سلطنة عمان
وزارة التربية والتعليم

رؤية عمان 2040 OmanVision

نتقدم بثقة
Moving Forward with Confidence

الضوابط الأمنية
لاستخدام تطبيقات الذكاء الاصطناعي
في وزارة التربية والتعليم

دائرة أمن المعلومات الإلكترونية

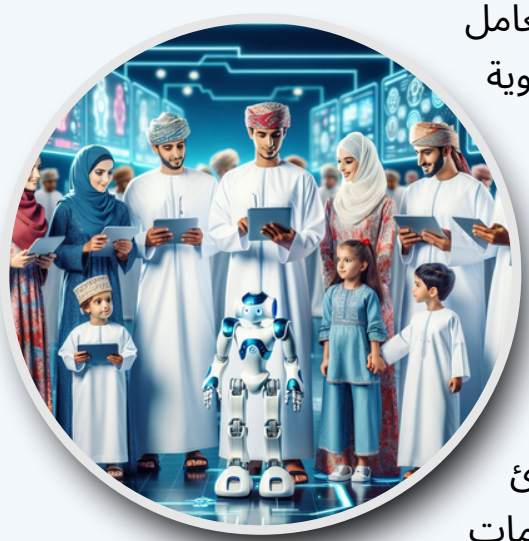
أكتوبر ٢٠٢٤م

المحتويات

مقدمة

يعيش العالم اليوم عصر الابتكار التكنولوجي، المرتبط بالكثير من الأدوات والرقميات الهائلة والمتنوعة التي تسمح له بالتطور والتقدم الفعال في الكثير من المجالات والتي من أهمها مجال التعليم. ولقد تبوأ الذكاء الاصطناعي مركز الصدارة في الاستخدام من قبل العاملين في الحقل التربوي؛ بما يُسهل عليهم عمليتي التعليم والتعلُّم وفق الأنظمة العصرية الذكية والمواكبة للمُستجدات العالمية.

وإذ تتنوع تطبيقات الذكاء الاصطناعي من حيث الأهداف والاستخدامات وتتفاوت في مستويات تأثيرها على الأفراد والمؤسسات، إلا أنه عادة ما تترافق مع بعض التحديات الأمنية التي تتطلب اهتمامًا دقيقًا وحذرًا بالغًا أثناء التعامل معها،لذا أصبح من الضروري جدًا وضع ضوابط أمنية قوية لضمان استخدام تلك التطبيقات بشكل آمن وفعّال.



وتأتي هذه الضوابط لتسليط الضوء على عددٍ من المعايير والمحددات اللازمة لاستخدام تطبيقات الذكاء الاصطناعي بطريقة مستدامة ومسؤولة من قبل مُستخدميها، وُمديريها، ومزودي الخدمة. حيث تعكس هذه الضوابط التزام وزارة التربية والتعليم بتمكين مبادئ الحوكمة التي تسعى إلى تعزيز أمان وخصوصية المعلومات والمحتوى المُتداول وتقديم الخدمات للمستفيدين بشكل أخلاقي ومِهني.

وتشير هذه الضوابط إلى عددٍ من المعايير الأمنية المتعلقة بحماية البيانات، والتحقق من الهوية، وتوفير تقنيات التشفير، وغيرها من الجوانب التي تسهم في تعزيز الاستخدام الآمن لتطبيقات الذكاء الاصطناعي. كما أن هذه الضوابط لا تقتصر فقط على توفير إرشادات الأمان، بل تعزز أيضًا مبدأ الابتكار المستدام والتنظيم الفعّال لاستخدام بعض عمليات التحليل والتفاعل المُستندة على نماذج مختلفة من تقنيات الذكاء الاصطناعي؛ لأتمتة العمليات الإدارية والتواصل مع الطلبة وأولياء الأمور والموظفين، بمعنى آخر، ستسهم هذه الضوابط في خلق بيئة مواتية للاستفادة القصوى منها.

إن وزارة التربية والتعليم ممثلة في دائرة أمن المعلومات الالكترونية لتطمح من خلال الالتزام بتنفيذ هذه الضوابط، إلى بناء مستقبل يعتمد على التكنولوجيا بشكل مسؤول وآمن؛ ليكون للذكاء الاصطناعي إسهام فاعل في تحسين جودة العملية التعليمية ورفع مؤشر التنافسية العالمية الذي يسعى إليه النظام التعليمي في سلطنة عمان وفق رؤية عُمان 2040م.

الأهداف

تحقق الضوابط الأمنية لاستخدام تطبيقات الذكاء الاصطناعي في وزارة التربية والتعليم الأهداف التالية:

1. التوافق مع القوانين والتشـريعات المنظمة لاستخدام تقنيات الذكاء الاصطناعي.
2. تحقيق أهداف البرنامج الوطني للاقتصاد الرقمي، من خلال بناء وتطوير اقتصاد رقمي مزدهر، وتوفير بنية آمنة ومتطورة داعمة لأعمال الحكومة الرقمية، ومتكاملة مع أهداف التنمية الاقتصادية والاجتماعية التي تستجيب لمتطلبات المستقبل والاستدامة بما يحقق رؤية عُمان ٢٠٤٠.
3. تنظيم التعامل مع الذكاء الاصطناعي.
4. التخفيف من المخاطر والتهديدات الأمنية الإلكترونية أثناء التعامل مع الذكاء الاصطناعي.

النطاق

تطبق الضوابط الأمنية لاستخدام تطبيقات الذكاء الاصطناعي على الفئات الآتية:

1. طلبة المدارس الحكومية والخاصة.
2. موظفي وزارة التربية والتعليم
3. المتعاقد معهم والمتدربين.
4. الجهات الخارجية أثناء تعاملهم مع الوزارة.
5. مزوِّدي الخدمات للوزارة.

الضوابط الأمنية لاستخدام تطبيقات الذكاء الاصطناعي

يمكن تصنيف الضوابط الأمنية لاستخدام تطبيقات الذكاء الاصطناعي إلى:

1. ضوابط استخدام المُستفيد لتطبيقات الذكاء الاصطناعي

تتمثل الضوابط الأمنية لاستخدام تطبيقات الذكاء الاصطناعي من قبل المُستفيدين منها فيما يأتي:

أ- الالتزام بالأنظمة والقوانين والتشريعات واللوائح التي ينص عليها قانون حماية البيانات والخصوصية في سلطنة عمان.

ب- الامتثال لضوابط الاستخدام الآمن لأصول الوزارة وسياسة أمن المعلومات المعتمدة فيها.

ج- تجنب الإدلاء إلى الجهات الخارجية – بما فيها مزوّدي الخدمة- بأية معلومات تخصُّ الوزارة أو مُنتسبيها.

د- الامتناع عن مُشاركة أيَّة معلومات تُصنَّف تحت (محدود، مكتوم، سري، سري للغاية).

هـ- الحصول على الموافقات الإدارية اللازمة لتطوير أيُّ محتوى معرفي يخصُّ الوزارة، ومُراجعته من قبل جهات الاختصاص فيها قبل اعتماده بصورته النهائية.

و- الاقتصار على استخدام التطبيقات الموثَّقة والمُصَّرح بها من قبل الوزارة فقط.

ز- استخدام البيانات العامة التي تتواءم ونطاق وزارة التربية والتعليم ورؤيتها ورسالتها.

ح- الإفصاح عن المحتويات الرقمية التي يقوم المُستخدم بإنشائها باستخدام تطبيقات الذكاء الاصطناعي.

ط- تحديد نوع البيانات الخوارزمية التي سيتم جمعها وتخزينها ومعالجتها وتوضيح الغرض الرئيسي من هذا الإجراء.

ي- الحرص على حماية بيانات تسجيل الدخول وهويَّة البيانات التي يتم استخدامها داخل هذه التطبيقات وعدم مُشاركتها مع الآخرين.

ك- أخذ الموافقة الصريحة من الأفراد في حال الرغبة بتصميم شخصيات حقيقية لهم باستخدام هذه التطبيقات.

الضوابط الأمنية لاستخدام تطبيقات الذكاء الاصطناعي

2. ضوابط إدارة تطبيقات الذكاء الاصطناعي

تتمثل الضوابط الأمنية الواجب مراعاتها عند إدارة استخدام تطبيقات الذكاء الاصطناعي فيما يأتي:

أ- التأكد من وضع خطة واضحة لإدارة البيانات تتضمن (آلية جمع البيانات/ آلية تحليل البيانات / آلية تصنيف البيانات / النشر والمشاركة / الاستخدام / حماية البيانات / ملكية البيانات/ الاحتفاظ بالبيانات / إتلاف البيانات).

ب- إخطار دائرة أمن المعلومات الإلكترونية بأيَّة تجاوزات تُخالف الأنظمة والضوابط المنصوص عليها في الوثيقة.

ج- تحديث قوائم التقنيات المُرخصَّة والموثقَّة ومتابعة تجديد رُخصها بصفة دورية.

د- تقييد وصول المستخدمين إلى التطبيقات غير المرخصة من قبل الوزارة.

هـ- التحقق من أن التطبيقات المستخدمة تدعم الخصائص الأمنية المتعلقة بتقييد وتمكين الوصول المصرح وغير المصرح لها (التحقق المتعدد WFA).

و- مُعالجة الثغرات الأمنية المُحتملة لهذه التطبيقات أولاً بأوَّل تجنبًا لمخاطرها.

ز- الإلتزام بالإجراءات / القرارات التنظيمية المنشورة أو المستقبلية الصادرة عن الجهات المعنية في سلطنة عُمان المتعلقة بإدارة البيانات ، أمن الشبكات وأمن وخصوصية بيانات المستخدمين .

3. ضوابط مزوِّدي خدمات تطبيقات الذكاء الاصطناعي

تختص هذه الضوابط بالبنود الواجب مراعاتها عند التعاقد مع مزودي خدمات تطبيقات الذكاء الاصطناعي للوزارة، والتي تتمثل في:

ا- التحقق من المعايير الأمنية فيها، وتقييم مستويات التعامل مع البيانات، وسياسة التشفير، وضوابط الوصول.

ب- تحديد أنواع المخاطر الأمنية عالية المستوى على المنظومة والتي تستوجب تطبيق أسس حماية عالية واتخاذ تدابير أمنية نحوها بمستويات مختلفة .

ج- اتخاذ كافة التدابير الأمنية للمراقبة والحد من الوصول غير المصرح من قبل شخص / أشخاص / جهات الى بيانات المستخدم.

د- التأكيد على أحقيَّة التدقيق على هذه التطبيقات من قبل المختصين بالوزارة؛ للتحقق من الالتزام بالتشريعات الصادرة بشأنها.

هـ- توفير تقنيات التشفير اللازمة لمعالجة البيانات المختلفة أثناء الحركة أو في أثناء التخزين.

و- ضمان استمرارية تقديم الخدمات في حال الانتقال إلى أنظمة تقنية أخرى بما لا يؤثر عليها ويؤدي إلى إيقافها.

قوائم المتابعة والتدقيق

لضمان تحقيق جوانب التوافق والامتثال لاستخدام تطبيقات الذكاء الاصطناعي في الوزارة، يتم مراجعة ذلك والتأكد من استيفاء متطلبات الالتزام بالضوابط الأمنية لذلك وفق قائمة التحقق في الجدول الآتي:

1. قوائم المتابعة والتدقيق الأمنية لاستخدام تطبيقات الذكاء الاصطناعي للمُستفيد ولمدير / مسؤول الخدمة

م	البند	مستوفي	غير مستوفي
1	**الامتثال والتشريعات**		
1.1	تتوافق التطبيق مع قوانين حماية البيانات والخصوصية - قانون (6/2022).		
1.2	تتوافق التطبيق مع احتياجات العمل بالوزارة - سياسة أمن المعلومات الإلكترونية_ تعميم وزاري (281976941).		
1.3	يتوافق استخدام التطبيق مع قوانين وسياسات تصنيف الوثائق بالسلطنة - مرسوم (118/2011).		
1.4	يتوافق استخدام التطبيق مع مدونة السلوك الوظيفي للقيم والأخلاق - قرار الخدمة المدنية (7/2019).		
1.5	يوجد موافقة إدارية داخلية باستخدام التطبيق- قرار (98/2021).		
2	**إدارة الوصول والتحكم**		
2.1	تدعم التطبيق الحماية المتعددة (MFA) أثناء عملية تسجيل الدخول.		
2.2	عدم استخدام بيانات الوزارة (بريد الوزارة) أثناء عمليات التسجيل بدون إذن أمني.		
2.3	وجود تعاقد ساري عند شراء تطبيقات الذكاء الاصطناعي.		

قوائم المتابعة والتدقيق

م	البند	مستوفي	غير مستوفي
3	**الاستخدام المقبول**		
3.1	أخذ موافقة صريحة مكتوبة في تصميم الشخصيات الحقيقة.		
3.2	الإقرار بالمرجعية أثناء استخدام تطبيقات الذكاء (كتابة المرجع).		
3.3	وجود تعهد بالاستخدام الأخلاقي والقانوني وعدم الإساءة.		
3.4	استكمال التدريب والتوعية لبنود الامتثال والتشريعات (1 - 4).		
4	**مكافحة التحيز وعدم العدالة**		
4.1	تقييم التطبيق بشكل منتظم للتحقق من عدم وجود أي تحيزات واتخاذ التدابير اللازمة.		
5	**الحماية والتقييم الأمني**		
5.1	التعهد بضبط الإعدادات الأمنية في التطبيق وإعدادات الخصوصية.		
5.2	التعهد بتحديث مشغلات التطبيقات والأنظمة بشكل مستمر بأخر الإصدارات.		
5.3	اختبار التطبيقات بشكل منتظم وتوثيق النتائج والتحسينات المطلوبة.		
5.4	وجود خطة للاستجابة للحوادث الأمنية المتعلقة بتطبيقات الذكاء الاصطناعي.		
5.5	اتباع إجراءات وقائية لتقليل مخاطر الحوادث الأمنية مثل إجراءات النسخ الاحتياطي والاستعادة.		
5.6	التأكد من أن مزودي خدمات تطبيقات الذكاء الاصطناعي يلتزمون بمعايير الأمان والخصوصية.		

قوائم المتابعة والتدقيق

2.قوائم المتابعة والتدقيق الأمنية لمزوّدي خدمة الذكاء الاصطناعي

م	البند	مستوفي	غير مستوفي
1	**بنود التعاقد للتطبيقات المدفوعة**		
1.1	تضمين بنود حماية البيانات وحقوق البيانات.		
1.2	تضمين إجراءات الاستجابة للحوادث والمخاطر الأمنية.		
1.3	تضمين بنود سياسات التشفير والأطراف الثالثة.		
1.4	تضمين بنود أدوات المراقبة والمتابعة وإدارة الصلاحيات.		
1.5	تضمين بنود التقييم الأمني الدوري لتحقيق الضوابط الأمنية.		
1.6	تضمين بنود تنفيذ التحديثات البرمجية بانتظام لتصحيح الثغرات الأمنية.		

المراجع

مرسوم سلطاني. (أ 2011). تصنيف وثائق الدولة وتنظيم الأماكن المحمية.

مرسوم سلطاني. (ب 2011). قانون مكافحة جرائم تقنية المعلومات.

مرسوم سلطاني. (2022). قانون حماية البيانات الشخصية.

تعميم وزارة التربية والتعليم. (2019). سياسة أمن المعلومات.

تعميم وزارة النقل والاتصالات وتقنية المعلومات. (2021). سياسة استخدام أنظمة الذكاء الاصطناعي.

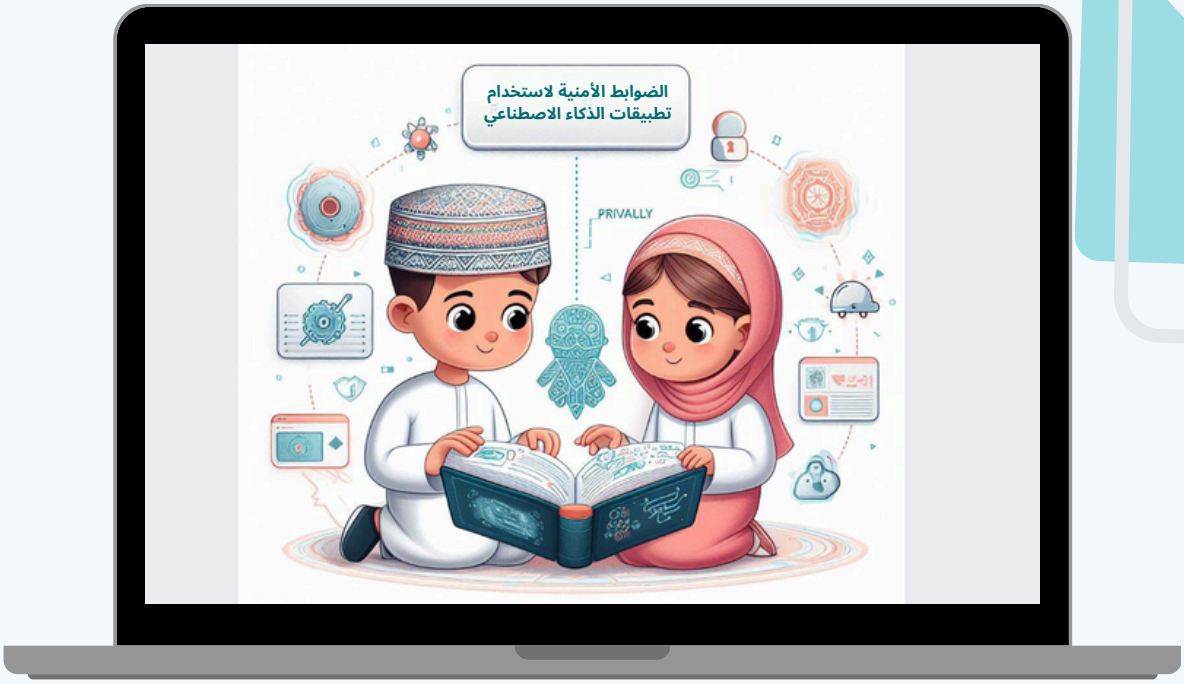
تعميم مركز الدفاع الإلكتروني.(2024). الاستخدام الآمن لتقنيات الذكاء الاصطناعي وحماية المعلومات الحساسة

وكالة الأمم المتحدة للعلوم والثقافة (اليونسكو). (2021). التوصية الخاصة بأخلاقيات الذكاء الاصطناعي.
https://unesdoc.unesco.org/ark:/48223/pf0000381137_ara

وكالة الأمم المتحدة للعلوم والثقافة (اليونسكو). (2023). أخلاقيات الذكاء الاصطناعي.
https://www.unesco.org/ar/artificial-intelligence/recommendation-ethics

European Commission. (2021). *Artificial Intelligence Act*.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

United Nations Educational, S. and C. O. (UNESCO). (2021). *UNESCO's Recommendation on the Ethics of Artificial Intelligence: key facts.*
https://unesdoc.unesco.org/ark:/48223/pf0000385082.page=4



www.moe.gov.om