ChatGPT

تذكرة تنفيذية: بناء نظام حوكمة جديد لمشروع Cursor من الصفر

1. الهدف التنفيذي

تهدف هذه التذكرة إلى إقرار وتنفيذ **نظام حوكمة جديد وشامل** لمنصة **Cursor AI** من الصفر، مخصص حصريًا لهذا المشروع. جاء هذا القرار بعد تحليل عميق كشف عن **خمس فجوات حرجة** في الوضع الحالي لمنصة Cursor تتعلق بالمعمارية والأمن والخصوصية والملكية الفكرية والتشغيل. تعتبر منصة Cursor **"منصة وكيل" (Agentic Platform)** متطورة وليست مجرد محرر أكواد بسيط، مما **يضاعف المخاطر النظامية** بشكل كبير. وعليه، فإن بناء نظام حوكمة جديد كليًا بات ضروريًا لضمان معالجة هذه الفجوات جذريًا وتأمين استخدام Cursor في المؤسسة. إن إعادة البناء من الصفر تتيح تصميم حوكمة **مخصوصة للمخاطر الفريدة لـ Cursor** بدلًا من محاولة ترقيع سياسات أو أنظمة حوكمة عامة غير ملائمة. الهدف التنفيذي هو **تحويل Cursor من مصدر مخاطرة كامنة إلى أداة إنتاجية مُدارة ومسؤولة** ، عبر إطار حوكمة محكم يضمن **عدم تنفيذ** المنصة دون ضوابط، ويحمي المؤسسة من الثغرات الأمنية، ويحفظ خصوصية وملكية الشيفرات البرمجية، مع الامتثال الكامل للمعايير والقوانين.

2. الجدول الزمني التنفيذي

وضع جدول زمني واضح من ثلاث مراحل لضمان تنفيذ النظام الجديد بشكل منظم وسريع، مع أطر زمنية محددة لكل مرحلة:

1. **المرحلة الأولى – الفرز والاستقرار (خلال 30 يومًا):** التركيز فورًا على **احتواء المخاطر الحرجة وإيقاف أي استخدام غير مُحَوْكَم** لـ Cursor. الإجراءات التنفيذية في هذه المرحلة تشمل فرض **تفويض "عدم التنفيذ"** على مستوى المؤسسة (حظر استخدام Cursor على أي كود إنتاجي أو حساس)، **الإلزام بوضع الخصوصية القديم** لجميع المستخدمين لضمان عدم تخزين الشيفرات خارجيًا، وتطبيق **عزل شبكي صارم** لـ Cursor (تشغيله في بيئة محمية أو صندوق رمل Sandbox) لمنع أي وصول غير مصرّح به للبيانات. كذلك يتم **تشكيل لجنة حوكمة الذكاء الاصطناعي** للإشراف على هذه الإجراءات الطارئة ووضع أسس الحوكمة الجديدة. الهدف بنهاية هذه المرحلة هو **إيقاف النزيف** التقني وضبط المخاطر الكبرى قبل المضي قدمًا.

2. **المرحلة الثانية – بناء الإطار (خلال 90 يومًا):** الشروع في **بناء الهيكل العظمي لنظام الحوكمة الجديد** بعد استقرار الوضع. في هذه الفترة سيتم تطوير واعتماد **سياسة ذكاء اصطناعي شاملة (AI Policy)** خاصة باستخدام Cursor، تغطي ضوابط الاستخدام والمسؤوليات. يتم أيضًا **إضفاء الطابع الرسمي على بروتوكول توثيق المخرجات** (IP Attribution Protocol) بحيث يصبح إلزاميًا لكل مطور توثيق أي جزء من الكود تم توليده أو تعديله بواسطة Cursor. بالإضافة إلى ذلك، **تُنفَّذ أدوات الحوكمة التقنية** : مثل تشغيل أداة **فحص التراخيص الآلية** على مخرجات Cursor لضمان عدم انتهاك تراخيص البرمجيات المفتوحة المصدر، ودمج أدوات **منع فقدان البيانات (DLP)** لمراقبة وحظر أي محاولة لإدخال بيانات حساسة في المنصة. أيضًا **تدريب المطورين** يتم في هذه المرحلة ("جدار الحماية البشري") لرفع الوعي بمخاطر استخدام الوكيل AI وأفضل الممارسات الآمنة. بنهاية الـ90 يومًا، يُفترض أن يكون **نظام إدارة الذكاء الاصطناعي (AIMS)** الأساسي قد تأسس، شاملاً السياسات والضوابط والعمليات اللازمة.

3. **المرحلة الثالثة – الترسيخ والتحسين (حتى 6 أشهر):** تحويل إطار الحوكمة المبني إلى **عملية حيّة ومستدامة** ضمن بيئة التطوير. خلال هذه المرحلة يتم **تفعيل وظائف المراقبة والإدارة المستمرة** لنظام الحوكمة وفق منهجية NIST (أي الانتقال من التخطيط إلى **القياس والإدارة** الدائمين). سيتم إعداد **لوحات متابعة ولوائح قياس** لمراقبة مخاطر الذكاء الاصطناعي بشكل دوري (مثل مراقبة أي انحراف أو تحيز في مخرجات Cursor أو ظهور ثغرات جديدة) وضمان بقاء الضوابط فعّالة. كذلك تُجرى **مراجعة حوكمة**

رسمية بنهاية الستة أشهر لتقييم أداء النظام الجديد وتحديد أي فجوات أو تحسينات إضافية. مع انتهاء هذه المرحلة، ينبغي أن يكون نظام الحوكمة الجديد مترسخًا في عمليات المؤسسة اليومية، مما يسمح بإزالة تفويض "عدم التنفيذ" والسماح باستخدام Cursor بشكل مُدار وتحت السيطرة الكاملة.

3. هيكلية نظام الحوكمة الجديد

تم تصميم هيكلية نظام الحوكمة الخاصة بـ Cursor بشكل **شامل ومتكامل يغطي دورة حياة استخدام المنصة من التخطيط إلى المراقبة** . يستند النظام إلى أفضل المعايير الدولية لضمان الصلابة والموثوقية، **بدمج إطار عمل NIST لإدارة مخاطر الذكاء الاصطناعي (AI RMF)** ووظائفه الأساسية (الحوكمة، والرسم أو تحديد السياق، والقياس، والإدارة) مع **معيار ISO/IEC 42001** الخاص بنظم إدارة الذكاء الاصطناعي لضمان اتباع نهج **إدارة مؤسسي (AIMS)** يمكن تدقيقه.

مكونات الهيكلية الأساسية تشمل:

- **حوكمة وإشراف استراتيجي:** يتضمن ذلك تشكيل **هيئة حوكمة AI** عليا (مثل لجنة أو مجلس متخصص) تضع السياسات والاستراتيجيات، وتضمن المواءمة مع أهداف المؤسسة والقوانين. هذه الهيئة مسؤولة عن مرحلة التخطيط والتوجيه الاستراتيجي لاستخدام Cursor، بما في ذلك تقييم المخاطر الأولي (Function: Map في NIST) وتحديد نطاق الاستخدام المسموح.
- **الضوابط التشغيلية (Operational Playbook):** وهو مجموعة من **السياسات والإجراءات التقنية الإلزامية** التي تحكم كيفية استخدام Cursor فعليًا في التطوير اليومي. يشمل ذلك سياسات الخصوصية والوصول، وإعدادات الأمن الافتراضية، وإجراءات التعامل مع مخرجات المنصة. هذا الدليل التشغيلي يضمن أنه عند الانتقال من التخطيط إلى التنفيذ اليومي هناك ضوابط واضحة لكل خطوة (من تطوير الكود بمساعدة Cursor إلى اختباره ونشره).
- **بروتوكول** التدخل البشري **وإدارة المخاطر البشرية:** جزء أساسي من الهيكلية هو تضمين **العنصر البشري في الحلقة (HITL)** بشكل منهجي. أي أن أي مخرجات يولدها Cursor تخضع لمراجعة بشرية وفق بروتوكول محدد قبل اعتمادها. كذلك يتضمن النظام برنامج **تدريب وتوعية مستمر** للمطورين ("جدار حماية بشري") لضمان فهم المخاطر (مثل هلوسة الكود أو التحيز المحتمل) والتعامل الصحيح معها. الجانب البشري هذا يغطي وظيفة **القياس** (Monitoring) حيث يلاحظ المطورون أية مشكلات في المخرجات، ووظيفة **الإدارة** (Management) عند اتخاذ إجراءات تصحيحية.
- **الإطار القانوني والامتثال:** جزء لا يتجزأ من الهيكل هو وجود **سياسة استخدام مقبول (AUP)** واضحة ومُلزمة تحكم استخدام Cursor وجميع أدوات الذكاء الاصطناعي التوليدية في المؤسسة. هذه السياسة تحدد **مسؤوليات الأطراف** (المطور، الفريق التقني، الإدارة)، وما هو مسموح وممنوع، وكيفية التعامل مع الملكية الفكرية والبيانات. كما يتضمن الإطار عملية **إدارة مخاطر الطرف الثالث** فيما يتعلق بمزوّد الخدمة (Cursor) لضمان التزامه بالمعايير المطلوبة.
- **المراقبة المستمرة والتحسين** : تشمل الهيكلية أيضًا آليات **مراقبة وقياس دورية** للأداء والالتزام (مثل لوحات مؤشرات الأداء الرئيسية KPIs المذكورة أدناه، وأدوات تدقيق آلية) للتأكد أن نظام الحوكمة يعمل بفعالية وأن الامتثال مستمر. نتائج المراقبة تُغذّي عملية **التحسين المستمر** (مشابه لفكرة دورة PDCA: خطط – نفّذ – تحقق – تحرك) بحيث يتم تحديث الضوابط أو السياسات حسب الحاجة لمواكبة أي تغييرات في المخاطر أو في منصة Cursor نفسها.

بهذا التصميم متعدد المستويات، يبدأ نظام الحوكمة من **مرحلة التخطيط الإستراتيجي** (تقييم مخاطر Cursor ووضع سياسات قبل الاستخدام)، مرورًا **بمرحلة التنفيذ والتطوير** (تطبيق ضوابط تقنية صارمة وإشراك المراجعة البشرية في وقت إنتاج المخرجات)، وصولًا إلى **مرحلة المراقبة والتدقيق** (قياس الامتثال والأداء والتغذية الراجعة للتحسين). جميع المستويات تعمل بتكامل لضمان أن استخدام Cursor في المؤسسة يتم بطريقة **مسؤولة وآمنة ومتوافقة** مع كل من أهداف الشركة والمتطلبات التنظيمية.

4. المسؤوليات والفرق المشاركة

يتطلب تنفيذ نظام الحوكمة الجديد تعاونًا وثيقًا بين جهات متعددة داخل المؤسسة، مع تحديد **واضح للمسؤوليات** لضمان المحاسبة والمساءلة. فيما يلي الجهات الرئيسية المشاركة وأدوار كل منها:

- **اللجنة التنفيذية لحوكمة الذكاء الاصطناعي (AERB): قيادة وإشراف** . هذه اللجنة (أو المجلس) تقود مبادرة بناء نظام الحوكمة الجديد. تتكون من أصحاب المصلحة رفيعي المستوى (مثل المدير التقني CTO، ومسؤول الأمن المعلوماتي CISO، وممثل عن الإدارة القانونية، ومسؤول الابتكار أو التحول الرقمي). مسؤوليتها اعتماد السياسات النهائية (مثل سياسة الذكاء الاصطناعي وAUP)، والموافقة على الضوابط والإجراءات، وتخصيص الموارد اللازمة، ومتابعة تقدم التنفيذ. كما تعمل كجهة **حسم للقرارات** المرتبطة بحوكمة Cursor وتذليل أي عقبات تنظيمية أو إدارية.

- **مسؤول حوكمة الذكاء الاصطناعي (AI Governance Officer): إدارة المشروع والتنسيق اليومي**. يتم تعيين فرد أو فريق كمسؤول عن حوكمة الـAI للإشراف على التنفيذ التفصيلي للخطة. يقوم هذا المسؤول بالتنسيق بين جميع الفرق المعنية، وضمان التزام كل طرف بدوره، وإعداد تقارير منتظمة للجنة التنفيذية حول التقدم والمخاطر. يكون نقطة الاتصال المركزية فيما يخص سياسات وإجراءات Cursor، ويدير جدول المراجعات والتدريبات والتدقيق المستمر.

- **فريق الأمن السيبراني (Security): تنفيذ الضوابط التقنية والمراقبة الأمنية** . يتولى هذا الفريق تطبيق الإجراءات الأمنية التقنية لنظام الحوكمة. يشمل ذلك إعداد **ضوابط الشبكة** لـ Cursor (عزل المنصة أو وضعها خلف جدار ناري مع قائمة بيضاء صارمة للاتصالات المسموح بها)، **تعطيل الميزات عالية الخطورة** أو تقييدها (مثل تعطيل أي وظيفة قد تسمح بتنفيذ أوامر خارجية أو استغلال ثغرات)، ومتابعة تطبيق التحديثات الأمنية والترقيعات لمنصة Cursor باستمرار. كما يراقب الفريق أي **محاولات اختراق أو حوادث أمنية** متعلقة باستخدام Cursor، ويقوم بإبلاغ وإجراءات الاستجابة الفورية (Incident Response) حسب السياسات. فريق الأمن مسؤول أيضًا عن **اختبار فعالية الضوابط** (مثلاً إجراء محاكاة لاختراق بيئة Cursor للتأكد من متانة العزل)، وإدارة أدوات **منع تسرب البيانات (DLP)** المدمجة لضمان عدم خروج بيانات حساسة.

- **فريق التطوير والهندسة (Engineering): الامتثال التقني والعمليات اليومية** . يقع على عاتق فريق التطوير الالتزام بتطبيق سياسات الحوكمة داخل دورة حياة التطوير اليومية. يقود هذا الفريق **دمج أدوات الحوكمة في خط التطوير** – على سبيل المثال، إدراج أداة فحص التراخيص الآلية في أنظمة إدارة المستودعات البرمجية لضمان فحص مخرجات Cursor قبل الدمج، وتطوير أو تكييف بيئة Cursor (بالتعاون مع فريق الأمن) لتفعيل **وضع الخصوصية القديم** بشكل افتراضي لكل المطورين. كما يقوم هذا الفريق بتنفيذ **بروتوكول التوثيق الإلزامي** في نظام إدارة الشيفرة (مثلاً عبر قوالب طلبات الدمج Pull Requests التي تتطلب تعبئة خانة توثيق مصدر الكود إن كان مولدًا بواسطة AI). بالإضافة إلى ذلك، يتعاون فريق التطوير مع الأمن في **اختبارات القبول** ؛ أي عدم السماح بتمرير كود مولد من Cursor إلى مستودع الإنتاج ما لم يستوفِ شروط المراجعة البشرية والتوثيق. على المستوى التنظيمي، يكون قادة فريق التطوير (مثل مدراء الفرق التقنية) مسؤولين عن **مراقبة التزام المطورين** وإبلاغ أي مخالفات أو صعوبات في تطبيق السياسات.

- **فريق الشؤون القانونية والامتثال (Legal & Compliance): الإطار القانوني وضمان الامتثال**. يقوم الفريق القانوني بصياغة واعتماد **سياسة الاستخدام المقبول (AUP)** الخاصة باستخدام أدوات الذكاء الاصطناعي (وعلى رأسها Cursor) بالتنسيق مع اللجنة التنفيذية. يتضمن ذلك معالجة جوانب الملكية الفكرية (توضيح أن حقوق الكود المولّد تعود للمؤسسة، ووضع إرشادات لتجنب إدخال مواد محمية أو سرية في المنصة)، وجوانب حماية البيانات (مثل منع إدخال معلومات شخصية أو سرية إلى Cursor لضمان عدم انتهاك قوانين الخصوصية). كما يتولى الفريق القانوني مسؤولية **ضمان الامتثال التنظيمي** ؛ أي التحقق من أن نظام الحوكمة يتماشى مع أي متطلبات قانونية أو معيارية حالية أو مستقبلية (مثل اللوائح المحلية لحماية البيانات، أو معايير الذكاء الاصطناعي العالمية). ضمن ذلك، يدير الفريق عملية **إدارة مخاطر الطرف الثالث** مع مزوّد Cursor: مراجعة شروط الخدمة واتفاقيات مستوى الخدمة (SLA) وضمان إدراج بنود لحماية

بيانات المؤسسة وحقوقها (مثل اتفاقية عدم استخدام البيانات المقدمة للتدريب، والتزام المزوّد بالإخطار عن الثغرات الأمنية). أخيرًا، يُقدّم هذا الفريق المشورة القانونية في حال حدوث أي حوادث متعلقة بـ Cursor (مثل خرق بيانات أو مطالبة مرتبطة بملكية فكرية)، لضمان اتخاذ الإجراءات القانونية المناسبة فورًا.

- **فريق التدريب والتوعية (HR/Training): بناء القدرات والوعي المستمر** . يكون مسؤول الموارد البشرية أو التدريب مسؤولًا عن تطوير وتنفيذ **برنامج تدريبي إلزامي** للمطورين وجميع من سيستخدم Cursor. هذا التدريب (المسمى أحيانًا **The Human Firewall**) يغطي سياسة الاستخدام المقبول، والمخاطر المحتملة (مثل مشكلة هلوسة الكود أو تسرب البيانات)، والإجراءات المطلوبة من المستخدم للتقيد بالحوكمة (مثل كيفية توثيق المخرجات أو متى يجب طلب مراجعة إضافية). يتم التأكد من **إكمال جميع المستخدمين المعنيين لهذا التدريب** قبل منحهم صلاحية استخدام Cursor، وتوثيق ذلك ضمن سجلات الامتثال. كما يستمر الفريق في تقديم **جلسات توعية دورية** (ربع سنوية مثلًا) لتحديث المعرفة حول أي تهديدات جديدة أو سياسات محدثة، وضمان بقاء الثقافة المؤسسية منسجمة مع أهداف الحوكمة.

باختصار، نجاح نظام الحوكمة يعتمد على **توزيع واضح للمسؤوليات** : جهة عليا تضع التوجه وتراقب، ومسؤول يُنسّق التنفيذ، وفرق تقنية تُطبق الضوابط يوميًا، وجهة قانونية تضبط الإطار النظامي، وجهة تدريبية تدعم بالمعرفة. هذا التعاون متعدد التخصصات سيضمن أن كل جانب من جوانب استخدام Cursor يحظى بالرقابة والتوجيه المناسبين.

5. الضوابط التقنية والسياسات الإلزامية الجديدة

يعتمد النظام الجديد على حزمة من **الضوابط التقنية الصارمة والسياسات الإلزامية** التي يجب تطبيقها فورًا عند استخدام Cursor، لضمان تقليل المخاطر المُحدَّدة إلى أدنى حد. فيما يلي أبرز تلك الضوابط والسياسات:

- **تفعيل وضع الخصوصية القديم (Legacy Privacy Mode) بشكل إلزامي:** يجب أن يعمل Cursor حصريًا في **وضع الخصوصية "القديم"** لجميع المستخدمين وبيئات العمل. هذا الوضع هو الوحيد الذي يضمن بشكل صريح عدم قيام المنصة **بتخزين أي شفرة مصدرية** على خوادم الشركة المزودة. جعل هذا الوضع الإفتراضي والإجباري يمنع تسرب الكود الداخلي إلى السحابة، ويحافظ على متطلبات السرية في البيئات الحساسة.

- **ضوابط شبكة صارمة (Network Whitelisting/Isolation):** يتم **عزل منصة Cursor شبكيًا** قدر الإمكان عن بيئة التطوير الداخلية. يتضمن ذلك تشغيل Cursor في شبكة فرعية محمية أو بيئة معزولة (Sandbox)، مع اعتماد **قائمة بيضاء صارمة للاتصالات الخارجية** التي يمكن أن يقوم بها Cursor. أي اتصال غير ضروري (مثلاً إلى خدمات أو APIs خارجية غير معتمدة) يتم منعه بشكل افتراضي. الهدف هو تقليص سطح الهجوم؛ فإذا حاولت برمجية Cursor الاتصال بخدمة غير مصرح بها أو إرسال بيانات خارجية، ستقوم الضوابط بمنع ذلك فورًا. هذا العزل يحمي أيضًا من مخاطر المعالجات الفرعية (Subprocessors) المتعددة التي تعتمد عليها Cursor، بمنعها من الوصول إلى موارد المؤسسة إلا في حدود ما هو مسموح.

- **التكامل الإلزامي مع أدوات منع فقدان البيانات (DLP): يُدمج نظام DLP** الخاص بالمؤسسة مع منصة Cursor لمراقبة المدخلات والمخرجات. أي محاولة من المستخدم لإدخال **بيانات شديدة الحساسية** (مثل مفاتيح سرية، أو بيانات تعريف شخصية PII، أو شفرة ملكية للغاية) إلى Cursor ستؤدي إلى **إنذار وحظر فوري** قبل إرسالها إلى السحابة. كذلك يتم مراقبة مخرجات Cursor للتأكد من أنها لا تحتوي مصادفةً على أجزاء من بيانات سرية من بيئة التطوير. هذا التكامل يضمن الالتزام الصارم بسياسة "عدم إدخال البيانات الحساسة" ويحمي خصوصية المعلومات وفق القوانين (مثل GDPR عند الاقتضاء).

- **تعطيل الميزات عالية الخطورة: تُعطَّل أو تُقيَّد أي وظائف في Cursor تعتبر ذات مخاطرة أمنية عالية** . على سبيل المثال، إذا كانت المنصة تسمح بتشغيل تعليمات برمجية تلقائيًا كجزء من ميزات الوكيل (مثل خاصية تنفيذ الأوامر أو ملفات قواعد يمكن استغلالها كـ backdoor)، فيجب تعطيل هذه الخاصيات أو وضعها تحت تحكم صارم. كما يتم تفعيل **إعدادات الأمان الافتراضية** الموصى بها (مثل تفعيل وضع

"الثقة في فضاء العمل" Workspace Trust لمنع تشغيل تعليمات برمجية غير موثوقة). الهدف هو منع **استغلال Cursor كناقل هجوم** من قبل مهاجم قد يحقن تعليمات خبيثة في مخرجات AI.

- **بروتوكول التوثيق الإلزامي للملكية الفكرية:** يتم **فرض بروتوكول توثيق** على جميع المطورين عند استخدامهم لمخرجات Cursor. أي جزء من الكود يتم توليده (أو تعديل جزء مهم منه) بواسطة المنصة يجب أن يقوم المطور **بتوثيقه صراحةً في سجلات النظام** (مثلاً في وصف الـCommit أو في التعليقات البرمجية) مع تحديد أنه من إنتاج AI ومراجعة صلاحيته. هذه السياسة تسد الفجوة التشغيلية التي كانت بين السرعة والامتثال؛ فبالرغم من أن التوثيق قد يبطئ العمل قليلاً، إلا أنه **غير قابل للتفاوض** للحفاظ على حقوق الملكية الفكرية للمؤسسة. توفر عملية التوثيق هذه شفافية حول مصدر كل قطعة شيفرة، مما يحمي الشركة في حال ظهور ادعاءات ملكية أو الحاجة لمراجعة مخرجات Cursor لاحقًا.

- **أداة فحص التراخيص الآلية (Automated License Scanner):** يتم إدماج وتشغيل أداة آلية لفحص الشيفرات المصدرية الناتجة عن Cursor **بحثًا عن أي كود قد يكون خاضعًا لتراخيص برمجيات مفتوحة المصدر** صارمة (مثل GPL أو غيرها). تقوم هذه الأداة بتحليل النص المولد ومقارنته بقاعدة بيانات الشفرات مفتوحة المصدر المعروفة للتعرف على أي تشابه كبير. في حال اكتشاف تطابق محتمل مع كود خاضع لحقوق نشر أو رخصة، يتم تنبيه الفريق القانوني وفريق التطوير لاتخاذ إجراء (مثلاً استبدال الجزء المتأثر أو الحصول على ترخيص مناسب). هذا الضابط يضمن تجنب **تلوث الرخص** في قاعدة الكود الخاص بالمؤسسة، ويحميها من خطر أن تصبح ملزمة بفتح مصدر برامجها نتيجة إدخال كود غير متوافق ترخيصيًا دون قصد.

- **التدخل البشري في الحلقة (HITL) كقاعدة إلزامية: يُفرض وجود الإنسان في دورة المراجعة** لكل مخرجات Cursor قبل دمجها أو استخدامها في قاعدة الكود النهائية. عمليًا، يعني ذلك أن أي كود أو اقتراح تولده المنصة يجب أن يخضع لمراجعة مطور بشري أو زميل تقني. يتم فحص المخرجات للتأكد من صحتها وخلوها من المشاكل (أمنية أو منطقية)، وكذلك مدى التزامها بمعايير الترميز الداخلية. لن **يُسمح بنشر أي كود إلى بيئة إنتاج** جاء من Cursor بدون اعتماد بشري صريح حتى لو اجتاز الاختبارات الآلية، وذلك لضمان وجود **طبقة أمان أخيرة بشرية** تقلل مخاطر الثقة العمياء بالمخرجات الآلية. هذه السياسة قد تؤثر على سرعة التطوير لكن تم تبنيها **للأولوية القصوى للأمان والموثوقية**.

- **منع التنفيذ المباشر في خطوط الإنتاج:** كجزء مكمل لـHITL، يتم منع التكامل التلقائي لمخرجات Cursor في خطوط الإنتاج أو النشر المستمر CI/CD دون خطوات مراجعة إضافية. أي عملية **توليد كود أو إصلاح تلقائي** تتم بواسطة Cursor في قاعدة الشفرة يجب أن تمر عبر **مرحلة مراجعة/اختبار مستقلة** قبل السماح بنشرها. هذا الإجراء يضمن أن بقاء Cursor **أداة مساعدة** ضمن العملية وليس صاحب القرار النهائي، مما يحمي من أي خطأ غير مكتشف قد يصل للإنتاج.

- **خطة بديلة (Plan B) للحالات عالية الحساسية:** في الحالات التي يكون فيها مشروع برمجي أو جزء من الكود على درجة عالية جدًا من السرية أو الحساسية، **لا يتم استخدام منصة Cursor على الإطلاق**. وبدلاً من ذلك، يتم **النظر في حلول داخلية آمنة** . على المدى الطويل، ستعمل الفرق التقنية على تقييم واعتماد **نسخة ذاتية الاستضافة من أدوات المبرمج الذكي** (سواء نسخة تجارية خاصة On-Prem من Cursor إن توفرت، أو أدوات مفتوحة المصدر مشابهة يمكن تشغيلها بالكامل داخل بيئة المؤسسة). هذه **الخطة البديلة** تهدف إلى إزالة أي احتمال لتسرب المعلومات الحساسة إلى خارج حدود الشركة، وضمان توفر خيار آمن حتى لو تعطلت الخدمة السحابية أو ثبت عدم توافقها التام مع سياساتنا. في الوقت الحالي، يُنصح بهذا النهج التحوطي في المشاريع الحرجة إلى حين اكتمال الثقة بمنصة Cursor ضمن الضوابط أعلاه.

جميع ما سبق هي **ضوابط إلزامية** يجب اتباعها حرفيًا من قبل كل مستخدم وفريق فيما يخص استخدام Cursor. سيتم تضمين هذه النقاط في **سياسة المؤسسة الرسمية لاستخدام المنصة** ، وأي خرق لها قد يؤدي إلى إجراءات تصحيحية أو تأديبية حسب خطورة المخالفة. الهدف هو توفير **شبكة أمان متعددة الطبقات** تغطي التقنية والبشر والإجراءات، بحيث نخفف المخاطر إلى مستوى مقبول دون أن نحرم الفريق تمامًا من فوائد Cursor في تعزيز الإنتاجية.

6. الضمانات القانونية والامتثالية

يتكامل النظام الجديد مع **ضمانات قانونية صارمة والتزامات امتثال** لضمان أن استخدام Cursor لا يعرّض المؤسسة لمخاطر قانونية أو انتهاكات تنظيمية. فيما يلي العناصر الرئيسة في هذا الجانب:

- **سياسة الاستخدام المقبول (AUP) للذكاء الاصطناعي:** سيتم إصدار **وثيقة سياسة رسمية** توضح شروط وضوابط استخدام أدوات الذكاء الاصطناعي التوليدية في الشركة، وفي مقدمتها Cursor. هذه السياسة – التي يقرّها القسم القانوني والإدارة العليا – تلزم جميع الموظفين والمقاولين باتباع الإرشادات المحددة لاستخدام Cursor بشكل مسؤول. تتضمن الـAUP بنودًا حول **المواد الممنوعة إدخالها** (مثل البيانات الشخصية أو أي معلومات سرية بدون إذن)، و **الملكية الفكرية** (توضيح أن مخرجات الذكاء الاصطناعي تعتبر ملكًا للمؤسسة مع ضرورة توثيقها، وحظر نسخ أي مواد محمية دون تصريح)، و**حماية الأمن والخصوصية** (مثل اشتراط استخدام أوضاع الخصوصية ومنع مشاركة الأكواد خارج القنوات المعتمدة). سيُطلب من كل مستخدم توقيع أو قبول هذه السياسة رقميًا قبل استعمال Cursor، وذلك لضمان قابلية الإنفاذ القانوني لها.

- **ضمان خصوصية البيانات وعدم تخزين الشيفرة:** تلتزم المؤسسة، ضمن عقودها وسياساتها، بعدم انتهاك خصوصية البيانات عند استخدام Cursor. عمليًا، يعني ذلك **ضمان أن شيفراتنا وبياناتنا لن تُخزن أو تُستخدم من قبل مزوّد Cursor لأي غرض غير مصرح به** . لتحقيق هذا الضمان، اعتمدنا فنيًا وضع الخصوصية القديم كما ذكر، ولكن قانونيًا سنسعى لتوثيق الأمر مع المزود. فريق الشؤون القانونية سيقوم بمراجعة اتفاقية معالجة البيانات (DPA) أو اتفاقية الخدمات مع شركة Cursor لضمان وجود **بنود ملزمة** حول عدم احتفاظهم بشيفرات العملاء وعدم استخدامها في تدريب النماذج، بالإضافة إلى متطلبات إشعارنا في حال حصول أي خرق أمني لديهم يمس بياناتنا. بهذا نكون قد فعلنا كل ما بوسعنا (فنيًا وقانونيًا) للحفاظ على سرية الكود المصدري الخاص بنا وخصوصية أي معلومات قد تمر عبر المنصة.

- **حماية حقوق الملكية الفكرية للمؤسسة:** تُقر السياسات بأن **أي كود أو ناتج يولده Cursor أثناء العمل يُعتبر ملكية فكرية للمؤسسة** مثل أي كود يكتبه موظف. للتأكد من صمود هذا الأمر قانونيًا، يتولى الفريق القانوني **تقييم تبعات ملكية المخرجات** والتأكد من عدم وجود بنود في شروط خدمة Cursor تمنحهم أي حق في مخرجات المستخدم. سيتم توثيق هذا الجانب في سياسة داخلية، وقد تتم إضافة **إشعار للمستخدمين** يظهر عند استخدام Cursor يؤكد على مسؤوليتهم في التوثيق وأن الحقوق تعود للمؤسسة. كذلك سيتم توجيه المطورين إلى **تجنب الاعتماد المفرط على Cursor في كتابة أجزاء كاملة وحساسة من الشيفرة بدون تدخل بشري وتفكير نقدي** ، حفاظًا على أصالة واستقلالية قاعدة الكود الخاصة بنا. في حال وجود أي ادعاء من جهة خارجية بأن جزءًا من ناتج Cursor ينتهك حقوق نشر، سيكون لدينا من خلال بروتوكول التوثيق سجل واضح لمنشأ ذلك الجزء وكيف تم توليده ومراجعته، مما يحمينا قانونيًا ويتيح معالجة سريعة (كتعديل الكود أو استبعاده إذا لزم الأمر). باختصار، النظام يضمن أننا **لا نفرط بأي حق ملكية فكرية** نتيجة استخدام المنصة، بل يؤطر استخدامها بشكل مسؤول ومراقَب.

- **الامتثال للمعايير والتنظيمات ذات الصلة:** تم تصميم نظام الحوكمة بحيث **يلتزم بأفضل الممارسات والمعايير الدولية** في مجال حوكمة الذكاء الاصطناعي وأمن المعلومات. فعلى سبيل المثال، المبادئ المستقاة من NIST AI RMF (كإطار مخاطرة) ومن ISO 42001 (كنظام إدارة) تعني أننا متوافقون بشكل كبير مع المتطلبات المتوقعة لأي **تدقيق خارجي** أو شهادة قد تطرح مستقبلًا لهذا المجال. سنستمر في **مراقبة المشهد التنظيمي** ؛ فإذا صدرت لوائح محلية أو دولية (مثل قانون الاتحاد الأوروبي للذكاء الاصطناعي AI Act أو تحديثات لقوانين الخصوصية) تمس استخدام أدوات مثل Cursor، سيتم **تحديث سياساتنا فورًا** للامتثال لها. هذا يشمل أيضًا الالتزام بسياسات أمن المعلومات العامة للمؤسسة (مثل سياسات ISO/IEC 27001 الخاصة بأمن المعلومات) فيما يتعلق بإدارة مفاتيح API وسرية البيانات ونحوها عند استخدام Cursor.

- **إدارة مخاطر الطرف الثالث (Third-Party Risk Management):** يعتبر مزوّد Cursor **طرفًا ثالثًا حيويًا** بالنسبة لنا، لذا سيتم تطبيق إجراءات صارمة لإدارة علاقتنا معه. سيُجري فريق الأمن وتقنية المعلومات **تقييمًا أمنيًا** لمزوّد Cursor (مراجعة تقارير الثغرات المعروفة، اختبار الخدمة لدينا في بيئة معزولة، التحقق

من آليات التحديث والاستجابة لديهم). كما سيحتفظ الفريق القانوني بحقه في **التدقيق التعاوني**؛ أي قد نطلب من المزوّد تقديم تقارير امتثال (مثل شهادات ISO أو SOC2) لإثبات مستوى نضج أمنهم وحوكمتهم الداخلية. علاوة على ذلك، أي تحديثات أو تغييرات كبيرة يطرحها المزوّد في منصة Cursor سيتم إخضاعها لـ **مراجعة مخاطر فورية** لدينا قبل السماح بها في بيئة المؤسسة (مثل إضافة ميزة جديدة ستقيمها اللجنة التنفيذية قبل تفعيلها لمستخدمينا). بهذه الطريقة، نضمن أن علاقتنا المستمرة مع الطرف الثالث لا تدخل منها مخاطر غير متحكم بها.

- **الضمانات والإلتزامات الداخلية:** داخليًا، سيتم **تحديد آليات للمساءلة** في حال عدم الالتزام بالحوكمة. على سبيل المثال، إذا تبين أن أحد المطورين خالف سياسة AUP (كتخزين كود حساس على المنصة في وضع غير مسموح)، فسيواجه إجراءات تصحيحية وتأديبية وفق لوائح الموارد البشرية. أيضًا سيتم توثيق كل الموافقات والاستثناءات (إن وجدت) المتعلقة باستخدام Cursor؛ أي إن أرادت أي وحدة عمل الحصول على **استثناء مؤقت** لأي سياسة (وهو أمر غير مستحسن إلا للضرورة القصوى)، فيجب الحصول على موافقة رسمية من اللجنة التنفيذية وتسجيلها. أخيرًا، سيتولى قسم التدقيق الداخلي أو الامتثال إجراء **مراجعات دورية** للتأكد من أن الجميع يلتزم بالضوابط المقررة وأن الضمانات القانونية فعالة عمليًا وليست حبرًا على ورق.

هذه الجوانب القانونية والامتثالية تشكل خط الدفاع الأخير الذي يكمل الضوابط التقنية والبشرية، لضمان أن حوكمة Cursor ليست مجرد توجيهات داخلية، بل هي **إطار مُلزم** يحمي المؤسسة قانونيًا وسمعتها ومصالحها على المدى الطويل.

7. مؤشرات الأداء الرئيسية (KPIs)

لقياس فعالية نظام الحوكمة الجديد وتتبّع امتثاله وأثره على المخاطر، تم تحديد مجموعة من **مؤشرات الأداء الرئيسية** التي سيتم رصدها بانتظام. هذه الـKPIs تركز على جودة الحوكمة وليس على الإنتاجية المحضة، لضمان أن الهدف (استخدام آمن ومسؤول) يتحقق. فيما يلي أهم المؤشرات المستهدفة:

- **زمن اكتشاف الحوادث الأمنية المرتبطة بـ Cursor:** الوقت المستغرق من وقوع أي حادث أمني متعلق باستخدام Cursor (مثل محاولة اختراق عبر المنصة أو اكتشاف ثغرة جديدة مستغلة) إلى حين اكتشافه من قبل فرقنا. **الهدف:** أقل من 24 ساعة. مؤشر الأداء هذا يضمن فعالية المراقبة والإنذار المبكر؛ فإذا كان النظام يعمل بكفاءة، سنكشف أي مشكلة بسرعة ونستجيب لها قبل تفاقم الضرر.

- **نسبة إكمال التدريب الإلزامي (AUP Training Completion):** نسبة المطورين والمستخدمين المستهدفين الذين أكملوا **برنامج التدريب الإلزامي على سياسة الاستخدام المقبول والحوكمة** الخاص بـ Cursor. **الهدف:** 100% من المستخدمين النشطين يجب أن ينجزوا التدريب ويجتازوا الاختبار الخاص به. هذا المؤشر يعكس مدى انتشار ثقافة الامتثال والوعي بالمخاطر بين الكوادر التقنية.

- **معدل منع تسرب البيانات الحساسة (DLP Enforcement Rate):** يُقاس بعدد الحالات التي قامت فيها أدوات **منع فقدان البيانات (DLP)** بحظر إدخال أو إخراج بيانات حساسة عبر Cursor. **الهدف:** الوصول إلى **صفر حادث** أو الاقتراب منه من خلال **التحسين المستمر**. انخفاض هذا الرقم بمرور الوقت يعني أن المستخدمين يلتزمون بسياسة عدم إدخال البيانات الممنوعة، أو أن أدواتنا فعالة في كل محاولة خاطئة. في البداية قد يظهر بعض الحوادث (مثلاً محاولة إدخال مفتاح API وتم منعه)، لكن الهدف هو **تقليل هذه المحاولات تدريجيًا** عبر التدريب والضبط.

- **معدل التجاوز البشري – Human Override Rate:** نسبة مخرجات Cursor التي يقوم المطورون **برفضها أو تعديلها يدويًا** بدلاً من قبولها كما هي. على عكس التصور المعتاد، **ارتفاع** هذا المعدل إلى حد معقول **إيجابي** لأنه يدل على يقظة بشرية وعدم اعتماد أعمى على المخرجات الآلية. **الهدف المبدئي:** > 15% (قابلة للتعديل حسب نضج النظام لاحقًا). أي نطمح أن لا يقل معدل المخرجات التي يقرر الإنسان تعديلها عن 15%، خاصة في الأشهر الأولى، لضمان أن المطورين يراجعون بوعي. إذا كان معدل التجاوز 0% مثلًا، فهذه علامة خطر (تعني أن كل ما تقترحه الآلة يتم قبوله دون تمحيص). بالمقابل، سنراقب أيضًا

النوعية: إن كان المعدل مرتفعًا جدًا ربما يشير إلى مشكلة في جودة مخرجات Cursor تتطلب تدخلاً في الإعدادات أو تدريب النموذج.

- **معدل "هلوسة" الكود (Code Hallucination Rate):** عدد الحوادث التي يتم فيها اكتشاف **أخطاء منطقية أو أكواد غير صحيحة** ناتجة عن Cursor وتم تمريرها دون قصد إلى مرحلة الاختبار أو ما بعده. قد يتم قياس ذلك عبر تقارير الأخطاء التي يرجع سببها إلى اقتراحات Cursor أو عبر مراجعات الكود حيث يقول المراجع أن الجزء الفلاني خاطئ تمامًا ("هلوسة" تقنية). **الهدف:** انخفاض مستمر لهذا المعدل. سنبدأ بتسجيل خط الأساس ثم نسعى عبر التحسينات في الضوابط والتدريب إلى تقليله بانتظام. هذا المؤشر يركز على **جودة المخرجات** ومدى نجاح الحوكمة في منع الأخطاء الجسيمة قبل وصولها للإنتاج.

- **نسبة توثيق إسناد المخرجات (IP Attribution Coverage):** نسبة عمليات الكوميت (Commits) في مستودع الشفرة التي تحتوي على كود مولد بواسطة Cursor وقام صاحبها **بتوثيق ذلك بشكل صحيح** وفق البروتوكول (ذكر أن الكود من AI ومراجعة صلاحيته). **الهدف:** الوصول إلى **95% فأعلى** من الالتزامات تحتوي على توثيق سليم عندما يكون هناك محتوى من إنتاج Cursor. هذا المؤشر يعكس مدى **التزام المطورين بالسياسة** ونجاح عملية المراجعة الداخلية؛ فإذا كانت التغطية أقل (مثلاً 70%) فهذا يعني أن هناك الكثير من مخرجات Cursor تندس في الكود بدون توثيق، ما يشكل خطرًا يستدعي تدخلاً إداريًا وتحسين العملية.

سيتم عرض هذه المؤشرات وغيرها ضمن **لوحة قياس خاصة بحوكمة الذكاء الاصطناعي** يشرف عليها قسم الامتثال وتقنية المعلومات. سيتم رفع تقارير شهرية للجنة التنفيذية تتضمن قيم هذه الـKPIs مع تحليل لأي انحرافات وخطة إجراءات تصحيحية عند الحاجة. بهذه الطريقة، نستطيع أن **نقيس فعليًا نجاح نظام الحوكمة** ونبرهن بالأرقام على تحسن الوضع (أو نتنبه بسرعة لأي خلل لنقوم بمعالجته).

8. خارطة طريق التطوير المستقبلي (بعد أول 6 أشهر)

بعد تنفيذ نظام الحوكمة الجديد واستقراره خلال ستة أشهر، من المهم وضع تصور **للتطوير المستمر والتحسينات المستقبلية** لضمان بقاء النظام مواكبًا للتغيرات وتوسيع نطاق فائدته. فيما يلي خارطة الطريق المقترحة لما بعد المرحلة التأسيسية الأولى:

- **مراجعة شاملة بعد 6 أشهر:** مع نهاية الشهر السادس، يتم إجراء **مراجعة تدقيق شاملة** لنظام حوكمة Cursor. هذه المراجعة تشمل تقييم كل عنصر: فعالية الضوابط التقنية (هل حصلت حوادث؟ هل من ثغرات جديدة؟)، مستوى الامتثال البشري (نتائج KPIs مقابل الأهداف)، ملاءمة السياسات والإجراءات الحالية. قد يشمل الأمر تكليف فريق خارجي أو مدقق داخلي مستقل لتقييم النظام بحيادية. بناءً على نتائج المراجعة، تُعد **توصيات تحسين** ويتم **تحديث خطة العمل للسنة التالية** اعتمادًا على ما تم اكتشافه.

- **تحسين مستمر وتحديث السياسات:** تعتبر الحوكمة عملية ديناميكية. بعد المرحلة الأولى، سيتم **تحديث السياسات والإجراءات بانتظام** لمواكبة أي تطورات. على سبيل المثال، إذا طرحت شركة Cursor تحديثًا كبيرًا للمنصة يتضمن مزايا جديدة، ستقوم اللجنة التنفيذية وفريق الأمن بتقييم المزايا وإضافة **ضوابط جديدة** أو تعديل القواعد الحالية قبل السماح باستخدام المزايا. كذلك، قد نكتشف من خلال الممارسة الحاجة إلى **سياسات أكثر تفصيلًا** في نقاط معينة (مثلاً توضيحات إضافية في سياسة AUP بناءً على أسئلة المطورين). سيتم إصدار ملاحق أو نسخ منقحة من الوثائق التنظيمية حسب الحاجة، على ألا تقل دورية المراجعة الرسمية عن مرة سنويًا حتى لو لم يحدث تغيير ظاهر.

- **توسيع نطاق نظام الحوكمة:** بمجرد إثبات نجاح نظام الحوكمة مع Cursor، يمكن توسيع **نطاق الحوكمة ليشمل أدوات ذكاء اصطناعي أخرى** حالية أو مستقبلية في المؤسسة. فمثلاً لو قررت فرق أخرى استخدام أدوات توليد أكواد منافسة لـ Cursor أو منصات ذكاء اصطناعي في مجالات مختلفة (كالموارد البشرية أو المالية)، فيمكن استخدام الإطار الحالي كقاعدة **لبناء حوكمة مماثلة** تعدّل لتلك السياقات. الهدف أن يكون لدينا **نموذج حوكمة موحّد** قدر الإمكان لكل تطبيقات الذكاء الاصطناعي، مما يبسط

الامتثال ويخلق ثقافة موحدة. هذا التوسع سيكون تدريجيًا وبالتنسيق مع أصحاب المصلحة في تلك المجالات.

- **الحصول على الشهادات واعتماد المعايير:** على المدى المتوسط (12 شهرًا فأكثر)، وبالتزامن مع نضوج نظام الحوكمة، سنسعى إلى **الحصول على شهادات** أو إقرارات رسمية لبرنامجنا للحوكمة. فإذا تم إصدار معيار ISO/IEC 42001 بشكل نهائي (أو أي معيار مشابه لحوكمة الذكاء الاصطناعي)، سنعمل على **مطابقة نظامنا معه والتقدم للاعتماد** ، مما يوفر ثقة إضافية للإدارة العليا وأصحاب المصلحة الخارجيين (مثل العملاء أو الجهات الرقابية) بفعالية ضوابطنا. كذلك سنضمن أن نظامنا يلبّي أي **متطلبات تنظيمية جديدة** قد تبرز، مثل الامتثال لقانون الذكاء الاصطناعي الأوروبي حال اعتماده، أو أي إرشادات حكومية محلية. إن تحقيق الامتثال معاييريًا سيجعل حوكمتنا **مستدامة ومعترفًا بها** وليس مجرد ممارسة داخلية خاصة.

- **تقليل الاعتماد على الطرف الثالث (استراتيجيات المدى البعيد):** بالرغم من أن الضوابط الحالية تجعل استخدام Cursor آمنًا إلى حد كبير، إلا أنه يظل خدمة خارجية بمخاطرها الخاصة. خلال الفترة التالية لـ6 أشهر، سنقيم بشكل أعمق **الخيارات البديلة** : مثل إمكانية **إنشاء نسخة داخلية** من نظام الذكاء الاصطناعي لتوليد الأكواد ليحل محل Cursor في بعض المهام. قد يكون ذلك عبر التعاون مع مزوّد Cursor لتوفير نسخة خاصة (On-Prem) أو باعتماد مشروع مفتوح المصدر نقوم بتطويره داخليًا وتدريبه على قواعد الشفرة لدينا. هذا التوجه، إن كان مجديًا تقنيًا وماليًا، يمكن أن يقلل المخاطر طويلة الأجل بشكل جوهري لأنه يضع كامل السيطرة التقنية في أيدينا. سنضع خطة دراسة وجدوى لهذا الخيار خلال العام الأول، وعلى ضوئها يُتخذ قرار استراتيجي حول المضي به أو الاكتفاء بتحسين العلاقة مع المزود الخارجي.

- **تعزيز أدوات المراقبة والتحليل التنبؤي:** بينما اعتمدنا لوحات مؤشرات للأداء والمخاطر، سنطور مستقبلاً قدرات **تحليل أعمق للمخاطر بشكل استباقي** . مثلاً، قد ننشئ نظامًا ذكيًا يراقب **سلوك Cursor** مع مرور الوقت ويستخدم خوارزميات لكشف أي **أنماط شاذة** في المخرجات أو الاستخدام (مثل اكتشاف ارتفاع مفاجئ في محاولات إدخال بيانات محظورة، أو تكرار نوع معين من الأخطاء مما قد يشير لثغرة أو نقص في التدريب). كذلك سيتم دمج حوكمة Cursor أكثر في عمليات **DevSecOps** العامة للمؤسسة، بحيث تصبح فحوصات الامتثال والأمان المتعلقة بـ Cursor جزءًا طبيعيًا من خطوط الأنابيب (Pipeline) لكل مشروع برمجي جديد. هذا التكامل المستقبلي سيجعل الالتزام أسهل وأوتوماتيكيًا قدر الإمكان، ويخفف العبء اليدوي عن الفرق مع الحفاظ على مستوى عالي من الحماية.

ختامًا، هذه الخارطة المستقبلية تضمن أن **نظام الحوكمة الجديد ليس جامدًا أو محدود الأفق** ، بل قابل للتطور والنمو مع نمو احتياجاتنا التقنية وتغير مشهد الأخطار والتشريعات. سنستمر في تبني **ثقافة التحسين المستمر** لضمان أن منصة Cursor – وأي تقنية ذكاء اصطناعي أخرى – تبقى دومًا أداة **منتجة وآمنة** في يد مؤسستنا.

بناءً على ما تقدم، يُطلب من فريق التنفيذ التقني البدء فورًا باتخاذ الخطوات اللازمة لكل مرحلة كما هو مفصل أعلاه، مع رفع التقارير الدورية عن التقدم المحرز إلى اللجنة التنفيذية لحوكمة الذكاء الاصطناعي. إن الالتزام الصارم بهذا الخطة سيُمكّن المؤسسة من الاستفادة من قدرات Cursor بصورة آمنة ومسؤولة، محققةً التوازن المنشود بين **الابتكار التكنولوجي** و**السلامة المؤسسية**.
