資訊安全、強制多因素驗證與責任限制聲明

Cybersecurity, Mandatory Multi-Factor Authentication and Limitation of Liability Notice

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

Maxwell Venture Service LLC（麥斯管顧，下稱「本公司」）重視網站、資訊系統、帳號及使用者資料之安全。

本公司資訊安全管理採取以下核心原則：

合理資安措施（Reasonable Security Measures）+ 可稽核證據（Auditable Security Evidence）+ 精確責任限制（Precise Limitation of Liability）

本公司依網站服務性質、資訊系統架構、所處理資料之性質及敏感程度、可合理預見之資訊安全風險，以及適用法律與法規要求，採取合理、適當且與風險相稱之技術性及組織性安全措施。

然而，任何連接網際網路之網站、資訊系統、雲端服務、軟體、第三方平台或通訊系統均無法保證百分之百安全。本公司採取資訊安全措施之目的，在於合理降低資訊安全事件發生之可能性及其影響程度，而非保證任何資訊系統永遠不會遭受攻擊、入侵、漏洞利用、資料外洩或服務中斷。

一、所有網站帳號強制使用 MFA

凡建立、持有或使用本網站帳號，並存取需要身分驗證之功能、服務、資料或管理介面之使用者，均必須使用本公司要求之：

多因素驗證（Multi-Factor Authentication, MFA）。

本政策適用於所有帳號類型，包括但不限於：

- 客戶帳號；
- 會員帳號；
- 顧問帳號；
- 合作夥伴帳號；
- 員工帳號；
- 系統維運帳號；
- 系統管理員帳號；以及
- 其他具有非公開系統或資料存取權限之帳號。

使用帳號期間不得停用或略過 MFA；使用者仍可刪除自己的帳號。刪除後停止帳號存取並撤回所有行銷同意，必要歷史紀錄依隱私政策保留且不得用於行銷。

未完成 MFA 設定或未能通過 MFA 驗證者，不得存取需要登入或身分驗證之網站功能。

本公司得依資訊安全風險要求使用者重新驗證身分、重新設定 MFA、增加其他驗證方式，或暫時限制帳號存取。

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。

二、MFA 不代表絕對安全保證

MFA 可以大幅降低單一密碼遭竊後造成未經授權登入之風險，但任何身分驗證技術均無法完全消除所有資訊安全風險。

即使已使用 MFA，仍可能發生包括但不限於：

- 網路釣魚（Phishing）；
- 社交工程（Social Engineering）；
- Session Hijacking；
- Cookie 或 Token 竊取；
- 惡意程式；
- 使用者裝置遭入侵；
- SIM Swap；
- MFA Fatigue Attack；
- 第三方身分驗證服務遭攻擊；
- 零時差漏洞（Zero-Day Vulnerability）；或
- 其他目前未知或不可合理預見之攻擊方式。

因此，MFA 應被理解為整體資訊安全架構之一部分，而非本公司對帳號或系統「絕對不會遭受入侵」之保證。

三、使用者亦負有帳號安全義務

使用者應合理保護其：

- 帳號；
- 密碼；
- MFA 驗證裝置；
- Passkey；
- Authenticator；
- Security Key；
- Recovery Code；
- 電子郵件帳號；
- 行動裝置；以及
- 其他身分驗證資訊。

使用者不得：

- 與他人共用帳號；
- 將密碼提供予第三人；

- 將 MFA 驗證碼提供予第三人；
- 將 Recovery Code 提供予第三人；
- 故意規避、破解或停用本公司要求之安全措施；或
- 允許未經授權之人員使用其帳號。

如使用者發現或合理懷疑帳號、密碼、驗證裝置或 MFA 資訊遭竊、遺失、洩漏或未經授權使用，應立即通知本公司並採取必要安全措施。

四、因使用者未遵守安全要求所造成之損害

如資訊安全事件係因使用者：

- 分享帳號；
- 洩漏密碼；
- 洩漏 MFA 驗證資訊；
- 未妥善保管驗證裝置；
- 未依要求完成 MFA；
- 故意規避資訊安全措施；
- 使用已遭入侵之設備；
- 未合理處理本公司提供之安全警告；或
- 其他可歸責於使用者之行為

所造成，且該事件並非可歸責於本公司者，本公司在適用法律允許之最大範圍內，不對因此產生之損害負責。

五、本公司採取合理資安措施

本公司依實際風險及系統需求，得採取包括但不限於下列資訊安全措施：

- Multi-Factor Authentication；
- Role-Based Access Control；
- Least-Privilege Access；
- 帳號與權限管理；
- 傳輸及必要資料加密；
- 系統與軟體更新；
- Security Patch Management；
- Vulnerability Management；
- 網路及應用程式安全防護；
- Backup & Recovery；
- Security Logging；

- Access Logging；
- 異常登入偵測；
- Incident Response；
- 第三方服務及供應商安全管理；以及
- 其他與風險相稱之資訊安全措施。

實際採用之安全措施得依威脅環境、技術發展、法令要求及系統架構持續調整。

六、建立及保存可稽核之資訊安全證據

本公司於合理且適法之範圍內建立、保存及管理必要之資訊安全紀錄，以支持：

- 資訊安全管理；
- 風險評估；
- 法令遵循；
- 異常事件分析；
- 資安事件調查；
- 系統復原；
- 稽核；
- 責任釐清；以及
- 持續改善。

相關紀錄得包括：

Risk Assessment → Security Controls → Authentication Logs → MFA Logs → Access Logs → Patch Logs → Backup Logs → Vulnerability Records → Vendor Reviews → Incident Records → Corrective Actions

前述紀錄之保存不表示本公司承諾保存所有系統活動之永久或百分之百完整紀錄。

本公司將依資料性質、法令要求、安全需要及合理保存期間進行管理。

七、第三方駭客及不可合理控制之資安事件

即使本公司已採取合理及適當之安全措施，仍可能遭遇超出本公司合理控制範圍之資訊安全事件，包括：

- 未經授權之第三方駭客攻擊；
- Zero-Day Vulnerability；
- Malware；
- Ransomware；
- DDoS；

- Supply Chain Attack；
- DNS Attack；
- Credential Stuffing；
- 第三方雲端服務事故；
- 電信或網路基礎設施事故；
- 第三方軟體或開源元件漏洞；或
- 其他不可合理預見或不可合理避免之網路安全事件。

本公司不聲明、不承諾亦不保證本網站或相關資訊系統：

- 永遠不會遭受網路攻擊；
- 永遠不存在資訊安全漏洞；
- 永遠不會發生未經授權存取；
- 永遠不會發生資料外洩、竄改、毀損或滅失；
- 永遠不中斷；或
- 可以完全排除目前或未來所有資訊安全威脅。

八、第三方服務

本網站可能使用由獨立第三方所提供之：

- 雲端服務；
- DNS；
- CDN；
- 電子郵件服務；
- 身分驗證服務；
- 金流服務；
- 電子發票服務；
- 網路基礎設施；
- 軟體；
- API；或
- 其他外部資訊服務。

本公司將於合理範圍內進行第三方服務之選擇、管理及安全風險評估，但本公司無法直接控制第三方之全部資訊系統、人員、內部管理程序及網路環境。

如事件係由獨立第三方所造成，且本公司已合理履行依法應負之選任、監督、安全管理或其他義務，本公司僅於適用法律要求之範圍內負擔責任。

九、資訊安全事件不當然代表本公司具有過失

資訊安全事件、駭客入侵、資料外洩或服務中斷之發生，本身並不當然表示本公司未採取合理資訊安全措施或具有故意、過失。

實際責任應依個別事件之：

- 發生原因；
- 可預見程度；
- 當時可合理取得之技術；
- 本公司已採取之安全措施；
- 使用者行為；
- 第三方行為；
- 因果關係；
- 損害範圍；以及
- 適用法律

個別判斷。

十、責任限制

在適用法律允許之最大範圍內，如本公司已採取與當時合理風險相稱之資訊安全措施，而相關事件並非因本公司故意、重大過失或其他依法不得限制責任之事由造成，本公司對於不可合理預見、不可合理防止或超出本公司合理控制範圍之第三方網路攻擊或其他資訊安全事件，僅於法律規定之範圍內負擔責任。

在法律允許之最大範圍內，本公司不對非因本公司依法應負責任之事由所造成之下列損失負責：

- 間接損害；
- 附帶損害；
- 特別損害；
- 衍生性損害；
- 所失利益；
- 商業機會損失；
- 營業中斷；
- 商譽損失；或
- 其他間接經濟損失。

十一、依法不得排除之責任不受影響

本聲明任何內容均不得解釋為排除或限制依法不得預先排除或限制之責任。

包括但不限於：

- 因本公司故意所生之責任；
- 因本公司重大過失所生之責任；
- 法律強制規定不得限制之個人資料保護責任；
- 消費者依法享有且不得以定型化契約排除之權利；以及
- 其他依法不得預先免除或限制之責任。

如本聲明之任何部分經依法認定為無效、不可執行或不得適用，其餘部分仍於法律允許之最大範圍內繼續有效。

十二、網站使用者之同意

建立帳號、登入或繼續使用需要身分驗證之本網站服務，即表示使用者了解：

資訊安全是一項由網站營運者、使用者及相關服務提供者共同參與之持續性風險管理工作，而不存在能夠完全消除所有網路安全風險之資訊系統。

使用者並同意遵守本網站之強制 MFA、帳號安全及其他資訊安全要求。

不同意遵守強制 MFA 或其他必要安全措施者，將無法使用需要登入或身分驗證之相關服務。

會員文件的簽署以網站文件簽署頁的明確提交及成功保存紀錄為準；本段不將單純瀏覽或登入視為已完成首次文件簽署。

十三、適用法律

本聲明之解釋及適用，以中華民國（台灣）法律及其他依法應適用之強制規定為準。

本聲明所定之免責、責任限制及風險分配，均僅於適用法律允許之最大範圍內有效。

因本聲明所生或與本聲明有關之爭議，雙方同意以臺灣臺北地方法院為第一審管轄法院。但法律另有專屬管轄或其他不得以合意排除之管轄規定者，從其規定。

English

Maxwell Venture Service LLC (the “Company”) values the security of its websites, information systems, accounts and user data.

Our core principles are: Reasonable Security Measures + Auditable Security Evidence + Precise Limitation of Liability.

We adopt reasonable, appropriate and risk-proportionate technical and organizational measures, taking into account the nature of the services, system architecture, the nature and sensitivity of data, reasonably foreseeable risks, and applicable laws and regulations.

No internet-connected website, information system, cloud service, software, third-party platform or communications system can be guaranteed completely secure. Security measures seek to reasonably reduce the likelihood and impact of incidents; they do not guarantee freedom from attacks, intrusion, exploitation, data breaches or interruption.

1. Mandatory MFA for every website account

Anyone who creates, holds or uses a website account to access authenticated features, services, data or administration interfaces must use the multi-factor authentication (MFA) required by the Company.

This applies to all account types, including:

- Customers;
- Members;
- Advisors;
- Partners;
- Employees;
- System operations personnel;
- System administrators; and
- Any other accounts with access to non-public systems or data.

MFA cannot be disabled or bypassed while using an account. Users may still delete their own accounts. Deletion ends account access and withdraws all marketing consent; necessary history is retained under the privacy policy and must not be used for marketing.

Users who have not enrolled in MFA or cannot pass verification may not access authenticated website features. Depending on security risks, we may require renewed identity verification, MFA re-enrollment, additional verification methods or temporary access restrictions.

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.

2. MFA is not an absolute security guarantee

MFA can substantially reduce unauthorized sign-in risk following theft of a password, but no authentication technology removes every security risk.

Risks may still include:

- Phishing;
- Social engineering;
- Session hijacking;
- Cookie or token theft;
- Malware;
- Compromised user devices;
- SIM swaps;
- MFA fatigue attacks;

- Attacks on third-party identity providers;
- Zero-day vulnerabilities; and
- Attacks that are currently unknown or not reasonably foreseeable.

MFA is part of the overall security architecture, not a guarantee that an account or system can never be compromised.

3. Users also have account-security responsibilities

Users must reasonably protect their:

- Accounts;
- Passwords;
- MFA devices;
- Passkeys;
- Authenticators;
- Security keys;
- Recovery codes;
- Email accounts;
- Mobile devices; and
- Other authentication information.

Users must not share accounts, passwords, MFA codes or recovery codes with others; deliberately circumvent, break or disable required safeguards; or allow unauthorized people to use their accounts.

If theft, loss, disclosure or unauthorized use is discovered or reasonably suspected, users must notify the Company immediately and take necessary protective measures.

4. Harm caused by a user’ s failure to follow security requirements

If an incident results from a user’ s account sharing, password or MFA disclosure, inadequate device protection, failure to complete required MFA, deliberate circumvention of safeguards, use of compromised equipment, unreasonable disregard of security warnings, or other conduct attributable to the user—and is not attributable to the Company—the Company is not liable for the resulting harm to the maximum extent permitted by applicable law.

5. Reasonable security measures

Depending on actual risks and system needs, measures may include:

- Multi-factor authentication;
- Role-based access control;
- Least-privilege access;
- Account and permission management;
- Encryption in transit and of data where needed;
- System and software updates;
- Security patch management;
- Vulnerability management;
- Network and application safeguards;
- Backup and recovery;
- Security logging;
- Access logging;
- Detection of unusual sign-ins;
- Incident response;
- Third-party service and vendor security management; and
- Other risk-proportionate safeguards.

The measures actually used may evolve with threats, technology, legal requirements and system architecture.

6. Creating and retaining auditable security evidence

Within reasonable and lawful limits, the Company creates, retains and manages necessary security records to support security management, risk assessment, compliance, anomaly analysis, incident investigation, recovery, audits, allocation of responsibility and continuous improvement.

Records may include:

Risk Assessment → Security Controls → Authentication Logs → MFA Logs → Access Logs → Patch Logs → Backup Logs → Vulnerability Records → Vendor Reviews → Incident Records → Corrective Actions

This does not constitute a commitment to permanent or completely exhaustive recording of all activity. Retention is managed according to the nature of the data, legal requirements, security needs and reasonable retention periods.

7. Third-party attacks and events beyond reasonable control

Even with reasonable and appropriate safeguards, incidents beyond our reasonable control may include:

- Unauthorized third-party attacks;
- Zero-day vulnerabilities;
- Malware;
- Ransomware;
- DDoS attacks;
- Supply-chain attacks;
- DNS attacks;
- Credential stuffing;
- Third-party cloud incidents;
- Telecommunications or network infrastructure incidents;
- Vulnerabilities in third-party software or open-source components; and
- Other events not reasonably foreseeable or avoidable.

We do not represent, promise or guarantee that our websites or systems will never be attacked, contain vulnerabilities, experience unauthorized access, suffer data disclosure, alteration, damage or loss, be interrupted, or be able to exclude all present and future threats.

8. Third-party services

The website may use independent providers of cloud services, DNS, CDN, email, identity authentication, payments, electronic invoices, network infrastructure, software, APIs or other external information services.

We undertake reasonable service selection, management and security-risk assessment, but cannot directly control every third party' s systems, personnel, internal procedures or network environment.

Where an independent third party causes an incident and we have reasonably fulfilled applicable duties of selection, supervision, security management and other legal obligations, we bear liability only to the extent required by applicable law.

9. An incident does not by itself establish Company fault

A security incident, intrusion, data breach or interruption does not by itself establish that the Company failed to take reasonable safeguards or acted intentionally or negligently.

Liability must be assessed case by case, considering causes, foreseeability, reasonably available technology at the time, safeguards adopted, user conduct, third-party conduct, causation, the extent of loss and applicable law.

10. Limitation of liability

To the maximum extent permitted by applicable law, where we have adopted safeguards proportionate to reasonably assessed risks at the time and an event is not caused by our intentional misconduct, gross negligence or another ground on which liability cannot lawfully be limited, our liability for third-party attacks or other incidents that are not reasonably foreseeable or preventable, or are beyond our reasonable control, is limited to what the law requires.

To the maximum extent permitted by law, we are not liable for the following losses where they do not arise from grounds for which we are legally responsible:

- Indirect damages;
- Incidental damages;
- Special damages;
- Consequential damages;
- Lost profits;
- Lost business opportunities;
- Business interruption;
- Loss of goodwill; or
- Other indirect economic losses.

11. Non-excludable liability remains unaffected

Nothing in this notice excludes or limits liability that cannot lawfully be excluded or limited in advance, including liability for intentional misconduct or gross negligence, mandatory personal-data protection obligations, consumer rights that cannot be excluded by standard terms, and other non-excludable duties.

If any part is found invalid, unenforceable or inapplicable, the remainder continues to operate to the maximum extent permitted by law.

12. User acknowledgment and agreement

By creating an account, signing in or continuing to use authenticated services, users acknowledge that security is an ongoing risk-management effort shared by operators, users and relevant service providers, and that no information system eliminates all cybersecurity risks.

Users agree to comply with mandatory MFA, account-security and other security requirements. Those who do not agree to mandatory MFA or other necessary safeguards cannot use authenticated services.

Member document assent requires explicit submission and a successfully saved record through the agreement page. Browsing or signing in alone does not complete first-use document signing.

13. Applicable law

This notice is interpreted and applied under the laws of the Republic of China (Taiwan) and any other mandatorily applicable provisions.

Its disclaimers, limitations of liability and risk allocations operate only to the maximum extent permitted by applicable law.

For disputes arising out of or relating to this notice, the parties agree that the Taiwan Taipei District Court shall be the court of first instance. This agreement does not override exclusive jurisdiction or other mandatory jurisdiction rules that cannot be excluded by agreement.