

دليل سياسات وسيادة واستخدام أدوات الذكاء الاصطناعي في المؤسسات الحكومية

إطار عملي للاستخدام الآمن والمسؤول

السيادة الرقمية

حماية البيانات والمصالح الوطنية

الاستخدام الآمن

ضوابط واضحة للموظفين

الحكومة

مسؤولية بشرية ومساءلة مؤسسية

إعداد وتطوير

المهندس فراس عبد الستار الدليمي

خبير التقنيات الحديثة والذكاء الاصطناعي

دليل سياسات وسيادة واستخدام أدوات الذكاء الاصطناعي في المؤسسات الحكومية

1. المقدمة والهدف

يمثل الذكاء الاصطناعي التوليدي نقلة نوعية في كفاءة الأداء الحكومي، إلا أن استخدامه يتطلب إطاراً تنظيمياً صارماً يوازن بين الابتكار وحماية المصالح الوطنية. يهدف هذا الدليل إلى وضع خارطة طريق واضحة للموظفين في **Place** حول كيفية التعامل مع هذه التقنيات (مثل ChatGPT, Claude, Gemini) لضمان السيادة الرقمية ومنع أي تسريب للمعلومات التي قد تمس بالأمن القومي أو الخصوصية الفردية.

2. نطاق التطبيق

تسري أحكام هذا الدليل على كافة الفئات التالية:

- جميع الموظفين الدائمين والمؤقتين في المؤسسة.
- المستشارين الخارجيين والخبراء التقنيين.
- الشركات المتعاقدة التي تطلع على بيانات المؤسسة أو تقدم خدمات تقنية.
- الجهات الفنية المسؤولة عن تطوير وصيانة البنية التحتية المعلوماتية.

3. تصنيف البيانات والضوابط الأمنية

تعتمد سلامة الاستخدام على الفهم الدقيق لطبيعة البيانات المدخلة في نماذج الذكاء الاصطناعي. يُمنع منعاً باتاً التعامل مع النماذج العامة المفتوحة للبيانات المصنفة.

فئة البيانات	أمثلة توضيحية	حالة الاستخدام
بيانات سيادية وحساسة	الوثائق المصنفة (سرية، سرية للغاية)، الاستراتيجيات الأمنية، محاضر الاجتماعات القيادية.	محظور تماماً
بيانات شخصية (PII)	الأسماء الكاملة، الأرقام الوطنية، السجلات الطبية، البيانات الحيوية، أرقام الهواتف.	محظور تماماً
الأمن السيبراني	الشفرات المصدرة للأنظمة الحكومية، هندسة الشبكات، ثغرات الأنظمة، كلمات المرور.	محظور تماماً
بيانات عامة	القوانين المنشورة، اللوائح التنظيمية العامة، الإحصائيات السكانية المعلنة، الأخبار الرسمية.	مسموح
المراسلات الإدارية	مسودات الخطابات الروتينية، إعادة صياغة رسائل البريد الإلكتروني غير الحساسة، تلخيص الأبحاث العلمية.	مسموح

4. قواعد الاستخدام الآمن والمسؤول

4.1 المسؤولية البشرية (Human-in-the-Loop)

يُعد الموظف هو المسؤول الأول والأخير عن صحة وموثوقية المخرجات. لا يجوز الاعتماد الكلي على الذكاء الاصطناعي في اتخاذ القرارات الإدارية أو القانونية دون مراجعة بشرية دقيقة وتوقيع معتمد من المسؤول المباشر  Person .

4.2 التحقق من الصحة والتحيز

يجب الحذر من ظاهرة "الهلوسة الرقمية" حيث قد تقدم الأدوات معلومات مغلوطة بصيغة وثيقة. يلزم الموظف بمطابقة المعلومات المستخرجة مع المصادر الرسمية المعتمدة قبل اعتمادها في أي تقرير حكومي.

4.3 ضبط إعدادات الخصوصية

عند استخدام الحسابات المؤسسية المصرح بها، يجب التأكد من:

- تعطيل خيارات "تحسين النماذج" أو "تدريب النماذج" (Training Mode) لضمان عدم تخزين البيانات المدخلة في قاعدة بيانات الشركات المزودة.
- استخدام واجهات البرمجيات (APIs) المخصصة للمؤسسات والتي توفر اتفاقيات حماية بيانات (Enterprise Privacy) بدلاً من النسخ المجانية للأفراد.

5. الأدوار والمسؤوليات

إدارة تكنولوجيا المعلومات والأمن السيبراني

- تقييم أدوات الذكاء الاصطناعي قبل اعتمادها ومنح تصاريح الوصول.
- تحديث "القائمة البيضاء" للأدوات الآمنة المسموح باستخدامها.
- تنفيذ عمليات محاكاة واختبارات دورية للتأكد من عدم وجود تسريبات بيانات عبر هذه المنصات.

الموظفون والمستخدمون

- الالتزام بحدود الاستخدام المهني وعدم خلط الحسابات الشخصية بحسابات العمل.
- التبليغ الفوري عن أي اشتباه في ثغرة أمنية أو تسريب غير مقصود للبيانات.
- حضور الورش التدريبية التي تنظمها المؤسسة في تاريخ **Date** وما يليه لرفع الوعي التقني.

6. الامتثال والمساءلة

إن الالتزام بهذا الدليل جزء لا يتجزأ من ميثاق العمل الحكومي. يخضع المخالفون لهذه السياسات، خاصة في حالات تسريب البيانات الحساسة أو استخدام أدوات غير مصرح بها للتعامل مع ملفات رسمية، للمساءلة القانونية والإدارية وفقاً لـ **File** وقوانين الجرائم الإلكترونية المعمول بها في الدولة.

يُراجع هذا الدليل دورياً لمواكبة التطورات السريعة في مجال الذكاء الاصطناعي.

اعتمد بواسطة:

المهندس فراس عبد الستار الدليمي (خبير التقنيات الحديثة والذكاء الاصطناعي)

التاريخ **File**

إعداد وتطوير: المهندس فراس عبد الستار الدليمي

ملخص بصري لأهم ضوابط الدليل

تتطلب البيانات قبل استخدام أدوات الذكاء الاصطناعي

بيانات سيادية وحساسة	محظور تماماً
بيانات شخصية	محظور تماماً
أمن سيبراني	محظور تماماً
بيانات عامة	مسموح
مراسلات إدارية غير حساسة	مسموح

المسؤولية البشرية



لا اعتماد نهائي دون مراجعة بشرية دقيقة ومصدر رسمي عند الحاجة

الخصوصية والأمن السيبراني

