開始使用 NIST 隱私框架：

中小企業快速指南

“建立隱私計劃很困難……NIST 隱私框架一直是我們能夠使用的一個工具，即使我們無法配備龐大的隱私團隊也無妨。”

——阿靈頓縣政府首席數據官 Jaime Lees

何為 NIST 隱私框架？我的組織要如何使用？

NIST 隱私框架 是一種自願性工具，可以幫助您的組織創建或改善隱私計劃。有效的隱私風險管理可助您建立對產品和服務的信任，更好地傳達您的隱私實踐，履行您的合規義務。良好的網絡安全很重要，卻並不能解決所有隱私風險。

按照一個的簡單模型——「準備、設定、開始」階段——開始使用隱私框架，讓您的企業或機構在五個隱私風險管理領域保持一致：識別、治理、控制、溝通和保護。

準備……

準備使用隱私框架來創建或改進您的隱私計劃，為識別和管理隱私風險奠定堅實的基礎。

識別：

- 識別出您正在處理（例如收集、使用、共享、存儲）的數據並在整個數據生命周期（從收集到銷毀）中規劃數據在您的系統中的流動。這並不需要非常全面，尤其是在開始時，但它是了解您的隱私風險的基礎。
- 進行隱私風險評估 ，使用您的數據圖來評估您的數據處理活動如何給個人帶來問題（如尷尬、歧視或經濟損失）。然後，評估出現此等問題對您的組織所造成的影響（例如失去客戶信任或聲譽受損），這可能會對您的底線產生負面影響。
- 詢問合約方案以及您用於經營業務的產品和服務，確保其設定能夠反映您的隱私優先事項。

治理：

- 隱私文化從高層開始。確定您的組織關注哪些隱私價值（例如，人類自主權、匿名、尊嚴、透明度、數據控制）。將您組織的隱私價值和政策與您的隱私風險評估聯繫起來，從而培養對您的產品和服務的信任。
- 了解與隱私相關的法律義務，這樣您即可構建合規的產品和服務。
- 幫助您的員工了解其角色和職責，以便員工能夠就如何在產品和服務的設計和部署中有效管理隱私風險做出更好的決策。
- 定期重新評估，確認您的隱私風險是否發生了變化。當您改進產品和服務、更改數據處理、或獲悉新的法律義務時，可能會發生這種情況。

「隱私框架可以成為組織發展業務的市場差異化因素。」
——ESPERION Therapeutics 公司信息安全和隐私总监、資訊系統安全認證專家、欧盟信息隐私认证专家 Mary N. Chaney

設定……

現在您了解了您的隱私風險和法律義務並有了治理結構，您的組織可以專注在您的系統、產品和服務的政策和技術能力方面。

控制：

- 您是否收集、共享或保存了自己不需要的數據？請考慮您的政策如何幫助您或其他組織保持對數據的控制，以及個人如何發揮作用。
- 在決定數據處理系統、產品或服務的功能時，請考慮您的隱私風險和法律義務。考慮靈活的設計，讓您能夠更經濟有效地應對不斷變化的客戶隱私偏好和動態法律環境。
- 您進行哪些類型的數據處理？您越能讓數據與個人和設備相分離，隱私收益就越大。考慮各個技術措施（例如去識別化、分散數據處理或其他技術）如何幫助您在保護隱私的同時實現業務或機構目標。

溝通：

- 制定有關數據處理活動的內部和外部溝通政策。

- 提供清晰易懂的通知和報告或實施警報、提醒或其他信號，向個人告知您的數據處理活動及對方的選擇，從而提高透明度和客戶理解度。
- 您是否進行調查或安排焦點小組來指導您的產品或服務設計？將隱私納入其中，這會讓您了解更多有關客戶隱私偏好的信息。
- 考慮如果發生數據泄露您會怎麼做。您將如何發出通知或提供補救措施（例如信用監控或凍結）？

保護：

- 控制誰登錄您的網絡、使用您的計算機和其他設備。
- 使用安全軟件保護數據。
- 對靜態和傳輸中的敏感數據進行加密。
- 定期備份數據。
- 定期更新安全軟件，如果可能請設置自動更新。
- 制定用於安全銷毀數據和舊設備的正式政策。

「如果您需要建立隱私計劃，NIST 隱私框架是您完美的起點。」
——BakerHostetler 合伙人 Jeewon Serrato

開始！

現在是時候從出發，去實現目標了。

- 您的計劃與我們在此提出的建議相比如何？
- 確定目標結果的優先順序，制定行動計劃。
- 在組織內討論您的計劃，通過計劃來獲取實現您的目標所需的資源，建立相應的團隊。
- 把您的計劃付諸行動！您正在為您的產品和服務贏得更多信任，與您的合作夥伴和客戶就隱私問題進行更有效地溝通，履行您的合規義務！