# 技術政策隱私權

## 1. 目的和適用範圍

本政策的目的是定義隱私權條件，ConstructSecure 依據此隱私權條件經營其一般網站，以及使用、處理和儲存向登入並使用 ConstructSecure 供應商資格預審應用程式之註冊客戶所收集的資料。

本政策的適用範圍為公開的 ConstructSecure 網站 (www.constructsecure.com) 和所有 ConstructSecure 網絡和 IT 系統，以及由註冊客戶使用 CS 系統時所提供的所有最終使用者資料。最終使用者資料包括但不限於姓名、公司電子郵件和公司電話號碼。CS Inspect 模組的使用者也可以選擇提供公司行動電話號碼，以接收關於調查結果的通知。這些私人最終使用者資料是註冊客戶進行互動和使用 CS 應用程式時所必要的資訊，供使用者建立安全的帳號並接收來自系統的訊息和通知。本政策在客戶帳號作用中的有效期間內具有完整的效力。

CS 隱私權政策旨在清楚且徹底地解釋我們對於 Cookie、資料收集、資料使用、資料處理、資料移轉、資料保留和刪除、個人資料洩露通知，以及如何聯繫 ConstructSecure 以管理或刪除您的資訊/帳號的政策。

## 2. 訪客與使用者

ConstructSecure 網站向一般大眾開放，網站的訪客不需要輸入任何個人資訊即可瀏覽網頁並了解我們的產品。但 ConstructSecure 會使用 Cookie 幫助提升訪客體驗，如下文章節 4 中詳述。第一次造訪 CS 網站的訪客會立即收到彈出式橫幅，告知他們我們使用 Cookie，且彈出式橫幅的內文以及網站的每個頁面底部均提供前往本政策的連結。

ConstructSecure 系統的使用者在本政策中的定義為註冊一或多項 CS 軟體的個人，這些軟體包括 CS Safety、CS Financial、CS Tracker，和/或 CS Inspect。本政策包含使用 CS 系統任何面向的所有客戶最終使用者，以及 ConstructSecure 員工。

CS 使用者可以設定為兩種類型其中之一來存取 CS 網頁應用程式 - 管理員或一般使用者。這兩種存取層級之間唯一的標準區別是，管理員使用者一開始是由 ConstructSecure 在系統中設置，並被賦予建立一般使用者的功能，以便在內部管

理員工清單，而這些員工將根據本身的特定業務需求來使用 CS 應用程式。當客戶的管理員新增一般使用者時，由管理員提供的唯一身份資料是一般使用者的姓名、公司電子郵件和電話號碼。客戶管理員建立一般使用者的個人檔案之後，CS 系統會傳送一封自動電子郵件給一般使用者，其中提供一個連結可前往開始正式建立唯一的使用者個人檔案。在這個設置的過程中，我們會使用 CAPTCHA (人機驗證，即全自動區分電腦和人類的公開圖靈測試)，這是一個問題 - 回應系統的測驗，設計用來區分人類和自動程式。CAPTCHA 可以區別人類和機器人，方式是要求完成一項大多數人類都可以輕鬆執行的任務，但現有的機器人技術不容易且需要較多的時間才能完成。此外，在設置過程中，所有使用者都必須根據一個嚴謹的密碼系統建立一個密碼，這一點在 CS 密碼政策中有詳細說明。

最終使用者帳號對每一位使用者來說都是唯一的，絕對不會共用。根據唯一的使用者名稱和密碼，一般使用者僅能夠存取自己輸入的特定資料。此外，最終使用者僅可根據其客戶合約協議中所定義，存取 CS 應用程式的特定模組 (如 CS Safety、CS Financial、CS Tracker、CS Inspect)。

## 3. 參考文件

與本政策相關的特定法規和架構包括但不限於：

- ISO/IEC 27001 標準。第 A.9.1.1、A.9.1.2、A.9.2.1 條：A.9.2.6、A.9.3.1、A.9.4.1、A.9.4.3。
- 一般資料保護規範 (GDPR)，2018 年 5 月 25 日
- 歐盟-美國及瑞士-美國隱私保護盾架構，美國商務部/歐盟執行委員會/瑞士政府
- 加州消費者隱私保護法 (CCPA)，1/1/2020
- 通用數據保護法 (LGPD)，2/1/2020

本 CS 隱私權政策和 CS 資訊安全政策是說明 ConstructSecure 對資訊安全之承諾的首要策略。CS 資訊政策旨在提供對於 ConstructSecure 資訊安全管理系統 (Information Security Management System，ISMS) 原則和做法的高層次理解。而 CS 資訊安全政策則提供關於資訊安全的一般做法，佐以十分具體的技術政策做為補充，這些技術政策定義了我們為確保資料的機密性和完整性所採取的措施，包括：

- CS 可接受的使用政策
- CS 存取控制政策
- CS 變更管理和安全工程/開發政策
- CS Clear Desk 和 Clear Screen 政策

- CS 資料備份政策
- CS 文件與資訊控制政策
- CS 加密政策
- CS 事件管理政策
- CS 內部和外部稽核政策
- CS 記錄和監控政策
- CS 密碼政策

此外還有幾份 CS 內部手冊，其中包含關於資訊安全的組織資訊，以及如何向員工和客戶傳達此類資訊，包括：

- CS 管理手冊
- CS 客戶/供應商參與和支援手冊
- CS 災難復原和業務連續性手冊
- CS ISMS 風險評估和風險處理方法
- CS ISMS 風險評估和風險處理報告
- CS 員工手冊
- CS 系統架構手冊

## 4. Cookie 政策

為了讓 ConstructSecure 網站正常運作，有時候會將一種稱 Cookie 的小型資料檔案放置在訪客或使用者的裝置中。這些 Cookies 以文字檔案的型式儲存在裝置上，以便稍後在瀏覽器中載入 CS 網站時，「記住」訪客或使用者的偏好 (例如語言、字體大小、登入資訊和其他顯示偏好設定)。這是一種常見的做法，絲毫不會影響 ConstructSecure 對於維護最高安全標準和保護客戶資訊的承諾。如同大多數的網站，ConstructSecure 使用 Cookie 來協助確保訪客和使用者享受穩定而高效的體驗，以及執行重要的功能，例如讓已註冊的使用者進行登記和保持登入。

ConstructSecure 也會使用 Cookie 來協助分析訪客和使用者與網站互動以及瀏覽網站的方式，幫助我們做出改進。Cookie 相關資訊也會用來記住與記錄註冊使用者的行為。Cookie 不會用於此處所述以外的任何目的。具體而言，ConstructSecure 網站不允許第三方追蹤機制以長時間和跨非聯盟網站的方式收集資料，用來根據興趣做廣告。此外，ConstructSecure 使用特殊的 HttpOnly 標誌來標記所有 Cookie，這個標誌指定僅能由哪些瀏覽器存取特定的 Cookie。這個 HttpOnly 標誌可以確保嚴格禁止攻擊者使用惡意的 JavaScript 存取 Cookie。訪客和使用者可以透過網路瀏覽器設定來封鎖任何網站的任何 Cookie。請注意，變更設定和 Cookies 的程序依瀏覽器而有所不同。如需更多關於在常見瀏覽器中停用 Cookie 的資訊，請參閱各別網站上的指示說明：

- Internet Explorer (http://support.microsoft.com/gp/cookies/en)
- Mozilla Firefox (http://support.mozilla.com/en-US/kb/Cookies)
- Google Chrome (http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95647)
- Safari (http://support.apple.com/kb/PH5042)
- Opera (http://www.opera.com/browser/tutorials/security/privacy/)

除了變更瀏覽器設定以防止 Cookie 置入，個人也可以刪除裝置上已儲存的所有 Cookie。若訪客或使用者選擇這種方式，則必須在每次造訪 ConstructSecure 網站時以手動的方式調整某些偏好設定，有些服務和功能可能無法正常運作。

第一次造訪 ConstructSecure 網站的訪客會立即收到彈出式橫幅，告知他們 ConstructSecure 使用 Cookie。

**5.** 資料收集在 ConstructSecure 應用程式中進行註冊時所收集、且歸類為個人資料或個人身份

資訊 (Personally Identifiable Information，PII) 的最終使用者資料，包括使用者全名、公司電子郵件和公司電話號碼。CS Inspect 模組的使用者也可以選擇提供公司行動電話號碼，以接收關於調查結果的通知。這些私人最終使用者資料是註冊客戶進

行互動和使用 CS 應用程式時所必要的資訊，供使用者建立安全的帳號並接收來自系統的訊息和通知。

## 6. 資料使用

ConstructSecure 的 ISMS 由我們的首席技術長進行內部管理，該首席技術長是 ISO 27001 中定義的首席資訊安全長 (CISO) 和 GDPR 第 37 條中定義的資料保護長。當客戶使用我們的服務和系統時，首席技術長為如何使用他們的資料以及如何保護使用者的隱私權界定了明確的規範，包括但不限於：

- 針對 CS 系統的使用者，ConstructSecure 完全依照「客戶軟體授權」和「服務協議」和/或「分包商參與協議」中所定義之目的進行資料處理，並且在所有的雲端計算中利用 Amazon Web Services，如下文章節 7 所述；
- 依合約協議及本文件規定所處理之個人資料，ConstructSecure 保證其機密性；
- ConstructSecure 不會和任何第三方共用資料，並且不使用任何第三方廣告提供者；
- ConstructSecure 確保其員工經過充份審查，並依 CS 管理手冊和 CS 員工手冊規定接受適當的個人資料保護訓練；
- ConstructSecure 員工確認知悉並簽署 CS 員工手冊中規定的保密要求；
- 所有資料移轉或下載均透過 SSL 協定；
- 若要存取資料，使用者必須依 CS 密碼政策中的詳細規定，以使用者名稱/密碼登入；
- 上傳資料時，檔案均依 CS 加密政策之詳細規定進行加密和儲存，包括每一個加密檔案都必須有本身的密碼；
- 儲存的備份和記錄均依 CS 資料備份政策中的詳細規定進行加密，包括 ConstructSecure 不得使用任何暫存；

## 7. 資料處理

如前所述，ConstructSecure 完全依照「客戶軟體授權」和「服務協議」和/或「分包商參與協議」中所定義之目的使用個人資料。此外，如 CS 管理手冊中詳述，ConstructSecure 和雲端科技領導者 Amazon Web Services 簽訂合約，建立 AWS 中一個邏輯上獨立的區域，在這個區域中，我們可以為自己的系統建立虛擬私有雲

(VPC)。雖然 AWS 不在 ConstructSecure 的 ISMS 範圍之內，選擇 AWS 的原因是他們在 ISO/IEC 27001:2013 有自己的認證。具體而言，AWS 在 2010 年 11 月 18 日獲頒證書 #2013-009，該證書在 2020 年 3 月 27 日更新並重新頒發。

此外，在我們和 AWS 的協議中，我們是其資料處理附錄 (DPA) 中的一方。這是我們對於資料安全和隱私權的承諾中極為重要的部分，因為 Amazon 的 DPA 徹底遵守並符合一般資料保護規範 (GDPR)、歐盟-美國和瑞士-美國隱私保護盾架構，以及加州消費者隱私保護法中的所有規定。列入 AWS 的 DPA 可以確保遵守重要的資料安全規範，包括但不限於：

- AWS 將僅依照客戶的指示處理客戶資料；
- AWS 已採取並將維持 AWS 網絡的強大技術和組織性措施；
- 在知悉發生安全性事件後，AWS 會立即將該安全事件通報給客戶，毫不遲延。

## 8. 資料移轉

ConstructSecure 不會和任何第三方共用資料或移轉資料給第三方，並且不使用任何第三方廣告提供者。

ConstructSecure 應用程式是以 SaaS 為基礎、網路託管的應用程式。如前面的章節所述，ConstructSecure 和 Amazon Web Services 簽訂合約，使用雲端服務。合約中載明，AWS 在美國和歐洲 (德國法蘭克福) 管理 ConstructSecure 的伺服器，以確保來自歐盟 (EU) 國家 (包括冰島、列支敦士登、挪威和瑞士) 的資料保存在歐盟國家。

AWS 遵守歐盟-美國隱私保護盾架構和瑞士-美國隱私保護盾架構，這兩個認證均歸類為「有效」，下一個認證期限為 2021 年 1 月 16 日。

## 9. 資料保留和刪除

ConstructSecure 僅在正當需求的存續期間、且在客戶或分包商協議的有效期間內保留所有最終使用者資料。帳號經 (客戶的管理員使用者或 ConstructSecure) 刪除或合約終止後，特定使用者帳號和個人身份資訊將立即刪除。ConstructSecure 盡力確

保我們的服務保護資訊不受意外或惡意刪除。因此，從使用者刪除內容、到從作用中和備份系統中刪除副本之間可能會有延遲。

如前所述，若要刪除特定使用者帳號，客戶的管理員使用者有權限刪除在 CS 系統中建立的帳號。此外，在客戶或分包商協議終止時，首席技術長將移除相關最終使用者帳號的存取權限，包括停用登入功能、將個人檔案從系統中移除，並確定存取權限已確實終止。

如「ConstructSecure 分包商參與協議」中所述，ConstructSecure 可將分包商所提交的資訊去識別化並統合，所有統合資訊歸 ConstructSecure 所擁有，可將該資訊用於任何目的並傳達給任何第三方，無需對分包商承擔任何義務。統合的資訊為匿名，不再是受資料保護法律和法規約束的個人資料。

## 10. GDPR 規定與隱私保護盾聲明

採用符合 ISO 27001 的資訊安全管理系統 (ISMS) 不僅是最佳做法，也是向客戶、分包商和第三方展現資料保護合規時不可或缺的條件。此外，藉由採用 ISO 27001，ConstructSecure 也建立起一個強有力的框架，確保遵守 2018 年 5 月 25 日起生效的歐盟一般資料保護規範 (GDPR)。

為確保遵守 GDPR 合規，ConstructSecure 遵守美國商務部所制定的歐盟-美國隱私保護盾架構和瑞士-美國隱私保護盾架構中，關於收集、使用和保留從歐盟和瑞士移轉到美國之個人資料的規範。

ConstructSecure 已通過美國商務部認證符合隱私保護盾原則。若 CS 隱私權政策中的條款和隱私保護盾原則之間發生衝突，以隱私保護盾原則為準。若要深入了解隱私保護盾計畫以及查看我們的認證，請前往：https://www.privacyshield.gov/。

根據隱私保護盾架構和原則，ConstructSecure 保證下列事項：

- ConstructSecure 的自我認證受聯邦貿易委員會的調查和執行權力約束；
- ConstructSecure 如前述章節 5 中的內容收集有限的個人資料，並僅依照前述章節 6 中所述之目的使用該項資訊；

- ConstructSecure 應用程式的個別使用者有權存取其個人資料，並檢閱、更正、修改、刪除或限制使用和/或揭露其個人資料。如同所有使用者，歐盟和瑞士的使用者可以隨時利用唯一的使用者名稱和密碼安全地登入 CS 系統，存取和檢閱其個人資料。若 ConstructSecure 應用程式的使用者想要修改、刪除或限制使用和 / 或揭露其個人資料，請傳送電子郵件聯繫 ConstructSecure：support@constructsecure.com，如章節 13 中的詳細說明；
- ConstructSecure 不會和任何第三方共用資料或移轉資料給第三方，並且不使用任何第三方廣告提供者。但是，ConstructSecure 也認知，當任何實體和第三方共用資料或移轉資料給第三方，若第三方處理個人資料的方式違反原則，則該實體 (包括 ConstructSecure) 仍將承擔責任；
- 根據我們的法律義務和依法請求的情況下，ConstructSecure 可將個人資料移轉給政府當局，用以執法或國家安全目的；
- ConstructSecure 鼓勵歐盟和瑞士的使用者以及所有使用者，若對於我們在隱私權保護盾之下處理其個人資料有疑問或申訴，請使用第 13 節所述的方式與我們聯繫。ConstructSecure 將盡快解決您的問題，不超過收到問題或申訴後的 30 天內；
- 如果您有未解決的隱私權或資料使用方面的申訴，而我們解決申訴的方式未能令您滿意，請聯繫 (免付費) 我們位於美國的第三方爭議處理機構，美國仲裁協會：https://www.adr.org/TechnologyServices；
- 若您是歐盟或瑞士的使用者且無法透過上述任何方式解決申訴，可以根據隱私保護盾架構援引具有約束力的仲裁，請前往：https://www.privacyshield.gov/article?id=How- 提交線上申訴。

## 11. 加利福尼亞和巴西的要求

ConstructSecure 同時也遵守於 2020 年 1 月 1 日起生效的加州消費者隱私保護法 (CCPA) 以及達勒斯（Les Geral deProtecãode Dados）（LGPD）將於 20/1/20 在巴西生效。若加州消費者隱私保護法 (CCPA) 或 LGPD 適用於使用者的資訊，本政策的章節 13 詳述使用者可利用的程序，以行使收到 ConstructSecure 資料措施相關資訊和/或要求刪除其資訊/帳號的權利。

ConstructSecure 絕不會共用、銷售或移轉使用者的個人資料。ConstructSecure 僅依照「客戶軟體授權」和「服務協議」、「分包商參與協議」以及本政策中所定義之商業目的使用和處理個人資料。

## 12. 隱私權政策變更或個人資料洩露通知

ConstructSecure 保留隨時修訂 CS 隱私權政策的權利。若本隱私權聲明有重大變更，ConstructSecure 將在 ConstructSecure 部落格中發佈關於該變更的通知，部落格可從我們的網站 www.constructsecure.com 上的連結前往。除此之外，本政策的最新版本將會立即重新發佈在 ConstructSecure 網站上，可透過 ConstructSecure 每一個頁面底部的「隱私權政策」連結直接存取。

此外，若發生任何個人資料洩露，ConstructSecure 將立即透過電子郵件通知客戶 (絕不超過知悉事件後的 72 小時)。該通知將包含所有必要的文件記錄，供客戶在需要時將該洩露事件通報責任主管機關，包括：

- 洩露事件的性質和描述，包括受影響的使用者數量；
- 故障分析與根本原因；
- 處理該洩露事件及緩解負面影響的立即修正行動；以及
- 提議或已採取的修正行動，以杜絕相同性質和類型的洩露事件再次發生。

## 13. 聯繫 ConstructSecure

ConstructSecure 的所在地址是 450 Bedford Street, Suite 2200, Lexington, Massachusetts, 02420。

若使用者對於 ConstructSecure 的資料措施有任何疑問或申訴，或是想要提出刪除資訊/帳號的要求，請使用上述地址聯繫首席技術長或合規副總裁，或傳送電子郵件到 support@constructsecure.com，或致電 866-817-2210。從我們的公開網站上也可以直接連結到 ConstructSecure 的電子郵件地址，使用者登入 ConstructSecure 系統後也可使用該電子郵件地址。

回應書面申訴時，ConstructSecure 會聯繫申訴人並根據 ConstructSecure 客戶或分包商協議中所列的服務層級協議 (Service Level Agreement，SLA)，直接而迅速地解決問題。除此之外，為遵守歐盟-美國和瑞士-美國隱私保護盾架構原則以及如章節

10 中所述，ConstructSecure 將視需要與合適的獨立資源機構合作，包括但不限於美國商務部、美國聯邦貿易委員會、歐盟資料保護主管機關 (Data Protection Authorities，DPA) 和瑞士聯邦資料防護與資訊委員會 (Swiss Federal Data Protection and Information Commissioner，FDPIC)，共同處理申訴直至使用者滿意，且使用者無需負擔任何費用。

**14.** 政策合規 a. 合規條件

評估本文件的有效性和適用性時，必須考慮下列條件：

- 系統發生違規的次數。
- 帳號遭刪除的數量。
- 要求提供資料安全資訊的次數和解決時間。
- 資料安全申訴的次數和解決時間。

b. 合規評量

上述各點具體的合規條件包含在 ConstructSecure 建立的 ISMS 綜合性合規評量表中，並在 CS 資訊安全政策附錄 1 中提供。首席技術長將在每個季度利用 ISMS 綜合性合規評量表進行審查，確認是否遵守整體資訊安全政策，以及所有其他技術政策。季度審查的結果將會被追蹤、分析，並包含在年度 ISMS 管理回顧會議的討論之中。

除了正式的季度審查外，也會透過各種方式持續不斷地評量合規性，包括但不限於定期演練、業務工具報告以及向政策負責人提出的意見回饋。

ConstructSecure 的整體員工訓練計畫中包含關於本政策的訓練和意識提升，如 CS 員工手冊中詳述。

c. 例外情形

本政策的任何例外情形都應事先經過政策擁有者的批准。

d. 未達到合規

蓄意違反本政策的員工一經發覺可能遭受紀律處分，最重可終止僱用。

**15.** 審查與文件開發

本政策的作者被視為文件的擁有者，且當職責所需必須進行任何變更時，負責更新本文件。此外，首席技術長將對本政策進行年度審閱，確保在任何法律、組織政策和/或合約義務的相關變更之下，該政策仍然維持適用。

如 CS 管理手冊規定，ISMS 文件的所有變更均須使用追蹤修訂的功能進行，僅以紅色文字或~~刪除線~~標示針對舊版所做的修訂。此外，ISMS 文件的所有舊版都儲存在 CS 合規副總裁的個人使用者硬碟中，以留做參考。本文件的版本修訂歷程如下表所示：

| 版本歷程 | 日期 | 作者 | 批准者 | 內容分類 |
|---|---|---|---|---|
| 版本 5 | 6/8/20<br>(隱私權保護) | S. Kirilenko | D. Milinazzo, K. Sardone | 機密 |
| 版本 4 | 1/13/20 (加入 CCPA) | S. Kirilenko | D. Milinazzo, K. Sardone | 機密 |
| 版本 3 | 5/15/19 | S. Kirilenko | D. Milinazzo, K. Sardone | 機密 |
| 版本 2 | 5/15/18<br>(Cookie 政策) | S. Kirilenko | D. Milinazzo, K. Sardone | 機密 |
| 版本 1 | 5/15/17 | S. Kirilenko | D. Milinazzo, K. Sardone | 機密 |
| 本政策將由首席技術長進行年度審閱。 | | | | |