وثبات الأداة

صدق الأداة:

تم عرض الاستبانة على مجموعة من المختصين في مجالي أمن المعلومات والإدارة الأكاديمية، بهدف التأكد من وضوح الصياغة وسلامة الترتيب المنطقي للفقرات، ومدى ملاءمتها لأهداف الدراسة ومحاورها وقد تم أخذ ملاحظاتهم القيمة بعين الاعتبار في الصياغة النهائية للاستبانة .

ثبات الأداة:

نظرًا لاعتماد الباحثة على عينة تتكون من الموظفين ذوي العلاقة المباشرة بنظام شؤون الطلاب في جامعة حضرموت، فقد تم التركيز على تحقيق الاتساق المنطقي واللغوي الداخلي لأداة الاستبانة أكثر من التركيز على المعالجات الإحصائية لمعاملات الثبات.

كما تم اختبار الأداة مبدئيًا على عدد محدود من الموظفين لتقييم مدى قابلية الفهم والتفاعل معها، مما ساعد على تعزيز وضوحها وضمان دقتها.

وعليه، تُعد الأداة مستقرة ومناسبة لأغراض الدراسة الوصفية والتحليلية، خاصة في ظل حجم المجتمع الصغير الذي تم استهدافه بالكامل.

حدود الدراسة

الحدود الموضوعية:

تركز الدراسة على أمن بيانات ونتائج الطلاب فقط في نظام شؤون الطلاب، ولا تشمل الجوانب المالية أو الأنشطة أو الرعاية أو بيانات الخريجين.

الحدود البشرية:

تقتصر العينة على موظفي الإدارة العامة للقبول والتسجيل وموظفي إدارة حوسبة شؤون الطلاب، ممن لديهم صلة مباشرة بالبيانات الأكاديمية.

الحدود المكانية:

أُجريت الدراسة في رئاسة جامعة حضرموت في ضمن نيابة شؤون الطلاب، كميدان تطبيقي لتقييم أمن النظام.

الحدود الزمانية:

تم تنفيذ هذه الدراسة خلال الفصل الدراسي الثاني من العام الجامعي 2025/2024م.

4. نتائج الدراسة وتفسيرها:

أولاً: خصائص المشاركين في الدراسة:

شارك في الاستبانة موظفو نيابة شؤون الطلاب بجامعة حضرموت، وتوزعوا بحسب الوظيفة الحالية كما هو موضح في جدول (1).

جدول 1. توزيع العينة وفق الوظيفة الحالية.

الوظيفة الحالية	التكرار	النسبة المئوية
مدخل بيانات	12	%44.4
مسئول إداري	10	%37.0
فني تقني	5	%18.5

يعكس هذا التوزيع تنوع المهام داخل النظام، ويُظهر أن معظم المشاركين لديهم ارتباط مباشر أو إشرافي ببيانات الطلاب، مما يعزز موثوقية النتائج المتعلقة بواقع حماية البيانات في النظام.

يوضح جدول (2) توزيع المشاركين في الاستبانة بحسب عدد سنوات خبرتهم في استخدام نظام شؤون الطلاب.

جدول 2. توزيع المشاركين وفق عدد سنوات الخبرة في التعامل مع نظام شؤون الطلاب.

عدد سنوات الخبرة في التعامل مع نظام شؤون الطلاب	التكرار	النسبة المئوية
أكثر من 6 سنوات	14	51.9%
4–6 سنوات	3	11.1%
1 – 3 سنوات	8	29.6%
أقل من سنة	2	7.4%

تشير هذه التوزيعات إلى أن آراء المشاركين تستند في معظمها إلى **خبرة تراكمية عملية** في النظام، مما يعزز موثوقية التقييمات المقدمة حول فعالية النظام ومواطن القصور في أمن البيانات.

لمعرفة مدى تأهيل الموظفين على استخدام نظام شؤون الطلاب، طُرح سؤال مباشر حول ما إذا كان المشاركون قد تلقوا تدريبًا رسميًا عند بدء استخدام النظام. يُوضح الجدول (3) نتائج الإجابات:

جدول 3. هل تلقى الموظفون تدريبًا على استخدام نظام شؤون الطلاب؟

الخيار	التكرار	النسبة المئوية
نعم	21	%77.8
لا	6	%22.2

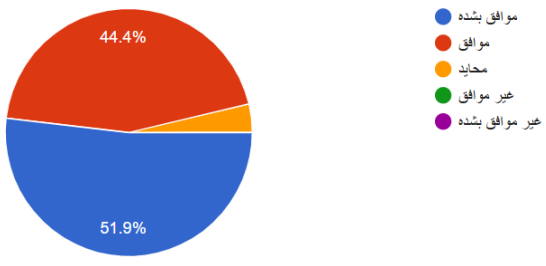
تُشير البيانات إلى أن الغالبية العظمى من الموظفين قد تلقوا تدريبًا رسميًا، مما يدل على وجود جهود تنظيمية لتأهيل الكوادر المعنية بإدارة بيانات الطلاب. إلا أن وجود نسبة تقارب الربع لم تتلقَ تدريبًا، يُعد مؤشرًا على احتمال وجود فجوات في التغطية التدريبية، أو عدم شمول البرامج لجميع الموظفين، خاصةً الجدد أو من نُقلوا حديثًا للعمل في ضمن النظام.

يُمكن أن يُؤثر ذلك في فعالية استخدام النظام وتطبيق الضوابط الأمنية المرتبطة به، مما يستدعي وضع آلية واضحة لتدريب الموظفين الجدد، وتحديث معلومات الموظفين القدامى في ضمن برامج دورية إلزامية.

ثانيًا: البنية التقنية للنظام:

1. وجود صلاحيات محددة لكل مستخدم:

أشارت نتائج الاستبانة الموضحة في شكل (2) وجدول (4)، إلى وجود مستوى عالٍ من الاتفاق بين المشاركين على أن النظام يوفّر صلاحيات دخول محددة لكل مستخدم، حيث تجاوزت نسبة الموافقة الكلية 96%. يُظهر ذلك أن بنية النظام تدعم مبدأ تقييد الوصول بناءً على المهام الوظيفية، وهو أحد المبادئ الأساسية في أمن المعلومات. أما النسبة الضئيلة من المحايدين (3.7%) فقد تعكس عدم وضوح في الصلاحيات بالنسبة لبعض المستخدمين، أو ضعفًا في التواصل بشأن آليات التفويض داخل النظام.



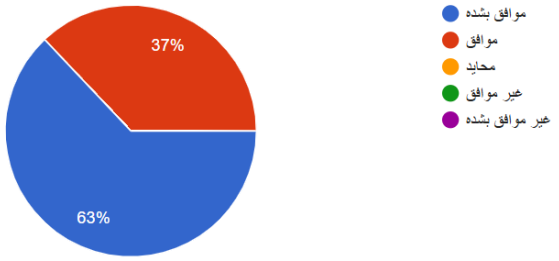
شكل 2. آراء المشاركين حول توفر صلاحيات وصول محددة للمستخدمين.

جدول 4. توزيع إجابات المشاركين بشأن احتواء النظام على صلاحيات محددة لكل مستخدم.

الخيار	التكرار	النسبة المئوية
موافق بشدة	14	%51.9
موافق	12	%44.4
محايد	1	%3.7
غير موافق	0	%0
غير موافق بشدة	0	%0

2. توفر وسائل التحقق من الهوية عند الدخول إلى النظام

تضمن الاستبانة سؤالًا حول وجود إجراءات تحقق من الهوية عند الدخول إلى نظام شؤون الطلاب، بهدف قياس مستوى الأمان المتبع في الوصول إلى البيانات كما هو موضح في شكل (3) وجدول (5).



شكل 3. آراء المشاركين حول توفر وسائل تحقق من الهوية عند الدخول إلى النظام.

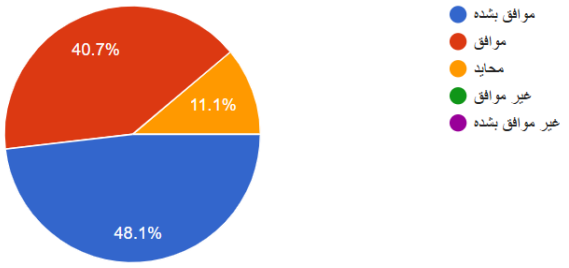
جدول 5. توزيع إجابات المشاركين بشأن توفر وسائل تحقق من الهوية عند الدخول للنظام.

الخيار	التكرار	النسبة المئوية
موافق بشدة	17	%63
موافق	10	%37
محايد	0	%0
غير موافق	0	%0
غير موافق بشدة	0	%0

تُظهر النتائج رضا شبه تام من المشاركين عن آليات التحقق الحالية، وهو ما يُشير إلى فاعلية الإجراءات المطبقة – على الأقل في صورتها الأساسية – مثل استخدام كلمات المرور المؤسسية. ومع ذلك، فإن غياب أي تقييم نقدي (0% لخياري الرفض) قد لا يعكس فقط جودة النظام، بل قد يُشير أيضًا إلى ضعف في إدراك المشاركين لخيارات الحماية المتقدمة، كالمصادقة متعددة العوامل (MFA) أو تقنيات التحقق البيومتري. كما أن نسبة كبيرة من المستجيبين من فئة موظفي إدخال البيانات – والذين يستخدمون النظام بشكل يومي – قد تفسر هذا الاتجاه الإيجابي، نتيجة اعتيادهم على النظام وسهولة استخدامه، حتى إن لم يكن بالضرورة الأعلى أمانًا.

3. النسخ الاحتياطي الدوري للبيانات

تضمّن الاستبانة سؤالًا حول ما إذا كان نظام شؤون الطلاب يوفّر نسخًا احتياطيًا دوريًا للبيانات، وهو من أبرز مؤشرات استمرارية العمل وحماية البيانات. وكما يوضّح كل من الشكل (4) والجدول (6)، فقد عبّر معظم المشاركين عن ثقتهم بوجود هذه الممارسة، حيث صرّح أكثر من 88% من الموظفين بأنهم "موافقون" أو "موافقون بشدة"، بينما عبّر 11.1% فقط عن موقف محايد، دون تسجيل أي نسب لخيارات الرفض.



شكل 4. آراء المشاركين حول النسخ الاحتياطي الدوري لبيانات الطلاب.

جدول 6. توزيع إجابات المشاركين بشأن وجود نسخ احتياطي دوري ضمن نظام شؤون الطلاب.

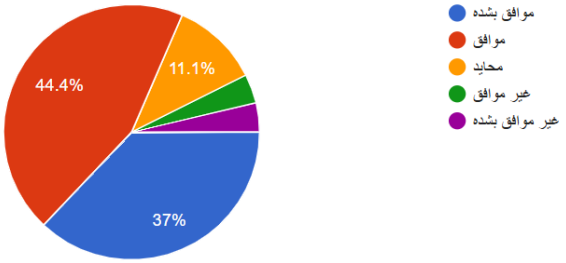
الخيار	التكرار	النسبة المئوية
موافق بشدة	13	%48.1
موافق	11	%40.7
محايد	3	%11.1
غير موافق	0	%0
غير موافق بشدة	0	%0

تعكس هذه النتائج تصوّرًا إيجابيًا عن البنية التقنية للنظام، ووجود إجراءات احترازية تهدف لحماية بيانات الطلاب من الفقدان أو

التلف. إلا أن النسبة المحايدة – رغم محدوديتها – قد تُشير إلى غموض في السياسات التقنية، أو إلى ضعف في التواصل المؤسسي بشأن طبيعة النسخ الاحتياطي (مثل التكرار الزمني أو نوعية التخزين)، مما يستدعي تحسين التوعية أو التوثيق الفني لدى المستخدمين غير التقنيين.

4. تحديث النظام والبرمجيات بشكل منتظم

شمل الاستبانة سؤالًا حول انتظام تحديث النظام والبرمجيات في نظام شؤون الطلاب، باعتداد ذلك عنصرًا محوريًا في حماية البيانات وضمان أداء مستقر للنظام. وكما هو موضح في الشكل (5) والجدول (7)، فإن غالبية المشاركين عبّروا عن تقييم إيجابي لهذا الجانب.



شكل 5. آراء المشاركين حول انتظام تحديث النظام والبرمجيات.

جدول 7. توزيع إجابات المشاركين بشأن تحديث النظام والبرمجيات.

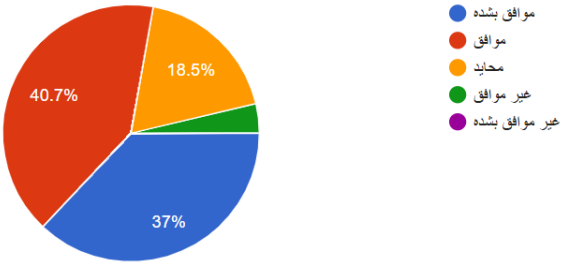
الخيار	التكرار	النسبة المئوية
موافق بشدة	10	%37
موافق	12	%44.4
محايد	3	%11.1
غير موافق	1	%3.7
غير موافق بشدة	1	%3.7

تُشير هذه النتائج إلى أن أكثر من 81% من العينة ترى أن هناك تحديثًا منتظمًا للنظام، مما يعكس مستوى مقبولًا من الثقة في أداء البنية التقنية. ومع ذلك، فإن نسبة المشاركين الذين اتخذوا موقفًا محايدًا أو رافضًا – وإن كانت محدودة – قد تُشير إلى أحد أمرين: إما ضعف التواصل حول إجراءات التحديث بين الفريق الفني وبقية الموظفين، أو غياب سياسة رسمية معلنة تُحدد آلية وجدولة تلك التحديثات.

لذا فإن تعزيز الوعي المؤسسي بالتحديثات التقنية وتوثيقها في ضمن سياسة معلنة يُعد أمرًا مهمًا لرفع مستوى الشفافية وتعزيز الثقة بين المستخدمين والنظام.

5. وجود قسم تقني متخصص لمتابعة أمن النظام

تناول أحد أسئلة الاستبانة مدى وجود قسم تقني مختص بمتابعة أمن نظام شؤون الطلاب، لما لهذا الجانب من أهمية في إدارة المخاطر والتصدي للتهديدات. تُظهر النتائج، في الشكل (6) والجدول (8) أدناه، وجود توجه إيجابي بين غالبية الموظفين نحو الاعتقاد بوجود هذه الجهة الفنية المتخصصة.



شكل 6. آراء الموظفين حول وجود قسم تقني مختص بمتابعة أمن النظام.

جدول 8. توزيع إجابات المشاركين بشأن وجود قسم تقني مختص بأمن النظام.

الخيار	التكرار	النسبة المئوية
موافق بشدة	10	%37
موافق	11	%40.7
محايد	5	%18.5
غير موافق	1	%3.7
غير موافق بشدة	0	%0

يُشير هذا التوزيع إلى وجود إدراك عام لدى معظم الموظفين بوجود جهة تقنية تتولى مهام حماية النظام، إلا أن نسبة غير قليلة من المشاركين تبنّت موقفًا محايدًا أو عبّرت عن عدم المعرفة، مما يعكس احتمالية وجود ضعف في التواصل المؤسسي أو غياب الوضوح في البنية التنظيمية التقنية داخل الإدارة.

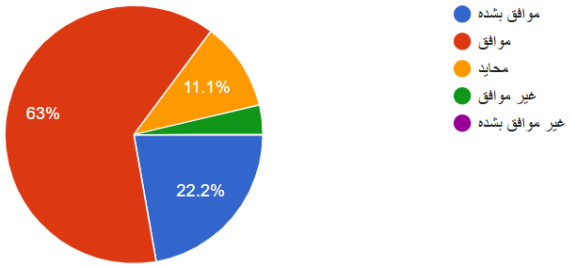
قد يعود ذلك إلى تركّز المهام الأمنية في نطاق ضيق داخل القسم الفني دون إشراك بقية الموظفين أو إعلامهم بوظيفة هذا القسم، مما يُقلل من التكامل في إدارة أمن النظام. إن تعزيز التواصل بين الوحدات الإدارية والفنية، وتوضيح مسؤوليات

الأقسام الأمنية، من شأنه رفع الوعي الجماعي وتحسين الاستجابة المؤسسية للتهديدات.

ثانيًا: السياسات والإجراءات الأمنية:

1. وجود سياسة مكتوبة لحماية بيانات الطلاب

يُعد وجود سياسة مكتوبة لحماية بيانات الطلاب أحد الركائز الأساسية لضمان الحوكمة الرشيدة لأمن المعلومات داخل الجامعة. وقد تضمّن الاستبانة سؤالًا مباشرًا لقياس مدى إدراك الموظفين لوجود هذه السياسات. يوضّح الشكل (7) والجدول (9) الآتيان نتائج إجابات المشاركين.



شكل 7. آراء الموظفين حول وجود سياسة مكتوبة لحماية بيانات الطلاب.

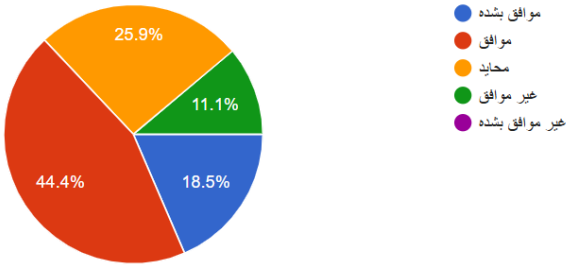
جدول 9. توزيع إجابات المشاركين بشأن وجود سياسة مكتوبة لحماية بيانات الطلاب.

الخيار	التكرار	النسبة المئوية
موافق بشدة	6	%22.2
موافق	17	%63
محايد	3	%11.1
غير موافق	1	%3.7
غير موافق بشدة	0	%0

تُشير البيانات إلى أن الغالبية العظمى من المشاركين (85.2%) يُقرّون بوجود سياسة مكتوبة لحماية بيانات الطلاب، مما يعكس اهتمامًا تنظيميًا بوضع الأطر الرسمية للأمن المعلوماتي. ومع ذلك، فإن وجود نسبة محايدة (11.1%) إلى جانب نسبة – وإن كانت ضئيلة – غير موافقة، قد يدلّ على قصور في تعميم هذه السياسات أو ضعف في مستوى اطلاع بعض الموظفين عليها. هذا التفاوت في الإدراك يُبرز فجوة محتملة بين وجود السياسات من جهة، وتفعيلها أو إيصالها بوضوح للمستفيدين من جهة أخرى، مما يستدعي تعزيز آليات التوعية والتدريب، وربط السياسات بممارسات يومية ملموسة داخل بيئة العمل.

2. إعلام الموظفين بسياسات الخصوصية بشكل دوري

يُعد إعلام الموظفين بسياسات الخصوصية بشكل دوري من العوامل المهمة لضمان الالتزام بالإجراءات الأمنية وتعزيز ثقافة الحماية داخل بيئة العمل. وقد طُرح سؤال في الاستبانة حول مدى التواصل المؤسسي بشأن هذه السياسات. توضح النتائج في الشكل (8) والجدول (10) الآتيين التوزيع التفصيلي لإجابات المشاركين.



شكل 8. آراء الموظفين حول إعلامهم بسياسات الخصوصية بشكل دوري.

جدول 10. توزيع إجابات المشاركين بشأن إعلامهم بسياسات الخصوصية بشكل دوري.

الخيار	التكرار	النسبة المئوية
موافق بشدة	5	%18.5
موافق	12	%44.4
محايد	7	%25.9
غير موافق	3	%11.1
غير موافق بشدة	0	%0

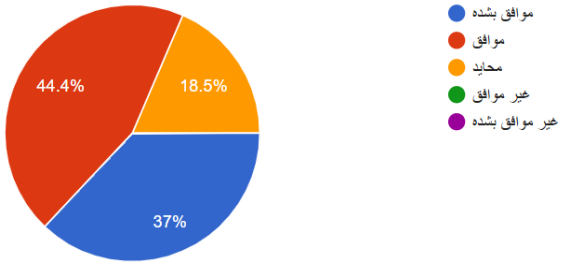
تُظهر النتائج أن ما يقارب ثلثي المشاركين يقرّون بوجود نوع من التواصل بشأن سياسات الخصوصية، مما يعكس حدًا أدنى من الوعي المؤسسي. إلا أن النسبة المرتفعة نسبيًا من المحايدين، بالإضافة إلى نسبة غير الموافقين، تفتح باب التساؤل حول فعالية هذا التواصل ومدى انتظامه.

هذه الأرقام تُشير إلى وجود فجوة بين وجود السياسات كمحتوى نظري وبين تفعيل برامج التوعية والتذكير بها على نحو مستمر. فقد يكون هناك ضعف في إيصال السياسات بشكل مفصّل أو عدم اعتماد خطة توعوية منتظمة تصل إلى جميع الموظفين، وهو ما قد يُؤثّر في مستوى الفهم والالتزام الفعلي بإجراءات الحماية.

3. تحديد صلاحيات الوصول حسب المهام الوظيفية

يُعد التحكم في صلاحيات الوصول أحد المبادئ الأساسية في نظم أمن المعلومات، إذ يضمن أن تكون البيانات متاحة فقط لمن يحتاجون إليها بحسب مهامهم الوظيفية. وقد تضمّنت الاستبانة

سؤالًا يقيس مدى التزام نظام شؤون الطلاب بتطبيق هذا المبدأ. يوضح الشكل (9) والجدول (11) نتائج المشاركين.



شكل 9. آراء الموظفين حول تحديد صلاحيات الوصول حسب المهام الوظيفية.

جدول 11. توزيع إجابات المشاركين بشأن صلاحيات الوصول حسب المهام.

الخيار	التكرار	النسبة المئوية
موافق بشدة	10	%37
موافق	12	%44.4
محايد	5	%18.5
غير موافق	0	%0
غير موافق بشدة	0	%0

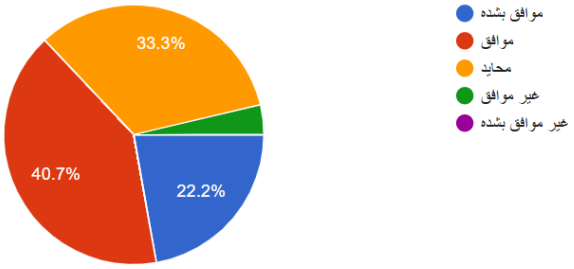
تُشير النتائج إلى وجود توجه عام إيجابي بين المشاركين، إذ أكد أكثر من 80% أن النظام يُراعي تخصيص الصلاحيات وفقًا للمهام الوظيفية. هذا يعكس وجود بنية إدارية وتنظيمية واضحة في ضبط الوصول للبيانات.

ومع ذلك، فإن نسبة المحايدين – التي بلغت قرابة خمس العينة – تلفت الانتباه إلى احتمالين؛ إما أن بعض الموظفين غير مطلعين على تفاصيل الصلاحيات، أو أنهم لا يلمسون تمييزًا فعليًا بين مما يُتاح لهم من وظائف داخل النظام وما يُتاح لغيرهم، ما قد يُشير إلى ضعف في التواصل أو توثيق السياسات الداخلية.

ومن ثم، فإن النتائج تُظهر التزامًا تنظيميًا جيدًا، لكنها في الوقت ذاته تُبرز الحاجة إلى تعزيز الشفافية الداخلية ورفع الوعي بتوزيع الصلاحيات، لا سيما بين المستخدمين ذوي الأدوار غير الفنية أو المحدودة داخل النظام.

4. وجود آلية للإبلاغ عن أي خرق أو تهديد أمني

يُعد وجود آلية واضحة للإبلاغ عن الخروقات أو التهديدات الأمنية أحد معايير النضج المؤسسي في إدارة أمن البيانات. وقد تضمّن الاستبانة سؤالًا حول مدى وضوح هذه الآلية داخل نظام شؤون الطلاب، وتُظهر الشكل (10) والجدول (12) في أدناه توزيع آراء المشاركين.



شكل 10. آراء الموظفين حول وجود آلية للإبلاغ عن أي خرق أو تهديد أمني.

جدول 12. توزيع إجابات المشاركين بشأن وجود آلية للإبلاغ عن التهديدات الأمنية.

الخيار	التكرار	النسبة المئوية
موافق بشدة	6	%22.2
موافق	11	%40.7
محايد	9	%33.3
غير موافق	1	%3.7
غير موافق بشدة	0	%0

تُشير البيانات إلى أن غالبية المشاركين يدركون – بدرجات متفاوتة – وجود قناة أو إجراء مخصص للإبلاغ عن الحوادث الأمنية. إلا أن النسبة اللافتة للمحايدين قد تعكس نقصًا في التواصل الداخلي أو ضعفًا في توثيق وتعميم الإجراءات الأمنية، خاصةً لدى الموظفين الإداريين غير المتخصصين تقنيًا.

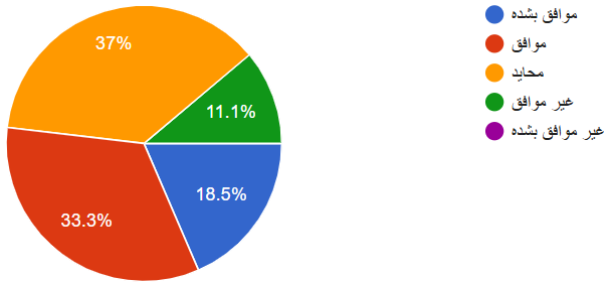
أما نسبة غير الموافقين – رغم ضآلتها – فهي تمثّل فئة قد تكون واجهت تجارب لم تشهد فيها وجود آلية واضحة، أو لم تتلقَّ أي توجيه رسمي في هذا الجانب.

تشير هذه المعطيات إلى أهمية توحيد إجراءات الإبلاغ، وتعميمها بوضوح لكافة العاملين، من خلال التدريب المستمر أو الأدلة التوضيحية، لضمان فعالية الاستجابة للحوادث وتقليل زمن اكتشافها والتعامل معها.

5. وجود لائحة عقوبات لمخالفة سياسات أمن المعلومات

من بين مؤشرات الالتزام المؤسسي بأمن المعلومات وجود لائحة عقوبات واضحة تُنظم كيفية التعامل مع المخالفات المتعلقة

بسياسات أمن البيانات. وقد تضمّن الاستبانة سؤالًا حول إدراك الموظفين لوجود مثل هذه اللائحة. يوضح الشكل (11) والجدول (13) نتائج إجابات المشاركين.



شكل 11. آراء الموظفين حول وجود لائحة عقوبات لمخالفة سياسات أمن المعلومات.

جدول 13. توزيع إجابات المشاركين بشأن وجود لائحة عقوبات لمخالفات أمن المعلومات.

الخيار	التكرار	النسبة المئوية
موافق بشدة	5	%18.5
موافق	9	%33.3
محايد	10	%37
غير موافق	3	%11.1
غير موافق بشدة	0	%0

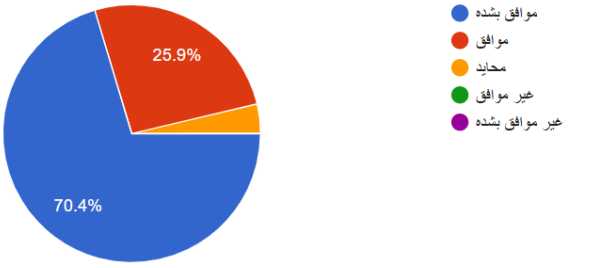
تشير النتائج إلى أن 51.8% فقط من المشاركين أكدوا وجود لائحة عقوبات، بينما عبّر عدد كبير (37%) عن موقف محايد، وهو ما قد يُفسر بضعف الاطلاع أو عدم وضوح الإجراءات التأديبية داخل بيئة العمل. كما أن نسبة الرفض – وإن كانت محدودة – تُعزز الحاجة إلى التحقق من مدى وضوح هذه اللوائح وشموليتها.

تعكس هذه المعطيات فجوة محتملة بين وجود اللائحة كوثيقة تنظيمية، وتفعيلها أو تعميمها بشكل فعّال بين الموظفين. ويُحتمل أن يكون ذلك نتيجة غياب برامج التوعية، أو ضعف الربط بين السياسات المكتوبة والممارسات اليومية عند وقوع حوادث أو مخالفات، مما يُقلل من فاعلية منظومة الردع الإداري في حماية البيانات.

رابعًا: وعي الموظفين بأمن البيانات:

1. فهم أهمية حماية بيانات الطلاب ونتائجهم

يُعد إدراك أهمية حماية بيانات الطلاب ونتائجهم مؤشرًا أساسيًا على وعي الموظفين بمسؤولياتهم تجاه أمن المعلومات. وقد تضمّن الاستبانة سؤالًا مباشرًا لقياس هذا البُعد من الوعي. يوضح الشكل (12) والجدول (14) النتائج التفصيلية لإجابات المشاركين.



شكل 12. مستوى وعي الموظفين بأهمية حماية بيانات الطلاب ونتائجهم.

جدول 14. توزيع إجابات المشاركين حول أهمية حماية بيانات الطلاب.

الخيار	التكرار	النسبة المئوية
موافق بشدة	19	%70.4
موافق	7	%25.9
محايد	1	%3.7
غير موافق	0	%0
غير موافق بشدة	0	%0

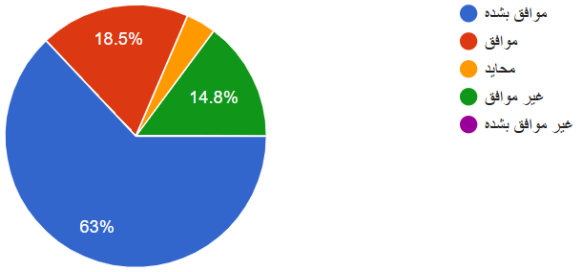
تُظهر البيانات وعيًا مرتفعًا بين المشاركين بأهمية حماية بيانات الطلاب، إذ عبّر ما يقرب من 96% عن موافقتهم أو موافقتهم الشديدة. بينما لم يُسجَّل أي رفض صريح لهذا المفهوم، واقتصر التردد على نسبة ضئيلة عبّرت عن موقف محايد.

تعكس هذه النتائج وجود أساس ثقافي جيد لدى الموظفين تجاه حماية البيانات، ما يُشير إلى فَهْم عام للأثر الحساس الذي تمثله السجلات الأكاديمية. وقد يكون هذا الوعي ناتجًا عن الخبرة العملية المباشرة في التعامل مع النظام، خاصة أن معظم أفراد العينة يعملون في إدخال أو مراجعة البيانات الطلابية.

مع ذلك، لا يُمكن اعتبار هذا الوعي كافيًا بمفرده ما لم يُترجم إلى ممارسات يومية مدعومة بسياسات وتدريب مستمر، وهو ما سيتم ربطه في تحليل الأسئلة الآتية.

2. معرفة أن مشاركة كلمة المرور تُعد مخالفة أمنية

تُعد مشاركة كلمات المرور من أكثر الممارسات التي تُهدد أمن النظام، لذا تضمّنت الاستبانة سؤالًا حول مدى إدراك الموظفين لاعتبار مشاركة كلمة المرور مخالفة أمنية. يوضّح الشكل (13) والجدول (15) النتائج التفصيلية لإجابات المشاركين.



شكل 13. وعي الموظفين بأن مشاركة كلمة المرور تُعد مخالفة أمنية.

جدول 15. توزيع إجابات المشاركين بشأن اعتبار مشاركة كلمة المرور مخالفة أمنية.

الخيار	التكرار	النسبة المئوية
موافق بشدة	17	%63
موافق	5	%18.5
محايد	1	%3.7
غير موافق	4	%14.8
غير موافق بشدة	0	%0

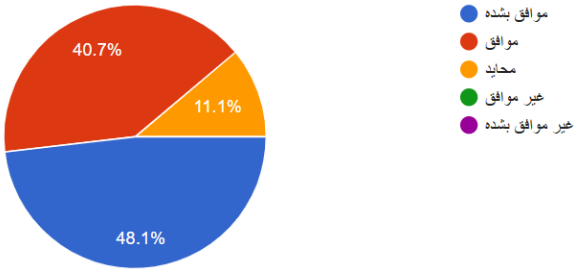
تُشير النتائج إلى أن الغالبية العظمى من المشاركين (81.5%) يدركون أن مشاركة كلمة المرور تُعد خرقًا لمبادئ أمن المعلومات، وهو مؤشر إيجابي على وجود مستوى جيد من الوعي.

إلا أن نسبة غير قليلة (14.8%) لم تتفق مع هذا المفهوم، ما يبرز فجوة معرفية تستدعي الانتباه، خاصة في ظل طبيعة النظام الذي يتعامل مع بيانات طلابية حساسة. كما أن وجود نسبة محايدة – وإن كانت ضئيلة – قد يعكس ضعفًا في تعميم السياسات أو قلة التركيز على هذا الجانب في ضمن البرامج التدريبية.

تؤكد هذه النتيجة على أهمية تعزيز التوعية المستهدفة حول ممارسات الحماية الأساسية، ومنها عدم مشاركة الحسابات، والتأكيد على أن كل موظف مسؤول عن بيانات النظام التي يدخل إليها أو يعدلها عبر حسابه الخاص.

3. معرفة كيفية التعامل مع بيانات الطالب الحساسة

إن التعامل مع البيانات الحساسة، مثل السجلات الأكاديمية ومعلومات الهوية، يتطلب مستوى عاليًا من الوعي بالإجراءات الوقائية والضوابط المؤسسية. وقد تضمّن الاستبانة سؤالًا لقياس مدى إدراك الموظفين لكيفية التعامل مع هذه البيانات في ضمن مهامهم. تُعرض نتائج الإجابات في الشكل (14) والجدول (16) في أدناه.



شكل 14. آراء الموظفين حول معرفتهم بكيفية التعامل مع بيانات الطالب الحساسة.

جدول 16. توزيع إجابات المشاركين حول معرفة التعامل مع البيانات الحساسة.

الخيار	التكرار	النسبة المئوية
موافق بشدة	13	%48.1
موافق	11	%40.7
محايد	3	%11.1
غير موافق	0	%0
غير موافق بشدة	0	%0

تُشير البيانات إلى أن 88.8% من المشاركين عبّروا عن موافقتهم – بدرجات متفاوتة – على امتلاكهم المعرفة اللازمة للتعامل الآمن مع بيانات الطلاب الحساسة، في حين لم تسجل أي نسبة رفض، واقتصر التردد على فئة المحايدين فقط.

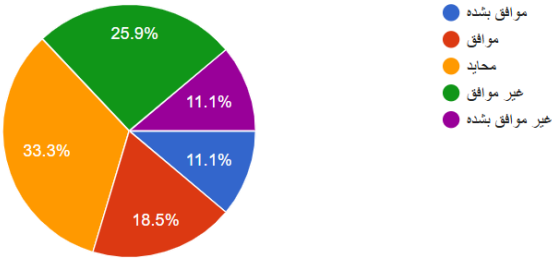
يُمكن تفسير هذه الثقة العالية بارتباطها بطبيعة المهام اليومية التي يقوم بها المشاركون، والتي تتضمن إدخال أو تعديل البيانات الأكاديمية. كما أن تراكم الخبرة العملية قد يُسهم في بناء هذه الثقة، حتى في غياب تدريب رسمي مستمر.

ومع ذلك، فإن غياب التقييم المؤسسي أو الاعتماد على المعايير المكتوبة يُبرز الحاجة إلى تدعيم هذا الوعي الذاتي بإطار مؤسسي واضح يشمل سياسات موثقة، ودورات تدريبية دورية، ونماذج تقييم للممارسات الأمنية، وذلك لضمان أن الثقة تنبع من ممارسة سليمة ومتوافقة مع معايير حماية البيانات.

4. المشاركة السابقة في تدريب عن أمن المعلومات

تُعد المشاركة في تدريبات متخصصة بأمن المعلومات إحدى الركائز الأساسية لضمان قدرة الموظفين على التعامل السليم مع البيانات الحساسة. وقد تناولت الاستبانة سؤالًا لقياس مدى

مشاركة الموظفين سابقًا في مثل هذه البرامج التدريبية. يوضح الشكل (15) والجدول (17) نتائج الإجابات.



شكل 15. مدى مشاركة الموظفين في تدريب سابق عن أمن المعلومات.

جدول 17. توزيع إجابات المشاركين حول المشاركة في تدريب عن أمن المعلومات.

الخيار	التكرار	النسبة المئوية
موافق بشدة	3	%11.1
موافق	5	%18.5
محايد	9	%33.3
غير موافق	7	%25.9
غير موافق بشدة	3	%11.1

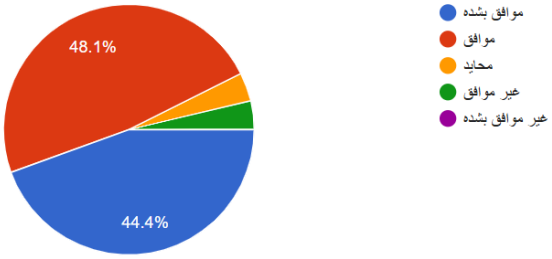
تُشير النتائج إلى أن أقل من 30% فقط من المشاركين أكدوا تلقيهم تدريبًا رسميًا في أمن المعلومات، في حين أن أكثر من 70% إما لم يتلقوا تدريبًا، أو لم تكن لديهم قناعة أو علم كافٍ بالمشاركة فيه. وتشير النسبة المرتفعة من المحايدين (33.3%) إلى غياب توثيق أو تذكير واضح ببرامج التدريب السابقة، أو ضعف في نظام متابعة حضور الموظفين لهذه البرامج.

تعكس هذه البيانات وجود فجوة فعلية في التغطية التدريبية، قد تُعزى إلى غياب خطة تدريبية دورية، أو اقتصار التدريب على فئات معينة دون غيرها. ويؤكد ذلك أيضًا ملاحظات سابقة أظهرت تفاوتًا في الفهم والممارسات الأمنية رغم ارتفاع الإدراك بأهمية حماية البيانات.

ومن هنا، تُبرز هذه النتائج أهمية الانتقال من برامج تدريبية عامة أو متقطعة إلى خطة استراتيجية للتدريب تشمل كافة الموظفين، مع تحديث المحتوى وتقييم الأثر لضمان تحويل المعرفة النظرية إلى سلوك مهني فعّال.

5. الثقة في القدرة الذاتية على حماية البيانات

تُعد الثقة في القدرة على حماية البيانات أحد المؤشرات الذاتية المهمة التي تعكس استعداد الموظف للتصرف الآمن عند التعامل مع نظم المعلومات. وقد تضمّنت الاستبانة سؤالًا يقيس هذا الجانب من الوعي الذاتي. تُعرض النتائج في الشكل (16) والجدول (18) في أدناه:



شكل 16. ثقة الموظفين في قدرتهم على حماية بيانات الطلاب.

جدول 18. توزيع إجابات المشاركين حول ثقتهم في قدرتهم على حماية البيانات.

الخيار	التكرار	النسبة المئوية
موافق بشدة	12	%44.4
موافق	13	%48.1
محايد	1	%3.7
غير موافق	1	%3.7
غير موافق بشدة	0	%0

تُشير البيانات إلى أن ما يقرب من 92.5% من المشاركين يشعرون بالثقة في قدرتهم على حماية بيانات الطلاب في أثناء استخدامهم للنظام، وهو مؤشر إيجابي يُعبر عن وعي أمني ذاتي منتشر بين الموظفين، وربما يرتبط بتجاربهم العملية المباشرة أو فهمهم للمهام الأمنية الأساسية.

إلا أن هذه النتيجة – رغم إيجابيتها – لا تعني بالضرورة أن جميع الممارسات آمنة أو صحيحة، خاصة في ظل غياب برامج تدريبية ممنهجة كما أظهرت الأسئلة السابقة. كما أن نسبة 7.4% من المحايدين وغير الموافقين تُشير إلى وجود شريحة تحتاج إلى دعم أكبر، سواء بالتوجيه أو التقييم العملي لمهاراتهم الأمنية.

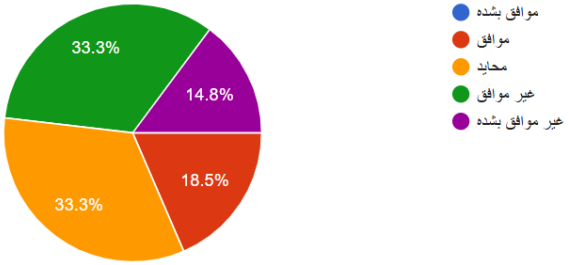
ويُعد الجمع بين الثقة الذاتية والتدريب المؤسسي المستمر هو السبيل لضمان تحويل الثقة إلى ممارسة فعلية تحمي النظام من المخاطر غير المرئية، وتُقلل من احتمالية الوقوع في الأخطاء الناتجة عن الإفراط في تقدير القدرات الشخصية.

خامسًا: التهديدات والمخاطر الفعلية:

1. تعرض النظام لمحاولات اختراق أو أعطال

يُعد قياس إدراك الموظفين للتهديدات الأمنية الفعلية التي تعرض لها النظام مؤشرًا مهمًا على مدى شفافية الإدارة، ومشاركة المعرفة الأمنية داخل المؤسسة. وقد تناولت الاستبانة سؤالًا

مباشرًا حول ما إذا كان نظام شؤون الطلاب قد تعرض لمحاولات اختراق أو أعطال في السابق. تُعرض نتائج الإجابات في الشكل (17) والجدول (19) في أدناه:



شكل 17. آراء الموظفين حول تعرض نظام شؤون الطلاب لمحاولات اختراق أو أعطال.

جدول 19. توزيع إجابات المشاركين حول وجود اختراقات أو أعطال في النظام.

الخيار	التكرار	النسبة المئوية
موافق بشدة	0	%0
موافق	5	%18.5
محايد	9	%33.3
غير موافق	9	%33.3
غير موافق بشدة	4	%14.8

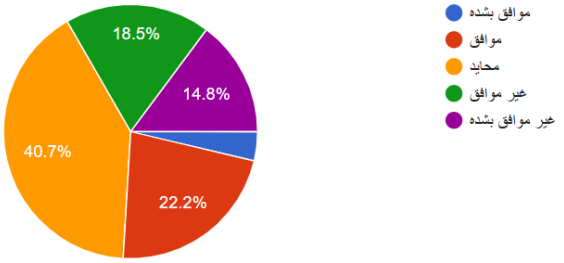
تُظهر النتائج تباينًا واضحًا في آراء الموظفين بشأن ما إذا كان النظام قد تعرّض بالفعل لأي نوع من التهديدات أو الأعطال. حيث لم تتجاوز نسبة الموافقين 18.5%، مقابل 48.1% ممن أنكروا ذلك بدرجات متفاوتة، بينما بقي ثلث العينة تقريبًا (33.3%) في موقع الحياد.

هذا التفاوت في الإجابات يُفسَّر غالبًا بغياب آلية معلنة لمشاركة معلومات الحوادث الأمنية داخل بيئة العمل، أو ربما بغياب حوادث ملحوظة أصلًا. ومع ذلك، فإن ارتفاع نسبة المحايدين يُعد مؤشرًا على ضعف في التواصل الداخلي أو غياب التوعية بشأن سجل الحوادث، وهو ما يُقلل من قدرة الموظفين على تقييم الواقع الأمني للنظام بدقة.

وتُبرز هذه المعطيات أهمية تبني سياسات شفافية أمنية مدروسة، تُشرك الموظفين في فهم طبيعة التهديدات، وآليات التعامل معها، وذلك في ضمن برامج التوعية المستمرة وبما لا يُخل بسرية المعالجات الفنية.

2. وجود ثغرات أمنية معروفة في النظام

يُعد إدراك الموظفين لوجود ثغرات أمنية داخل النظام مكوّنًا أساسيًا لفهم مدى وعي المؤسسة بحالة أمنها المعلوماتي، واستعدادها للتحسين المستمر. وقد تضمّنت الاستبانة سؤالًا لقياس مدى إدراك المشاركين لوجود ثغرات أمنية معروفة في نظام شؤون الطلاب. وتُعرض النتائج في الشكل (18) والجدول (20) في أدناه:



شكل 18. تقييم الموظفين لوجود ثغرات أمنية معروفة في النظام.

جدول 20. توزيع آراء المشاركين حول وجود ثغرات أمنية في النظام.

الخيار	التكرار	النسبة المئوية
موافق بشدة	1	%3.7
موافق	6	%22.2
محايد	11	%40.7
غير موافق	5	%18.5
غير موافق بشدة	4	%14.8

تُظهر النتائج تباينًا كبيرًا في إدراك الموظفين لمسألة وجود ثغرات أمنية في النظام، إذ عبّر 25.9% فقط عن قناعتهم بوجود مثل هذه الثغرات، في حين رفض الفكرة 33.3% بدرجات متفاوتة، بينما بقيت النسبة الأكبر (40.7%) في موقع الحياد.

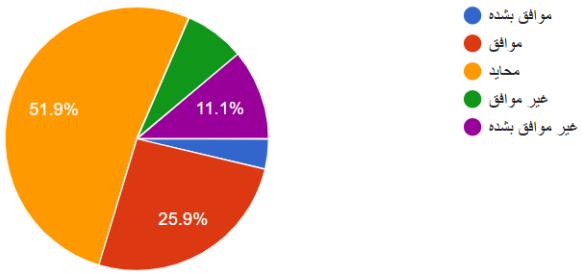
هذا التباين اللافت يُشير إلى أن الوعي التقني لدى معظم الموظفين غير حاسم، وربما يعود ذلك إلى عدة عوامل، أبرزها: ضعف التواصل بين الفريق الفني والمستخدمين، أو غياب تقارير دورية حول الحالة الأمنية للنظام، أو عدم إدماج الموظفين في عمليات التقييم والتحسين الأمني.

ويُلمّح ارتفاع نسبة "المحايدين" إلى أن الكثير من الموظفين غير ملمين بالمخاطر الأمنية أو بأدوات الكشف عنها، الأمر الذي يُبرز فجوة معرفية بين الفريق التقني وبقية الطاقم الإداري. كما أن غياب الشفافية في هذا الجانب قد يُقلل من القدرة المؤسسية على الاستجابة السريعة والفعالة للتهديدات المستقبلية.

3. القلق من تسرب بيانات الطلاب

يُعد قياس القلق من تسرب البيانات مؤشرًا مهمًا على مستوى إدراك الموظفين لمخاطر أمن المعلومات، وهو ما ينعكس على

سلوكهم الوقائي اليومي داخل النظام. وقد تضمّن الاستبانة سؤالًا حول ما إذا كان هناك تخوف فعلي لدى الموظفين من احتمال تسرب بيانات الطلاب. وتُعرض النتائج في الشكل (19) والجدول (21) في أدناه:



شكل 19. آراء الموظفين حول القلق من تسرب بيانات الطلاب.

جدول 21. توزيع الإجابات حول وجود تخوف من تسرب البيانات.

الخيار	التكرار	النسبة المئوية
موافق بشدة	1	%3.7
موافق	7	%25.9
محايد	14	%51.9
غير موافق	2	%7.4
غير موافق بشدة	3	%11.1

تُظهر النتائج أن أكثر من نصف المشاركين (51.9%) اتخذوا موقفًا "محايدًا" تجاه وجود تخوف من تسرب بيانات الطلاب، في مقابل 29.6% فقط من الموظفين الذين عبّروا عن القلق بدرجات متفاوتة، مقابل 18.5% ممن لم يبدوا قلقًا على الإطلاق.

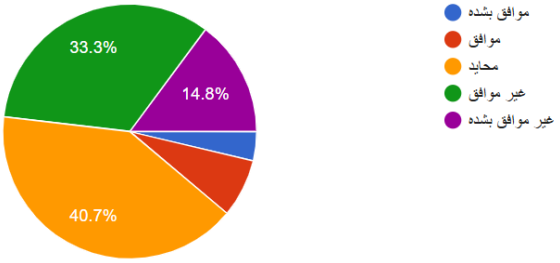
يُشير هذا التوزيع إلى ضعف في الوعي أو عدم وضوح التهديدات الفعلية المتعلقة بتسرب البيانات، إما بسبب غياب التثقيف الأمني المستمر، أو نتيجة نقص الشفافية من الإدارة التقنية بشأن مخاطر أو حوادث سابقة. كما قد يُعبر عن شعور زائف بالأمان مبني على الاعتياد أو الثقة غير المدعومة بتقييمات أمنية حقيقية.

وتُظهر هذه النتائج وجود فجوة في تصور المخاطر الأمنية لدى شريحة واسعة من الموظفين، وهو ما قد يؤثر سلبًا في تبني سلوكيات وقائية أو الإبلاغ المبكر عن الملاحظات التقنية، ومن ثم يُضعف من قدرة النظام على حماية بياناته الحساسة.

ويُعد رفع مستوى القلق المدروس – القائم على المعرفة – أمرًا ضروريًا، لأنه يُمثل محفزًا مهمًا لتعزيز التدابير الوقائية، والالتزام بالإجراءات الأمنية اليومية.

4. الصعوبات في التعامل الآمن مع البيانات

يمثل تقييم الصعوبات التي يواجهها الموظفون في التعامل الآمن مع البيانات جانبًا مهمًا لفهم التحديات اليومية في تطبيق مبادئ أمن المعلومات، خاصة في بيئة إدارية تعتمد على الأنظمة الرقمية. وقد تناولت الاستبانة سؤالًا مباشرًا حول ما إذا كان المشاركون يواجهون صعوبات في التعامل الآمن مع بيانات الطلاب. تُعرض نتائج هذا البند في الشكل (20) والجدول (22) في أدناه:



شكل 20. آراء الموظفين حول صعوبات التعامل الآمن مع بيانات الطلاب.

جدول 22. توزيع إجابات المشاركين بشأن صعوبة التعامل الآمن مع البيانات.

الخيار	التكرار	النسبة المئوية
موافق بشدة	1	%3.7
موافق	2	%7.4
محايد	11	%40.7
غير موافق	9	%33.3
غير موافق بشدة	4	%14.8

تُشير النتائج إلى أن معظم المشاركين لا يواجهون صعوبات واضحة، حيث أفاد 48.1% بعدم موافقتهم على وجود صعوبات، مقابل 11.1% فقط ممن أقرّوا بوجودها. بينما حافظت نسبة كبيرة من العينة (40.7%) على موقف "محايد"، مما يعكس غياب تصور دقيق أو موثّق لمفهوم التعامل الآمن، أو عدم إدراك كامل للتحديات التقنية التي قد تتخلل العملية.

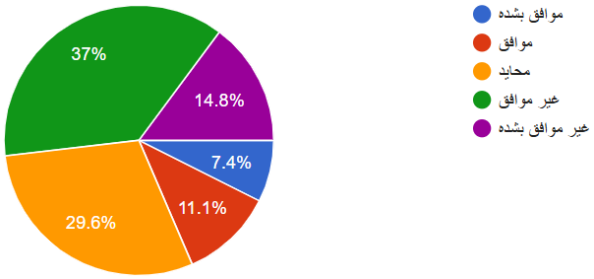
يمكن تفسير هذه النتيجة بأن بعض الموظفين يُمارسون مهامهم في ضمن إجراءات مؤسسية جاهزة دون تعمّق في الجوانب الفنية، أو ربما لا يملكون أدوات تقييم ذاتية حقيقية لقياس درجة "الأمان" في ممارساتهم اليومية.

يشير ذلك إلى الحاجة الماسّة إلى تقديم تدريبات تطبيقية شاملة تتضمن حالات واقعية وتقييمات دورية، تساعد الموظفين في

التمييز بين الاستخدام الاعتيادي للنظام وبين الممارسات التي قد تُعرض البيانات للخطر. كما أن رفع مستوى الوضوح حول ما يُعد "تعاملًا آمنًا" أو "مخاطرة" يُمكن أن يُقلل من نسبة التردد (المحايدين) ويزيد من جودة الاستجابة المؤسسية للمخاطر.

5. تجاوز الصلاحيات من قبل بعض المستخدمين

يُعد تجاوز الصلاحيات الممنوحة في النظم المعلوماتية أحد أبرز مؤشرات الخلل في نظام التحكم بالوصول (Access Control)، وقد يرتبط ذلك إما بضعف الضبط التقني، أو بتراخي في الالتزام بالسياسات، أو بوجود ثقافة مؤسسية غير صارمة في هذا الجانب. وقد تضمّنت الاستبانة سؤالًا حول ما إذا كان الموظفون يعتقدون أن بعض المستخدمين يتجاوزون الصلاحيات المحددة لهم في النظام. وتُعرض النتائج في الشكل (21) والجدول (23) أدناه:



شكل 21. تقييم الموظفين لمدى وجود تجاوز للصلاحيات في النظام.

جدول 23. توزيع آراء المشاركين حول تجاوز بعض المستخدمين لصلاحياتهم.

الخيار	التكرار	النسبة المئوية
موافق بشدة	2	%7.4
موافق	3	%11.1
محايد	8	%29.6
غير موافق	10	%37
غير موافق بشدة	4	%14.8

تُظهر النتائج أن نسبة من المشاركين (18.5%) عبّروا عن اعتقادهم بوجود حالات تجاوز لصلاحيات المستخدمين، وهي نسبة لا يمكن إغفالها، إذ قد تُشير إلى ممارسات غير منضبطة أو قصور في إدارة صلاحيات الوصول.

في المقابل، نفى 51.8% من المشاركين وجود مثل هذه التجاوزات، مما يُظهر أن غالبية الموظفين لا تلاحظ أو لا تعتقد بوجود اختراقات في هذا الجانب، وربما يعود ذلك إلى ثقتهم في النظام أو إلى عدم اطلاعهم على أنشطة الآخرين داخل النظام.

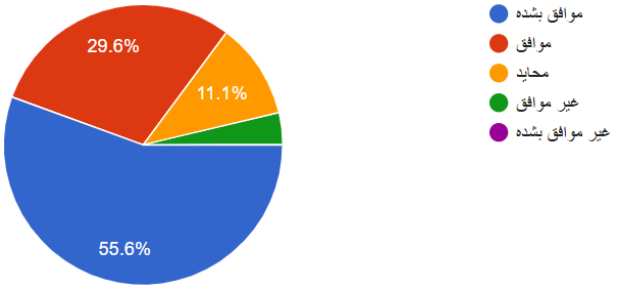
من اللافت كذلك أن 29.6% من المشاركين اختاروا الموقف "المحايد"، وهي نسبة كبيرة تعكس إما عدم وجود معلومات كافية لديهم عن هذا الجانب، أو عدم رغبتهم في التصريح بموقف واضح، وربما يُفسَّر ذلك بتقاطع العلاقات الإدارية أو غياب الرصد الفعلي داخل المؤسسة.

تُسلّط هذه النتيجة الضوء على أهمية تفعيل أنظمة مراقبة الاستخدام (User Activity Monitoring)، وضمان وجود سجلات واضحة للعمليات داخل النظام، مع مراجعة دورية للصلاحيات الممنوحة، بما يضمن الالتزام التام بالمهام الوظيفية المخصصة لكل مستخدم.

سادسًا: مقترحات التحسين

1. تطبيق تقنيات التشفير لحماية البيانات

يعد التشفير من أكثر الوسائل التقنية فاعلية في حماية البيانات الحساسة من الوصول غير المصرح به. وقد تضمّن الاستبانة سؤالًا مباشرًا حول ما إذا كان المشاركون يؤيدون تطبيق تقنيات التشفير في نظام شؤون الطلاب لضمان حماية البيانات. وتُعرض النتائج في الشكل (22) والجدول (24) في أدناه:



شكل 22. آراء الموظفين حول ضرورة تطبيق تقنيات التشفير لحماية البيانات.

جدول 24. توزيع إجابات المشاركين حول تطبيق التشفير لحماية البيانات.

الخيار	التكرار	النسبة المئوية
موافق بشدة	15	%55.6
موافق	8	%29.6
محايد	3	%11.1
غير موافق	1	%3.7
غير موافق بشدة	0	%0

تُظهر النتائج توافقًا واسعًا بين الموظفين على أهمية تطبيق التشفير كوسيلة ضرورية لحماية البيانات الطلابية، إذ عبّر

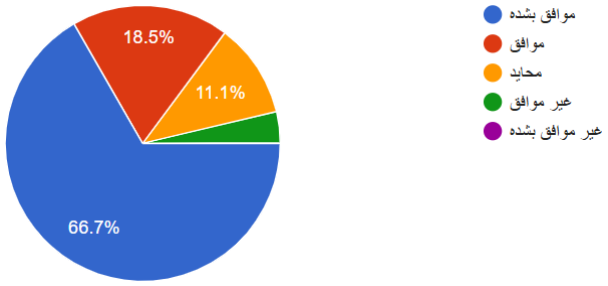
85.2% من المشاركين عن تأييدهم (موافق وموافق بشدة)، مما يعكس وعيًا تقنيًا إيجابيًا بأهمية التشفير في حماية سرية المعلومات.

في المقابل، عبّر 11.1% عن موقف "محايد"، مما قد يُشير إلى عدم إلمامهم الكامل بفوائد التشفير أو عدم تعاملهم المباشر مع هذه الخاصية في ضمن النظام. أما نسبة الرفض فقد كانت شبه معدومة، مما يعزز من مشروعية التوصية بتطبيق بروتوكولات تشفير قوية على مستوى قاعدة البيانات، والملفات، والاتصالات الداخلية للنظام.

هذه النتيجة تمثل أرضية مؤسسية جيدة لتبني تقنيات التشفير، لا سيما في ظل تصاعد المخاطر السيبرانية وحساسية البيانات الأكاديمية، وتُعد داعمة لأي خطوات مستقبلية في هذا الاتجاه.

2. الحاجة إلى تدريب دوري على أمن المعلومات

أظهرت إجابات المشاركين اتجاهًا واضحًا نحو الإقرار بأهمية التدريب المستمر في مجال أمن المعلومات، وفق النتائج في الشكل (23) والجدول (25) أدناه:



شكل 23. آراء الموظفين حول الحاجة إلى تدريب دوري على أمن المعلومات.

جدول 25. توزيع إجابات المشاركين حول الحاجة إلى تدريب دوري على أمن المعلومات.

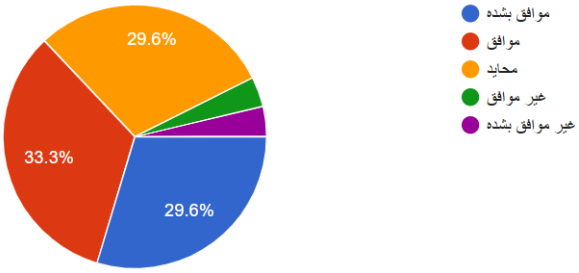
الخيار	التكرار	النسبة المئوية
موافق بشدة	18	%66.7
موافق	5	%18.5
محايد	3	%11.1
غير موافق	1	%3.7
غير موافق بشدة	0	%0

حيث عبّر حوالي 85.2% على حاجتهم إلى برامج تدريب دورية لتعزيز ممارسات الأمان في النظام.

تعكس هذه النتائج أن هناك وعيًا متناميًا بين الموظفين بضرورة مواكبة التحديثات في مجال أمن المعلومات من خلال التدريب المنتظم، خاصة في ظل التطورات التقنية المتسارعة وزيادة الاعتماد على الأنظمة الإلكترونية لإدارة بيانات الطلاب. كما أنها تُبرز إدراكًا بأن التدريب لا يجب أن يكون حدثًا منفردًا، بل ممارسة مؤسسية مستمرة تعزز من السلوك الأمني العام في بيئة العمل.

3. أفضلية التخزين المحلي مقارنة بالسحابة

أظهرت نتائج المشاركين توجهًا إيجابيًا نسبيًا نحو تفضيل تخزين البيانات محليًا بدلًا من الاعتماد الكامل على الحوسبة السحابية كما توضح النتائج في الشكل (24) والجدول (26).



شكل 24. آراء الموظفين حول أفضلية التخزين المحلي مقارنة بالسحابة.

جدول 26. توزيع إجابات المشاركين حول أفضلية التخزين المحلي مقارنة بالسحابة.

الخيار	التكرار	النسبة المئوية
موافق بشدة	8	%29.6
موافق	9	%33.3
محايد	8	%29.6
غير موافق	1	%3.7
غير موافق بشدة	1	%3.7

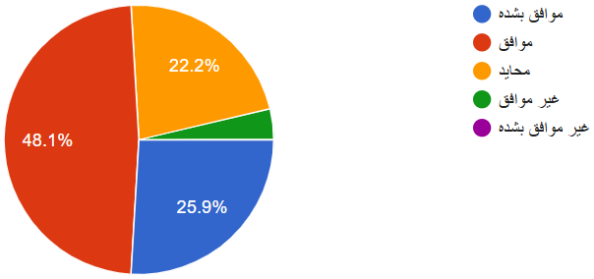
حيث مال حوالي 62.9% من العينة إلى اعتبار التخزين المحلي أكثر أمانًا أو ملاءمة.

في المقابل، اتخذ 29.6% موقفًا "محايدًا"، مما يشير إلى تردد أو عدم حسم الرأي لدى جزء من المشاركين، وقد يُعزى ذلك إلى قلة المعرفة التقنية حول الفرق بين التخزين المحلي والسحابي من حيث الأمان، أو إلى غياب تجربة مباشرة في التعامل مع أنظمة تخزين متنوعة.

تعكس هذه النتائج وجود رغبة واضحة لدى الموظفين في الحفاظ على السيطرة الداخلية على البيانات الأكاديمية، ربما بسبب القلق من سياسات الخصوصية في الخدمات السحابية، أو بسبب محدودية البنية التقنية المخصصة للتعامل الآمن مع السحابة داخل الجامعة.

4. إمكانية استخدام التحقق متعدد العوامل لتأمين الدخول

عبّر أغلب المشاركين عن تأييدهم لاستخدام تقنيات التحقق متعدد العوامل (Multi-Factor Authentication – MFA) لتعزيز أمان الدخول إلى نظام شؤون الطلاب، حيث رأى حوالي 74% من العينة أن إضافة طبقة أمنية إضافية خطوة ضرورية لتعزيز الحماية كما توضح النتائج في الشكل (25) والجدول (27).



شكل 25. آراء الموظفين حول إمكانية استخدام التحقق متعدد العوامل لتأمين الدخول.

جدول 27. توزيع إجابات المشاركين حول إمكانية استخدام التحقق متعدد العوامل لتأمين الدخول.

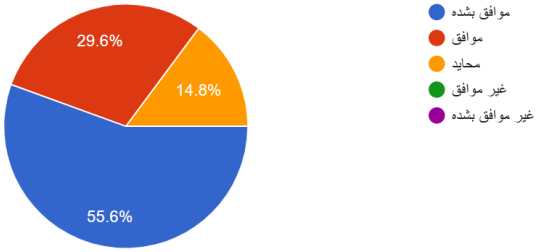
الخيار	التكرار	النسبة المئوية
موافق بشدة	7	%25.9
موافق	13	%48.1
محايد	6	%22.2
غير موافق	1	%3.7
غير موافق بشدة	0	%0

تشير هذه النتائج إلى وجود وعي واضح بين الموظفين بأهمية استخدام أساليب تحقق أكثر تطورًا من كلمات المرور التقليدية، مثل إرسال رموز تحقق عبر الهاتف أو البريد الإلكتروني، أو استخدام التطبيقات الأمنية، وذلك لمواجهة المخاطر المتزايدة التي تهدد البيانات الأكاديمية الحساسة. كما أن النسبة الكبيرة من الموافقين تدعم توجهًا مؤسسيًا نحو تطبيق هذا النوع من الحماية دون مقاومة كبيرة من المستخدمين.

5. تأييد تعيين مسؤول رسمي لحماية البيانات

أظهر المشاركون دعمًا كبيرًا لفكرة تعيين مسؤول رسمي لحماية البيانات داخل الجامعة، حيث عبّر 85.2% من العينة على أهمية تخصيص جهة مسؤولة تتولى الإشراف على أمن بيانات الطلاب وسجلاتهم الأكاديمية كما توضح النتائج في الشكل (26) والجدول (28).

في المقابل، اتخذ 14.8% موقفًا محايدًا، دون تسجيل أي نسبة رفض صريحة، مما يعزز من الاتجاه العام الإيجابي نحو هذه الخطوة المؤسسية.



شكل 26. آراء الموظفين حول تأييد تعيين مسؤول رسمي لحماية البيانات.

جدول 28. توزيع إجابات المشاركين بشأن تعيين مسؤول رسمي لحماية البيانات.

الخيار	التكرار	النسبة المئوية
موافق بشدة	15	%55.6
موافق	8	%29.6
محايد	4	%14.8
غير موافق	0	%0
غير موافق بشدة	0	%0

تشير هذه النتائج إلى وجود قناعة واسعة بين الموظفين بأن وجود مسؤول مختص بأمن البيانات أمر ضروري لتنظيم السياسات، ومتابعة الالتزام بها، والاستجابة للحوادث الأمنية بشكل احترافي. ويُعزز هذا التوجه الحاجة إلى بناء بنية إدارية واضحة لحوكمة أمن المعلومات، بما يتجاوز الجهود الفردية أو التقنية المؤقتة.

سابعًا: اقتراحات وملاحظات لتحسين أمان بيانات الطلاب (سؤال مفتوح)

في نهاية الاستبانة، طُلب من المشاركين تقديم اقتراحات حرة لتحسين أمان البيانات في نظام شؤون الطلاب، وقد ركزت أبرز الملاحظات على الجوانب التقنية والبنية التحتية، وهو ما يعكس وعيًا عمليًا لدى بعض الموظفين بطبيعة التحديات الأمنية في النظام.

تضمنت أبرز الاقتراحات ما يلي:

- التحول إلى سيرفرات عالية الكفاية والسرعة لضمان استقرار النظام وسرعة الاستجابة، مما يعكس إدراكًا لأثر الأداء التقني في تقليل الثغرات.
- مراقبة نشاط النظام باستخدام برامج متخصصة في رصد التهديدات، وهو ما يُشير إلى الحاجة لاستخدام أدوات تحليل سلوكي أو نظم كشف التسلل (IDS).

- فصل بيانات الطلاب عن البيانات الإدارية الأخرى كوسيلة لعزل المخاطر وتقليل نقاط الضعف.

تشير هذه الملاحظات إلى وعي متنامٍ لدى بعض الموظفين بجوانب تقنية حساسة قد لا تكون في ضمن مسؤولياتهم المباشرة، لكنها تؤثر في كفاية وأمن النظام ككل، مما يعزز أهمية إشراك المستخدمين النهائيين في تطوير السياسات والحلول.

5. التوصيات

جاءت التوصيات الآتية استنادًا إلى النتائج التي تم التوصل إليها من خلال تحليل بيانات الاستبانة موزعة على موظفي نيابة شؤون الطلاب بجامعة حضرموت، بالإضافة إلى ما تم جمعه من ملاحظات ومعلومات نوعية خلال المقابلات المباشرة مع عدد من الموظفين ومسؤولي النظام. وقد عكست هذه المدخلات معًا صورة شاملة للوضع الأمني للنظام، بما أتاح بناء توصيات عملية تعالج التحديات الواقعية وتدعم سُبل التحسين.

1- **تعيين مسؤول رسمي لحماية البيانات(Data Protection Officer):** ضرورة استحداث وظيفة رسمية تتولى مسؤولية وضع السياسات الأمنية، ومراقبة الامتثال، والاستجابة للحوادث، بما يعزز الحوكمة المؤسسية لأمن المعلومات.

2- **تفعيل أنظمة التحقق متعددة العوامل (Multi-Factor Authentication):** نظرًا لتأييد الموظفين الواسع لهذا الإجراء، يوصى بتطبيقه لتعزيز طبقات الأمان عند الدخول إلى النظام، خاصة للوظائف ذات الوصول الحساس.

3- **التحول إلى تقنيات التشفير لحماية البيانات:** يوصى بتشفير بيانات الطلاب في أثناء التخزين والنقل باستخدام خوارزميات حديثة، كجزء من استراتيجية أمنية شاملة.

4- **إنشاء وتحديث سياسات الخصوصية والأمن بشكل دوري:** يجب صياغة سياسات مكتوبة وواضحة تُحدّث بانتظام، وإعلام جميع الموظفين بها بشكل دوري، مع تضمينها آليات الإبلاغ والعقوبات.

5- **توفير برامج تدريب دورية إلزامية لأمن المعلومات:** نتيجة لضعف المشاركة في التدريب الأمني، يُوصى بإطلاق دورات تدريبية منتظمة تغطي مفاهيم أمن البيانات، وسلوكيات الاستخدام الآمن للنظام.

6- **تحسين آليات النسخ الاحتياطي والتحديث الفني:** تعزيز أنظمة النسخ الاحتياطي المنتظم، وتوثيق جداول التحديث البرمجي لتقليل المخاطر التقنية الناتجة عن الثغرات أو الأعطال.

7- **ضبط صلاحيات الوصول بشكل أكثر دقة وتوثيقها:** ينبغي مراجعة آلية التحكم في الصلاحيات بشكل دوري، مع إنشاء سجلات تدقيق (logs) لمراقبة الوصول والتعديلات التي تتم على النظام.

8- **تعزيز مراقبة النظام والتعامل مع التهديدات:** ضرورة اعتماد أنظمة ذكية لرصد التهديدات والتصرف حيالها مثل(IDS) ، بما يدعم التفاعل السريع مع أي محاولة اختراق أو تجاوز للصلاحيات.

9- **فصل البيانات الحساسة عن المكونات الإدارية الأخرى:** لتقليل خطر التسرب، يُفضل فصل قواعد بيانات الطلاب عن قواعد البيانات الإدارية الأخرى، بما يتيح عزلاً وظيفيًا يسهم في الحد من المخاطر.

10- دراسة إمكانية توظيف تقنية البلوك تشين لتأمين بيانات نتائج الطلاب وسجلاتهم الأكاديمية، لما لها من قدرة على ضمان عدم التلاعب بالبيانات، وتمكين الجامعات من إثبات صحة الوثائق إلكترونيًا، خصوصًا في العمليات الحساسة مثل التخرج والتحويلات الأكاديمية.

الخاتمة

تناولت هذه الدراسة تقييم واقع أمن البيانات ونتائج الطلاب في نظام شؤون الطلاب بجامعة حضرموت، من خلال استبانة موجهة إلى الموظفين المختصين، وتحليل شامل لردودهم. وقد أظهرت النتائج وجود بنية تقنية أساسية جيدة إلى حدٍ ما، مع التزام مقبول بالسياسات الأمنية، ووعي عام بأهمية حماية البيانات.

غير أن الدراسة كشفت أيضًا عن عدد من التحديات، أبرزها: ضعف التدريب، نقص في التواصل المؤسسي حول السياسات، تفاوت في فهم الإجراءات الأمنية، وعدم كفاية بعض وسائل الحماية التقنية.

بناءً على ذلك، أوصت الدراسة بجملة من التوصيات لتحسين أمن النظام، شملت جوانب تنظيمية، وتقنية، وتوعوية. وتُعد هذه التوصيات إطارًا مقترحًا لتعزيز الأمن السيبراني داخل الجامعة، بما يضمن حماية بيانات الطلاب الأكاديمية، ويعزز من كفاية النظام وجودته في خدمة المجتمع الجامعي.

تفتح هذه الدراسة المجال أمام مزيد من الأبحاث في موضوع أمن المعلومات في قطاع التعليم العالي، خاصة في ظل التحول الرقمي المتسارع، وضرورة مواكبة الجامعات للتحديات المرتبطة بحماية البيانات الحساسة.

المراجع:

[1] S. Peisert, "An Examination and Survey of Data Confidentiality Issues and Solutions in Acad,emic Research Computing", Trusted CI Report, June 2021.

[2]أ. ح. ص. عوض الله، "أثر خصائص أمن المعلومات على تحقيق التميز المؤسسي عبر قدرات التعلم التنظيمية في الجامعات الأردنية"، جامعة السودان للعلوم والتكنولوجيا، 2018.

[3] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education", *Future Internet*, vol. 13, no. 2, p. 39, Feb. 2021.

[4] J. R. Price, "Data Security in Higher Education: Protecting Confidential Financial Aid Data", Ed.D. Dissertation, Graduate School of Education, Northeastern University, Boston, Massachusetts, USA, 2022.

[5] H. Al-Kharusi, "Design and Implementation of Student Information System", *International Journal of Computer Science and Information Security*, vol. 9, no. 3, pp. 46–52, 2011.

[6] F. O. Samuel, "Secure Web-Based Student Information Management System", B.S. thesis, Dept. Comput. Sci., Nigeria Police Academy, Wudil, Kano, Nigeria, 2018.

[7] J. B. Earp and F. C. Payton, "Data Protection in the University Setting: Employee Perceptions of Student Privacy", *in Proc. 34th Hawaii Int. Conf. System Sciences*, 2001.

[8] Campus Cafe Software, "Cybersecurity Best Practices to Safeguard Student Data", [Online]. Available: https://campuscafesoftware.com/cybersecurity-student-information-system/. [Accessed: Apr. 15, 2025].

[9] Emerald Insight, "Cybersecurity behaviours of the employees and students at the university", [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/ocj-02-2024-0001/full/html. [Accessed: Apr. 10, 2025].

[10] K. Kipchirchir, K. Kosgey, G. Ongare, and J. Owoche, "Assessing Security Vulnerabilities in University Student Management Information Systems (SMIS) and Their Impact on Student Data Security", *Int. J. Adv. Res. Comput. Commun. Eng. (IJARCCE)*, vol. 13, 2024, doi: 10.17148/IJARCCE.2024.13901.

[11] M. Feng, "Research on Information Data Security of University Archives", *Scientific and Social Research*, vol. 6, no. 5, 2024.

[12] J. Zainudin, F. Puteri, F. Miserom, and N. Roslan, "Securing Academic Student File Using AES Algorithm for Cloud Storage Web-Based System", *in Proc. Int. Conf. Sustainable Practices, Development and Urbanisation (ICONSPADU)*, 2021, pp. 269–279.

[13] M. Yang and J. Wang, "The Security of Student Information Management System Based upon Blockchain", *Journal of Electrical and Computer Engineering*, vol. 2022, Article ID 8186189, 9 pages, 2022.

[14] M. R. DeLong, A. Ingham, R. Carter, and R. Franke, "Protecting Sensitive Research Data and Meeting Researchers' Needs: Duke University's Protected Network", arXiv preprint arXiv:1710.03317, Oct. 2017.

[15] R. Ramya and E. Ranjith, "Student Information Management System", *International Journal of Research Publication and Reviews*, vol. 3, no. 6, pp. 4550–4556, Jun. 2022.

[16] M. Jones, "An Evaluation of Privacy and Security Issues at a Small University", *Technology Interface Journal*, vol. 10, no. 2, 2009.

[17] W. M. Stahl and J. Karger, "Student Data Privacy, Digital Learning, and Special Education: Challenges at the Intersection of Policy and Practice", *Journal of Special Education Leadership*, vol. 29, no. 2, pp. 79–88, Sep. 2016.

[18] N. McKelvey, "Data Protection Issues in Higher Education with Technological Advancements", *International Journal of Evaluation and Research in Education (IJERE)*, vol. 3, no. 3, pp. 133–141, Sep. 2014.

[19] D. Amo, P. Prinsloo, M. Alier, D. Fonseca, R. Kompen, X. Canaleta, and J. Martín, "Local Technology to Enhance Data Privacy and Security in Educational Technology", *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 7, no. 2, pp. 262–273, Nov. 2021.

[20] J. Li, W. Xiao, and C. Zhang, "Data Security Crisis in Universities: Identification of Key Factors Affecting Data Breach Incidents", *Humanities and Social Sciences Communications*, vol. 10, no. 270, 2023.