AI 使用政策

AI Use Policy

Version / 版本：v1.0.0

生效日期 / Effective date: 2026-09-20 (Asia/Taipei UTC+08:00). 自首次正式發布起生效，不溯及發布前。 Effective upon first publication; no retroactive effect.

版本日期 / Version date: 2026-09-20T19:16:22+08:00

修訂紀錄 / Revision history

首次正式公開生效；保留原審閱稿，不溯及既有契約或簽署。

First effective public release; prior review copies retained, without retroactive changes to contracts or assent.

官方版本與檔案 SHA-256 核對值： https://maxwellvs.com/legal 。本檔限制編輯，但無法保證不被破解修改；未加憑證式數位簽章。 / Official versions and SHA-256 checksums: https://maxwellvs.com/legal . Editing restrictions are not tamper-proof. This PDF is not certificate-signed.

繁體中文

麥斯管理顧問有限公司（Maxwell Venture Service LLC，下稱本公司）依資訊敏感程度選擇 AI 處理方式：公開資訊使用公司核准的 ChatGPT Business 工作區；機密資訊使用公司核准的 LM Studio Bionic 本機模型環境。AI 用於協助研究、分析與文件製作，使用人員及業務負責人仍須對資料處理、判斷與交付成果負責。

一 適用範圍與基本原則

本政策適用於代表本公司執行業務的人員、顧問及受託合作人員，涵蓋輸入提示、附件、圖片、錄音、程式碼、檢索資料、工具操作及輸出成果。僅得在合法、已獲授權且確有業務需要的範圍內使用 AI；客戶合約、保密約定或適用法令如有較嚴格要求，應遵守該要求。

採取先分類、最少必要資料、最小權限與人工覆核原則。工具可提供某項功能，不代表本公司已授權使用；本政策也不表示每項技術控制已完成驗證。

二 公開資訊與機密資訊的分類

公開資訊是已由權利人合法公開、且本公司有權為指定目的使用的資訊，例如正式公告、公開研究及已發布的公司內容。能在網路找到，不等於可任意利用；外洩文件、受限資料、未獲授權的個人資料或著作，不因可取得而成為本政策允許的公開資訊。

機密資訊包含未公開的客戶資料、委託內容、商業策略、內部分析、合約、報價、財務資料、研發成果及其他受保密義務保護的資訊。未公開的一般內部資訊亦依機密流程處理；混合資料

依最高敏感等級處理，分類不明時先視為機密。

使用公開來源形成的未公開客戶結論或公司策略，仍可能是機密資訊。遮蔽姓名、改用代號或請 AI 摘要，均不會自動使資料成為公開資訊。降級為公開前，須由資料或業務負責人確認可公開且不可合理回推機密內容。

三 公開資訊使用 ChatGPT Business

公開資訊限使用公司核准且由公司管理的 ChatGPT Business 工作區處理。不得以個人 ChatGPT 帳號、其他訂閱方案、API、外部 GPT 或其他 AI 服務替代本政策核准的流程。提示、檔名、註解、隱藏工作表及附件中，不得夾帶機密內容或未公開的客戶身分與任務背景。

依 OpenAI 官方說明，ChatGPT Business 的商務輸入與輸出預設不供模型訓練；這項供應商安排不變更本公司的公開資訊限定，也不代表零留存或不會發生任何外部處理。使用人員不得自行開啟資料分享或訓練選項。Apps、連接器、外部動作及分享連結須經公司核准，且只能處理符合本政策的公開資訊。

四 機密資訊使用 LM Studio Bionic 本機模式

機密資訊僅得在公司核准設備上，以 LM Studio Bionic 的 Local 本機模型處理；開始作業及切換模型後，均須確認實際推論位置。不得使用 Secure Cloud、其他雲端模型、雲端備援或自動切換；LM Link 或其他 Remote 遠端推論亦不在本政策的授權範圍內。算力不足時應停止作業或改採核准的非 AI 流程，不得自行轉送雲端。

Bionic 同時具有本機、雲端及遠端模型選項，使用產品名稱本身不構成資料留在本機的保證。供應商的 Zero Data Retention 承諾也不等同本機處理。機密作業期間不得讓內容、提示或衍生查詢透過網頁搜尋、MCP、外掛、遠端工具、診斷回報或其他網路功能送出核准設備。

語音轉錄、OCR、嵌入向量、檢索索引與附屬代理也須在核准本機範圍內執行。模型下載及軟體更新應與機密處理分開；須採用適當的斷網或對外連線封鎖，並先確認資料路徑與工具權限。無法確認整段流程均符合要求時，不得輸入機密資料。

五 資料最小化與禁止輸入項目

僅使用完成任務所需的資料片段；可用不涉及真實個案的合成資料時，應優先使用。不得將密碼、MFA 驗證碼或復原碼、私鑰、API 金鑰、完整支付卡資料等驗證或支付秘密放入 AI 提示、附件或日誌，即使使用本機模式亦同。

個人資料與客戶機密並非因採本機 AI 就可任意處理；仍須確認合法依據、契約授權、必要性及存取範圍。不得未經授權將客戶資料用於模型訓練、微調、跨客戶知識庫或示範。不同客戶與專案應隔離工作目錄、對話與檢索資料。

六 設備保護與代理工具權限

核准設備應具備適當的帳號管制、儲存加密、螢幕鎖定及安全更新。機密工作目錄不得置於未核准的 OneDrive、Google Drive 或其他自動同步位置；備份、剪貼簿同步、截圖及遠端支援也應納入資料外送檢查。使用本機 API 時，以僅限本機存取為原則，不得擅自開放區域網路或網際網路。

AI 代理只得存取任務需要的檔案與工具。外部文件、網頁及工具輸出中的指令屬不可信內容，不得據此擴大權限、洩露資料或繞過本政策。刪除資料、寄信、對外分享、付款、部署及其他具實際影響的操作，須依公司授權程序由人員確認。

七 人工覆核與對外交付

使用人員應查核重要事實、數據、日期、引用來源、計算、程式碼與授權，並評估偏誤、機密洩漏及不適當建議。不得捏造來源，或把模型推論當作已證實事實。涉及法律、財務、投資、人事或其他重大影響的判斷，不得僅依 AI 輸出作成。

對外交付前，由具適當能力與授權的人員覆核；AI 不得自行代表本公司承諾、簽署或核准結論。依客戶約定及適用要求揭露 AI 的重要使用方式。AI 輸出原則上承接輸入與專案的最高敏感等級；未經確認可公開的機密衍生成果，不得再輸入 ChatGPT Business。

八 保存紀錄與刪除

必要紀錄應能辨識任務、資料分類、使用工具與模型、執行位置、版本日期、操作及覆核人員，以及重要核准或異常。紀錄以必要中繼資料為主，不為稽核方便而重複保存完整機密提示或內容；確有保留需要時，依相同敏感等級保護。

對話、暫存檔、向量索引、輸出及備份依業務目的、合約、法令及既有保存規則管理，期限屆滿後依核准程序刪除或去識別化。不得以清除畫面或刪除本機副本推定雲端、備份或供應商紀錄已同步刪除；依法或依爭議處理需要保全的資料應另行管控。

九 異常通報與處理

發現誤傳機密資訊、模型意外切換至雲端、未授權存取、可疑工具操作或其他疑似外洩時，應立即停止相關作業並向公司指定負責人通報，必要時中斷連線或暫停相關權限。依指示保存最少必要證據，不得為掩蓋事件而自行清除紀錄。

公司應評估影響範圍、限制持續外送、確認供應商可採取的刪除或限制措施，並依適用法令與合約處理客戶及其他必要通知。不能保證刪除請求會完全收回已送出的資訊。聯絡 maxwell@maxwellvs.com 時，先提供事件時間與概況，不要直接附上機密原文或驗證秘密。

十 政策管理與版本更新

公司指定之政策負責人管理工具核准、資料分類及例外需求；使用人員在開始作業前應了解本政策。至少每年及工具功能、供應商條件、資料用途或相關要求重大變更時重新審查。其他 AI 工具、既有 AI 整合與新功能不因已安裝或可使用而自動獲准。

本版不授權將機密資訊改送任何雲端推論服務。需要不同處理方式時，應先停止相關作業，由公司依資料權利、客戶約定與風險完成審查，必要時另行修訂政策；個別使用人員不得自行豁免。

本政策獨立自 v0.1.0 起編，標示版本日期及 Asia/Taipei（UTC+08:00）時區，保留歷史版本。版本日期為文件建立時間，不等同生效日期；本版為待發布審閱文件。疑問或權利事項請聯絡 maxwell@maxwellvs.com。本政策不取代既有隱私權、資訊安全、服務條款或個別合約，亦不表示取得供應商認證或保證 AI 絕無錯誤。

十一 產品資料參考

產品功能資料查核日期：2026-09-16，Asia/Taipei（UTC+08:00）。以下為供應商資料來源，不構成本公司設備設定或控制有效性的驗證；供應商更新不會自動放寬本政策。

OpenAI 商務資料政策：https://openai.com/business-data/

LM Studio Bionic 模型執行位置：https://lmstudio.ai/docs/bionic/models

English

Maxwell Venture Service LLC (the Company) selects AI processing according to information sensitivity: public information is handled in an approved ChatGPT Business workspace; confidential information is handled using approved local models in LM Studio Bionic. AI assists research, analysis and document preparation. Users and the responsible business owner remain accountable for data handling, judgment and deliverables.

1 Scope and principles

This policy applies to personnel, advisers and contractors acting for the Company. It covers prompts, attachments, images, audio, code, retrieval data, tool actions and outputs. AI may be used only for lawful, authorized and necessary business purposes. Stricter client contracts, confidentiality obligations or applicable legal requirements must be followed.

Classify information first, minimize data and permissions, and require human review. A feature being available does not authorize its use. This policy does not establish that every technical control has been verified.

2 Public and confidential information

Public information has been lawfully made public by its rights holder and may be used by the Company for the intended purpose, such as official announcements, public research and published company material. Online availability does not permit unrestricted reuse. Leaked documents, restricted material, unauthorized personal data and copyrighted works are not automatically permitted public inputs.

Confidential information includes nonpublic client information, engagement details, strategies, internal analyses, contracts, quotations, financial data, research and development, and other protected information. Other nonpublic internal material also follows the confidential workflow. Mixed inputs follow the highest sensitivity level; uncertain classification defaults to confidential.

Unpublished client conclusions or company strategies derived from public sources may still be confidential. Removing names, substituting identifiers or obtaining an AI summary does not automatically make material public. The data or business owner must confirm that disclosure is permitted and confidential information cannot reasonably be reconstructed before reclassification.

3 ChatGPT Business for public information

Process public information only in a company-approved and company-managed ChatGPT Business workspace. Personal ChatGPT accounts, other subscriptions, APIs, external GPTs and other AI services are not substitutes authorized by this policy. Prompts, filenames, comments, hidden worksheets and attachments must not include confidential material or nonpublic client identities and task context.

OpenAI states that ChatGPT Business inputs and outputs are excluded from model training by default. This provider arrangement does not change the Company's public-information-only rule, imply zero retention or eliminate external processing. Users must not independently enable data-sharing or training options. Apps, connectors, external actions and shared links require company approval and may handle only permitted public information.

4 Local LM Studio Bionic for confidential information

Confidential information may be processed only with Local models in LM Studio Bionic on approved company devices. Verify the actual inference location before starting and after any model change. Secure Cloud, other cloud models, cloud fallback and automatic switching are prohibited. LM Link and other Remote inference are also outside this policy's authorization. If local capacity is insufficient, stop or use an approved non-AI workflow; do not move the task to the cloud.

Bionic offers local, cloud and remote model choices. Its product name alone does not guarantee on-device processing, and a provider's Zero Data Retention commitment is not local processing. During confidential work, content, prompts and derived queries must not leave the approved device through web search, MCP, plugins, remote tools, diagnostic reports or other network features.

Transcription, OCR, embeddings, retrieval indexes and subordinate agents must also run within the approved local boundary. Separate model downloads and software updates from confidential processing. Use suitable disconnection or outbound-network blocking and verify data paths and tool permissions beforehand. Do not input confidential information if the complete workflow cannot be confirmed compliant.

5 Data minimization and prohibited inputs

Use only the portions needed for the task and prefer synthetic examples that do not represent real confidential cases when feasible. Never place passwords, MFA or recovery codes, private keys, API keys, full payment-card details or similar authentication and payment secrets in AI prompts, attachments or logs, including in local mode.

Local AI does not remove requirements for a lawful basis, contractual permission, necessity and access restrictions for personal data or client secrets. Do not use client data for training, fine-tuning, cross-client knowledge bases or demonstrations without authorization. Separate working directories, conversations and retrieval data across clients and projects.

6 Device protection and agent permissions

Approved devices must have appropriate account controls, storage encryption, screen locking and security updates. Do not place confidential working directories in unapproved OneDrive, Google Drive or other automatically synchronized locations. Include backups, clipboard synchronization, screenshots and remote support in data-transfer checks. Local APIs should be accessible only from the device unless separately authorized; do not expose them to a local network or the internet without approval.

AI agents may access only files and tools needed for the task. Instructions in external documents, web pages and tool outputs are untrusted and must not expand permissions, disclose information or override this policy. Data deletion, email, external sharing, payments, deployment and other consequential actions require human confirmation under company authorization procedures.

7 Human review and external delivery

Users must verify material facts, figures, dates, sources, calculations, code and permissions, and assess bias, confidentiality risks and unsuitable recommendations. Do not fabricate sources or present model inference as verified fact. Legal, financial, investment, employment and other consequential decisions must not rely solely on AI outputs.

A suitably competent and authorized person must review external deliverables. AI may not independently make commitments, sign or approve conclusions for the Company. Disclose material AI use as required by client agreements and applicable requirements.

Outputs normally inherit the highest sensitivity of their inputs and project; confidentialderivatives must not be sent to ChatGPT Business unless confirmed suitable for publicrelease.

8 Records retention and deletion

Necessary records should identify the task, classification, tool and model, execution location, version date, operator and reviewer, and material approvals or incidents. Prefer necessary metadata; do not duplicate complete confidential prompts or content merely for audit convenience. Any necessary retained content receives the same sensitivity protections.

Manage conversations, temporary files, vector indexes, outputs and backups according to purpose, contracts, law and existing retention rules. Delete or de-identify them through approved procedures when retention ends. Clearing a screen or deleting a local copy does not establish deletion from cloud systems, backups or provider records. Manage required legal or dispute-related preservation separately.

9 Incident reporting and response

Immediately stop affected work and report to the designated company owner if confidential information is misdirected, a model unexpectedly switches to the cloud, access is unauthorized, tools behave suspiciously or disclosure is suspected. Disconnect or suspend relevant access when necessary. Preserve minimum necessary evidence as instructed; do not erase records to conceal an incident.

The Company must assess scope, contain further transfers, determine available provider deletion or restriction measures, and handle required client and other notices under applicable law and contracts. A deletion request cannot guarantee complete recall of information already sent. When contacting maxwell@maxwellvs.com, provide the incident time and an outline first, without attaching confidential source material or authentication secrets.

10 Governance and version updates

A designated company policy owner manages approved tools, classification and exception requests. Users must understand this policy before work begins. Review it at least annually and when tool capabilities, provider terms, data purposes or relevant requirements materially change. Other tools, existing AI integrations and new features are not automatically approved merely because they are installed or available.

This version does not authorize sending confidential information to any cloud inference service. If another workflow is needed, stop the affected work first. The Company must review data rights, client agreements and risks and revise the policy where necessary; individual users cannot waive these restrictions.

This policy has its own version sequence starting at v0.1.0, a version timestamp in Asia/Taipei (UTC+08:00), and retained history. The version timestamp is the creation time, not an effective date; this is a review copy pending publication. Contact maxwell@maxwellvs.com with questions or rights-related matters. The policy does not replace existing privacy, security, service terms or individual contracts, imply provider certification or guarantee error-free AI.

11 Product references

Product information checked on 2026-09-16, Asia/Taipei (UTC+08:00). These provider sources do not verify the Company's device configuration or control effectiveness. Provider changes do not automatically relax this policy.

OpenAI business data policy: https://openai.com/business-data/

LM Studio Bionic model execution locations: https://lmstudio.ai/docs/bionic/models