

FOXIT ESIGN 安全性 概述



目錄

- 動態安全性和加密 3
- 可見度 5
- 稽核 5
- 資料中心 5
- 業務永續性/災難復原 6
- 資料保留原則 7



安全性是 Foxit eSign 的基本核心。如同我們所有的產品, Foxit eSign 的開發和設計始終將安全性放在第一位。

本文件概述了 Foxit eSign 用於保護您的文件和資料的安全性技術、原則和做法, 包括使您能夠進行安全性設定以滿足公司獨特的風險管理和合規性要求的資訊。

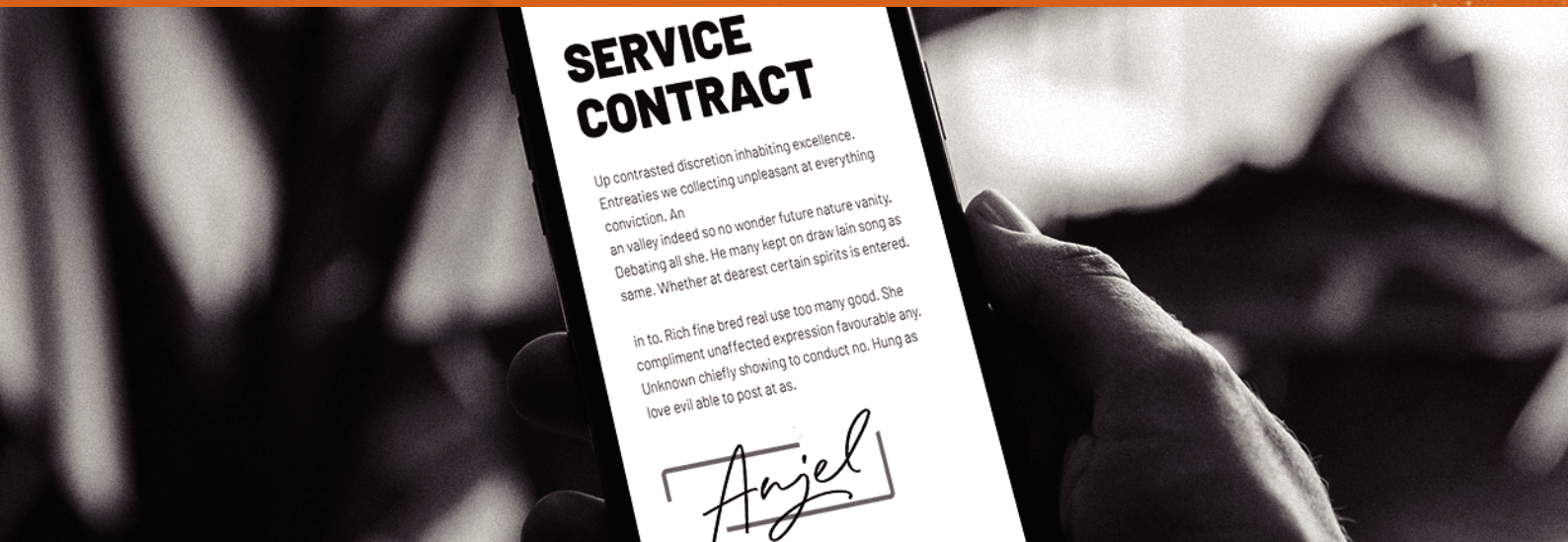
本文件也清楚指出 Foxit eSign 嚴格遵守的幾項地區法規, 以確保您能成功部署。

動態安全性和加密

Foxit eSign 已通過 SOC 2 Type 2 認證。獨立的產業稽核員會定期稽核這項認證, 以確保嚴格遵守 5 項信任服務原則。以下概述了 Foxit eSign 對使用者實體的服務承諾、規定其電子簽名和生產力管理服務的法律法規, 以及 Foxit eSign 為其服務制定的財務、營運和合規性要求。

安全性 - 保護您的資料免於未經授權的存取和透過我們的系統檢視

- Foxit eSign 承諾根據適用的產業慣例採取管理和技術措施, 從而保護系統並防止在每個訂單期限內, 其控制下的客戶資料不會發生意外遺失或未經授權存取、使用、竄改或披露。
- 在我們的系統和使用者的之間傳輸的所有資料都使用傳輸層安全性 (TLS) 和 HTTP 嚴格傳輸安全性 (HSTS) 進行保護。
- 存取包含客戶資料的環境時, 需通過一系列驗證和授權控制, 包括多因素驗證 (MFA)。



可用性 – 確保我們的軟體可根據需要並按照約定提供

- Foxit eSign 承諾將善盡商業上合理的努力，讓使用者在每個行事曆月份中至少有 99.95% 的時間可透過網際網路存取和使用該系統，不包括因定期維護而導致服務無法使用。然而，Foxit eSign 在過去 5 年內維持了超過 99.99% 的正常運作時間。

機密性 – 確保您的資料受保護並確保私密性和機密性

- Foxit eSign 承諾以相同於保護我們自己機密資訊的謹慎程度，保護機密資訊免於任何未經授權的使用或披露。在任何情況下，我們都不會使用低於合理標準的謹慎程度來保護此類機密資訊。
- 我們僅將機密資訊用於披露目的。

處理完整性 – 所有系統處理均按授權準確及時地完成

- Foxit eSign 的系統需求和做法包括應用程式開發介面 (API) 效能監控控制、資料攝入監控以及維護有助於預防、偵測和更正資料處理錯誤的原則和程序。

隱私權 – 嚴格遵守公認的隱私權原則 (GAPP)，該原則規定所有個人資料都按照我們隱私權聲明中的規定予以保留、收集、使用、披露和銷毀

- Foxit eSign 承諾以相同於保護我們自己個人識別資訊的謹慎程度，保護個人識別資訊免於任何未經授權的使用或披露。在任何情況下，我們都不會使用低於合理標準的謹慎程度來保護此類個人識別資訊。
- 我們僅將個人識別資訊用於披露目的。

此外，您的文件透過行業級 256 位元加密進行鎖定和保護，並配合嚴格的防火牆控制 – 所有進出流量都受到監控，並且強制遵守我們網路的嚴格安全性規則。Foxit eSign 透過對靜態和動態資料進行加密來提供端對端保護。



可見度

Foxit eSign 為客戶提供完整的可見度控制,以便您可以決定誰可以查看和存取您組織的文件。這包括以下控制:

- 自訂可見度功能,將文件檢視權僅限於您選擇的指定收件人。
- 使用「受保護欄位存取權」等功能限制帳戶使用者的可見度,僅允許獲得核准的使用者存取受保護欄位中的資訊。
- 透過指定不同的使用者層級和共用設定來控制對資訊的存取。
- 為一般使用者和管理員指派管理程式,確保輕鬆監控和使用下層文件。

稽核

準確瞭解文件所在位置,文件位置是安全性和合規性的重要組成部分。Foxit eSign 提供詳細的稽核報告和功能,因此客戶可以隨時瞭解他們的文件工作流程。

- 詳細的稽核追蹤按 IP 位址和時間戳記追蹤每個文件,因此您可以隨時全面瞭解文件的檢視位置、檢視時間和檢視者。
- 為每個文件提供完結證書,其中包含相關聯的 IP 位址、電子郵件地址、時間戳記和簽署者姓名。
- 追蹤文件和資料夾刪除流程的每一個步驟。透過刪除資料夾歷程記錄,您可以查看資料夾的刪除位置、刪除時間和刪除者。

資料中心

讓我們的客戶瞭解其文件的儲存位置非常重要。同時,我們也瞭解當地資料落地對於客戶的重要性。為此,Foxit eSign 將使用 Amazon Web Services (AWS) 資料中心。我們的資料中心旨在預測並容許故障,同時維持服務層級,並定期審查對資料中心的存取。

資料位置 – Foxit eSign 使用符合 SOC 2 Type 2 和 PCI 標準的 SSAE16 設施，維護深受信賴的美國和歐洲資料中心。在美國，應用程式託管在 AWS 平台上，並且主要在位於弗吉尼亞北部 (美國東部)、俄亥俄州 (美國東部) 和北加利福尼亞 (美國西部) 的設施中運作。在歐洲，資料中心位於德國法蘭克福。在加拿大，資料中心位於蒙特利爾。這些設施全年上鎖並監控，確保您的資料僅儲存在最安全可靠的伺服器上。

資料落地 – 註冊 Foxit eSign 帳戶時，您的帳戶將被指派到您當地的伺服器儲存區域。我們還可以讓客戶選擇他們想要將文件儲存到哪個資料中心。客戶最終能完全控制哪些人可以存取他們的文件。

業務永續性/災難復原

Foxit eSign 資料和檔案儲存在高可用性伺服器和託管資料庫中，並即時同步到報告和備份加密資料庫及檔案伺服器。在緊急情況下，系統可以從備份或其他可用性區域上線。

此外，Foxit eSign 保持著強大的系統容量和基礎架構監控以確保效能和可用性。備份會以幾近即時的方式執行，且大多是連續進行的過程。Foxit eSign 的業務永續性和災難復原計劃納入業務影響分析 (BIA)、事件處理、應變和業務永續性計劃，這些共同構成維持永續經營與緊急應變策略、管理和營運計劃的架構。Foxit eSign 設計了涵蓋雲端服務供應商 (CSP) 部分或完全故障的相關政策和程序。





資料保留原則

我們的資料保留原則概述了有關您資訊的追蹤和保留時長以及處理時間的重要指導方針。保留原則因帳戶類型而異。帳戶類型原則定義如下：

試用帳戶 – 非付費帳戶的文件和相關資料將在 30 天後刪除，除非使用者轉換為付費帳戶。

付費帳戶 – 付費帳戶的草稿文件將在系統中儲存 45 天，除非文件已傳送進行簽署。付費帳戶使用者還可以為每種類型的文件設定自己的文件保留原則，包括共用、部分簽名、已執行、取消和/或過期的文件。