隱私權政策

Privacy 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。 補充洽詢、Cookie、服務商、兩年保存及權利申請。

First effective public release; prior review copies retained, without retroactive changes to contracts or assent. Adds enquiries, cookies, providers, two-year retention and rights requests.

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

本政策適用於網站瀏覽、合作洽詢、信箱驗證、電子同意及實際開放的帳號功能。公開閱讀不要求登入；目前不提供線上付款或自動續訂。洽詢表單的個別告知與本政策併行；不因本政策更新擴張已取得資料的利用目的。

營運及個資蒐集主體

本網站由麥斯管理顧問有限公司（Maxwell Venture Service LLC）經營，統一編號：42629242；公司所在地：臺北市大同區太原路50號2樓。文件、個資及服務相關事項請聯絡 maxwell@maxwellvs.com。

一、我們蒐集的資料

透過 Email 洽詢時，我們會收到您提供的聯絡信箱、公司、需求說明及附件，用於回覆與確認合作需求。公開閱讀不要求登入；使用帳號功能時，才涉及以下會員資料。

會員資料包括姓名、聯絡 Email、公司與職稱（如提供）、偏好語言、國家 / 市場地區、時區、內容興趣及分語言電子行銷選擇。社群登入由 Supabase Auth 處理；MVS 不會取得您的社群密碼，也不蒐集身分證、護照或居留證號碼。

為保護會員與處理爭議，系統另保存註冊資料建立與異動前後值、異動欄位、事件時間、當事人與操作者識別碼、社群登入連結 / 解除及管理員查閱 / 匯出紀錄。Supabase Auth 平台日誌亦可能包含登入結果、IP 位址與 User-Agent。

二、使用目的與依據

資料用於提供會員服務、內容權限、交易聯繫、偏好設定、資安防護及您另行同意的電子行銷。電子行銷同意可分別針對中文與英文撤回，不影響基本會員功能。

稽核紀錄僅用於帳號安全、防止濫用、履行法令義務、內部調查、法律主張或抗辯、爭議處理，以及回應具有法定權限機關的正式要求；不作一般電子行銷分析。

三、服務供應商與跨境處理

本網站目前不透過線上結帳蒐集信用卡、帳單地址或付款資料。帳號與登入資料由 Supabase 雲端服務處理；洽詢信件由電子郵件服務處理。資料可能在服務供應商營運地區跨境處理。請勿在洽詢信件中提供完整卡號、密碼或身分證件。

四、保存、存取與安全

一般會員資料保存至會員帳號刪除、法定保存期屆滿或蒐集目的消失為止。會員資料異動與帳號安全稽核紀錄自各事件發生日起保存五年；如有司法、主管機關、爭議或其他書面法律保全需求，相關紀錄得延長保存至案件終結及適用法定期間屆滿。保全原因與調取 / 匯出行為亦會留下紀錄。

稽核資料採管理員限權、資料庫禁止更新 / 刪除及逐事件 SHA-256 鏈結等防竄改措施。這些措施可協助驗證一致性，但不代表法院、公證人或鑑識機構已預先認證其證據能力。

五、您的權利

您可登入會員帳號更正資料或撤回行銷同意，也可來信申請查閱、複製、更正、停止利用或刪除。為遵守法令、建立 / 行使 / 防禦法律權利或執行有效法律保全所必須的稽核資料，可能無法立即刪除；MVS 會說明限制理由。適用法律另有更高保障時，從其規定。

六、聯絡方式

資料控管者：麥斯管理顧問有限公司（Maxwell Venture Service）。聯絡信箱：maxwell@maxwellvs.com。

資訊安全紀錄與 MFA

為身分驗證、異常事件分析、稽核與復原，本公司於合理且適法範圍管理必要安全紀錄，依資料性質、法令要求及安全需要決定合理保存期間；不承諾永久或百分之百完整記錄所有活動。詳見資訊安全與強制 MFA 聲明。既有特定紀錄之保存規則仍依本政策及適用法律辦理。

簽署紀錄與必要資料

為確認會員同意、履行契約、資訊安全及處理爭議，保存帳號識別碼、簽署姓名、文件版本與完整快照、文件雜湊、選擇語言、逐項同意內容、文件提供時間、伺服器簽署時間及 MFA 驗證層級。文件紀錄不包含 MFA 密鑰、QR Code、驗證碼或完整登入 Token，也不將簽署用於廣告追蹤。必要簽署資料不提供時，無法啟用會員功能，但仍可公開瀏覽；行銷選擇獨立且可撤回。簽署及相關稽核紀錄原則自事件日起保存五年，依法有必要的保全另行記錄，期滿依適用法律評估刪除或去識別化。可透過會員文件頁下載本人副本，或寄信申請個資權利。

帳號刪除、歷史保留與行銷排除

使用者可在帳號安全頁完成 MFA 後刪除自己的帳號，無須先接受新條款。確認後移除登入身分，終止帳號存取，清除非必要個人資料，並以「已刪除帳號」保留必要歷史主體。舊工作階段不得繼續存取；重新註冊不繼承舊權限或行銷同意。

刪除時撤回所有行銷同意。已刪除帳號及其歷史紀錄不得加入行銷活動、名單、行銷匯出或同步，不得用於行銷分析、廣告受眾或投放。任何行銷流程須在實際使用前重新檢查帳號狀態與目前同意，不得沿用快取名單或歷史同意。

必要稽核、文件簽署、交易、授權與刪除紀錄僅限授權人員用於原已告知的安全、合規、爭議或權利處理。既有稽核紀錄依原五年保存規則及有記錄的保全例外處理；其他類別依適用目的與期限管理，不代表永久保留全部個資。到期處理與備份管理由授權人員依受控程序辦理。刪除帳號不自動取消既有個別合約或完成退款，相關事項可聯絡 maxwell@maxwellvs.com。

合作洽詢、驗證與電子同意

蒐集姓名、Email、公司 / 組織、職稱、產業、初步需求及您選填的電話、網站與聯絡偏好；另保存文件全文、版本、雜湊、勾選事項、驗證及簽署時間，並處理必要防濫用紀錄。用途為信箱驗證、需求評估、聯絡、客製問卷與必要權利處理；不因此建立會員、付費委任、預約或行銷訂閱。

網站資料僅由依職務授權的人員處理，管理介面要求 MFA；公司通知副本寄至 maxwell@maxwellvs.com，收件確認寄至您的信箱。洽詢內容不自動送入 AI。必要資料不提供時，無法使用驗證及洽詢表單，但仍可匿名閱讀或另洽公司討論其他聯絡方式。請勿提交密碼、證件、敏感個資或未獲授權的第三人機密。

服務商、利用地區與外部社群

網站主機及必要執行服務使用 Netlify，資料庫與相關身分驗證服務使用 Supabase，洽詢系統寄信使用 Resend SMTP，並涉及寄件、公司及收件人信箱所使用的郵件服務商。利用方式包括受限存取、資料庫儲存、加密傳輸、寄信、備份及必要安全維護。利用對象限本公司依職務授權人員、上述受託服務商及依法有權機關；不出售洽詢資料。

資料由臺灣的本公司處理，亦可能於上述服務商及其受託處理者提供主機、儲存、備份、郵件傳遞或支援的境外地區處理；本網站不表示資料僅存於臺灣或單一國家。涉及特定洽詢的實際處理地區，可來信申請查詢，由本公司依當時使用的服務設定核實回覆。需限定資料所在地者，請在提交機密前另議合約安排。

前往 Facebook、Vocus、LinkedIn 等外部網站後，亦適用其自身條款及資料政策。加入 Facebook 社團不等於訂閱 MVS 行銷；社團發文的可見性依平台與社團設定，並非保密提交管道。

Cookie 與本機偏好

本網站以 mvs_locale Cookie 保存中英文偏好，設定期限為一年。可透過瀏覽器刪除或限制 Cookie；刪除後可能需重新選擇語言。實際使用登入功能時，驗證服務另需工作階段 Cookie；其期限依工作階段及服務設定。必要的驗證 / 安全 Cookie 被封鎖時，相關功能可能無法使用。

若日後加入非必要分析、廣告追蹤或第三方嵌入功能，應先更新用途、服務商與保存期限說明，並依適用法律提供必要選擇；本政策不是對尚未揭露追蹤用途的概括同意。

洽詢保存期限與人工刪除

未成交或已結案的洽詢內容、聯絡資料及公司郵件副本，自確認不承接或結案日起最長保存兩年；必要目的提前消失或合法刪除請求成立時，提前處理。超過期限須由授權人員人工檢視並刪除或去識別化，不因尚未檢視而取得額外的一般使用權。尚在處理中的洽詢僅於目的必要期間保存，並定期確認是否應結案。

必要的簽署證據與稽核紀錄依既有規則，自事件日起原則保存五年；不得藉此將整份洽詢內容一律延長至五年。司法、主管機關或具體爭議需保全時，記錄保全依據、範圍及解除條件，限目的使用，結束後恢復期限管理。已成立的委任依個別合約與適用法定保存義務處理。

人工作業須核對網站資料庫、公司可控制的郵件副本及備份；不能逐筆即時刪除的隔離備份，限制一般存取，依備份輪替處理，復原時重新套用刪除清單。接獲申請時會說明實際限制與預計處理方式，不宣稱所有服務商備份可立即抹除。收件人自行保存的副本由其控制。

個資權利及申訴入口

請至「個資權利申請與申訴流程」（/privacy-rights）查看申請方式、法定處理期間、行銷拒絕及後續申訴。無須建立會員、接受新條款或同意行銷才能提出申請。

English

This policy covers browsing, consulting enquiries, email verification, electronic assent and account features actually available. Public reading requires no account; online payments and automatic renewal are unavailable. The enquiry-specific notice applies alongside this policy. This update does not expand the purposes for previously collected data.

Website operator and data collector

This website is operated by 麥斯管理顧問有限公司 (Maxwell Venture Service LLC), Taiwan Unified Business Number 42629242. Registered address: 臺北市大同區太原路50號2樓 (2F., No. 50, Taiyuan Rd., Datong Dist., Taipei City, Taiwan). Contact maxwell@maxwellvs.com for documents, personal data and services.

1. Data we collect

Email inquiries provide us with the contact address, company details, needs and attachments you choose to send, so we can respond and clarify potential engagements. Public reading does not require sign-in; the member information below applies when account features are used.

Member data includes name, contact email, optional company and title, language, country or market region, time zone, content interests and language-specific marketing choices. Social sign-in is processed by Supabase Auth. MVS does not receive social passwords or collect government identity document numbers.

To protect members and resolve disputes, the system also records profile creation and before/after changes, changed fields, event time, subject and actor identifiers, social-account link/unlink events, and administrator access/export events. Supabase Auth platform logs may also contain sign-in results, IP addresses and User-Agent data.

2. Purposes and legal bases

Data is used for membership, content access, transaction communications, preferences, security and separately consented marketing. Chinese and English marketing consent can be withdrawn independently without affecting core membership.

Audit records are used only for account security, abuse prevention, legal compliance, internal investigations, legal claims or defence, dispute resolution, and valid requests from legally authorised authorities. They are not used for general marketing analytics.

3. Service providers and international processing

The website does not currently collect card, billing-address or payment information through online checkout. Account and authentication data is processed by Supabase; inquiries are processed through email services. Data may be processed across provider locations. Do not include full card numbers, passwords or identity documents in inquiries.

4. Retention, access and security

General member data is retained until account deletion, expiry of legal duties or the end of its purpose. Profile-change and account-security audit records are retained for five years from each event. Where a documented judicial, regulatory, dispute-related or other legal hold applies, relevant records may be retained until the matter and applicable statutory period end. The hold reason and access/export activity are also logged.

Audit data is protected by administrator-only access, database-level update/delete blocking and a per-event SHA-256 chain. These controls support integrity verification but do not amount to advance certification of admissibility by a court, notary or forensic authority.

5. Your rights

You may update data and withdraw marketing consent in your account, or contact us to request access, a copy, correction, restriction or deletion. Audit data required for legal compliance, establishing, exercising or defending legal rights, or a valid legal hold may not be deleted immediately; MVS will explain the restriction. Any stronger mandatory rights under applicable law remain unaffected.

6. Contact

Data controller: Maxwell Venture Service LLC. Contact: maxwell@maxwellvs.com.

Security records and MFA

Necessary security records support authentication, anomaly analysis, audits and recovery within reasonable and lawful limits. Retention follows data type, legal requirements and security needs; permanent or exhaustive recording is not promised. See the Security and Mandatory MFA Notice. Specific existing retention rules remain subject to this policy and applicable law.

Assent records and necessary data

To establish member assent, perform the contract, protect security and resolve disputes, we retain the account identifier, signatory name, document version and complete snapshot, document hash, selected language, individual confirmations, document-offer time, server signing time and MFA assurance level. These records contain no MFA secret, QR code, verification code or complete login token and are not used for advertising tracking. Without necessary assent data, account features cannot be activated; public browsing remains available. Marketing choices are separate and withdrawable. Assent and related audit records are ordinarily retained for five years from the event; necessary legal holds are documented separately, followed by deletion or de-identification assessment under applicable law. Members may download their own copy or email a data-rights request.

Account deletion, retained history and marketing exclusion

After MFA, users may delete their own accounts from Account security without accepting new terms. Confirmation removes the sign-in identity, ends account access, clears nonessential profile fields and retains a historical subject labelled Deleted account. Old sessions cannot continue access; new registrations inherit neither old access nor marketing consent.

Deletion withdraws all marketing consent. Deleted accounts and retained history must not enter campaigns, lists, marketing exports or synchronisations, marketing analytics or advertising audiences. Every marketing workflow must recheck account status and current consent immediately before use; cached lists and historical consent are insufficient.

Necessary audit, agreement, transaction, entitlement and deletion records are restricted to authorised staff for previously disclosed security, compliance, dispute or rights handling. Existing audit records follow the stated five-year rule and documented holds; other categories follow their applicable purposes and retention periods, not indefinite retention of all personal data. Authorised staff manage expiry and backups through controlled procedures. Account deletion does not automatically cancel separate contracts or complete refunds; contact maxwell@maxwellvs.com.

Enquiries, verification and electronic assent

We collect name, email, organization, job title, industry, initial needs and optional phone, website and contact preferences. We retain the document, version, hash, confirmations, verification and assent times and necessary anti-abuse records. Purposes are email verification, assessment, contact, tailored questionnaires and necessary rights handling; this creates no membership, paid engagement, appointment or marketing subscription.

Authorized personnel handle records for their duties, with MFA required for administrative access. A company notification copy goes to maxwell@maxwellvs.com and a receipt to your email. Enquiries are not automatically sent to AI. Without required data, verification and the enquiry form cannot be used; anonymous reading and discussion of alternative contact remain available. Do not submit passwords, identity documents, sensitive personal data or unauthorized third-party secrets.

Providers, processing locations and external communities

Hosting and necessary execution use Netlify; database and related authentication use Supabase; enquiry delivery uses Resend SMTP and the email providers serving sender, company and recipient mailboxes. Processing includes restricted access, database storage, encrypted transmission, email, backups and necessary security maintenance. Recipients are authorized company staff, these service providers and lawfully authorized authorities. Enquiry data is not sold.

The Company processes data in Taiwan; overseas processing may occur where these providers and their subprocessors host, store, back up, deliver email or provide support. We do not represent that data stays exclusively in Taiwan or one country. You may ask us to verify the actual locations relevant to an enquiry against the service settings in use. Discuss contractual location restrictions before submitting confidential material.

External destinations such as Facebook, Vocus and LinkedIn also apply their own terms and data policies. Joining a Facebook group does not subscribe you to MVS marketing. Post visibility depends on platform and group settings; groups are not confidential submission channels.

Cookies and local preferences

The mvs_locale cookie stores Chinese/English preference with a one-year expiry. Browser settings can remove or restrict cookies; you may need to select a language again. When sign-in is actually used, authentication also requires session cookies whose expiry follows session and service settings. Blocking necessary authentication/security cookies may prevent those features from working.

Before adding nonessential analytics, advertising tracking or third-party embeds, we will update purposes, providers and retention disclosures and provide choices required by applicable law. This policy is not blanket consent to undisclosed tracking.

Enquiry retention and manual deletion

For enquiries declined or closed without an engagement, enquiry content, contact data and company email copies are retained for at most two years from recorded decline or closure. We act earlier when the necessary purpose ends or a valid deletion request applies. Authorized personnel must manually review and delete or de-identify expired data; pending review grants no additional ordinary-use rights. Active enquiries are kept only as necessary and periodically reviewed for closure.

Necessary assent evidence and audit records normally follow the existing five-year period from the event. This does not extend every enquiry in full to five years. Judicial, regulatory or specific dispute holds must document basis, scope and release conditions, restrict use, and return to ordinary retention management after the hold. Established engagements follow their contracts and applicable statutory duties.

Manual handling checks the website database, company-controlled email copies and backups. Isolated backups that cannot immediately delete individual records are restricted, handled through backup rotation, and have deletion requests reapplied on restoration. We explain actual limitations and expected handling when a request is received; we do not promise instant erasure across provider backups. Recipients control their own copies.

Rights and complaints

See Personal Data Rights and Complaints (/privacy-rights) for requests, statutory decision periods, marketing objections and escalation. No membership, acceptance of new terms or marketing consent is required to submit a request.