Adobe Acrobat DC 搭配 Document Cloud 服務安全性總覽

目錄

1: 執行摘要
1: Acrobat DC 與 Document Cloud 服務總覽
1: Acrobat 文件安全性功能
1: 資產設定和分享限制
2: Microsoft 資訊保護 (MIP)
2: Document Cloud 服務架構
3: Document Cloud 服務安全性
3: Document Cloud 服務內容儲存空間
4: Amazon Web Services
4: AWS 和 Adobe 的營運責任
7: Adobe 風險與弱點管理
7: Adobe 安全性組織
7: Adobe 安全產品開發
7: Adobe 安全產品生命週期
8: Adobe 軟體安全性認證課程
8: Document Cloud 服務合規性
9: Adobe 員工
10: 總結

雖然 Adobe Sign 是 Document Cloud PDF 服務的一部分，但其安全性功能為獨立運作。

執行摘要

在 Adobe，我們非常重視您數位體驗的安全性。安全性做法已深植於我們的內部軟體開發、作業程序及工具。我們的跨部門團隊嚴格遵循這些做法，協助我們迅速預防、偵測及回應事件。透過與合作夥伴、傑出的研究人員、安全研究機構及其他產業組織合作，隨時掌握最新的威脅與弱點。同時定期在我們提供的產品和服務中納入進階安全性技術。

觸及客戶內容的 Adobe 服務已完成了多項產業認證。如需所有合規性認證與標準，以及 Adobe 產品和服務目前所支援政府法規的詳細清單，請參閱最新認證、標準及法規清單。如需 GDPR 的相關資訊，請參閱 GDPR 應對頁面。

本白皮書中說明 Adobe 實施的深度防禦及安全性程序，用以強化 Adobe Acrobat DC、Acrobat Reader DC、Document Cloud、Document Cloud 服務，以及相關資料的安全性。

Acrobat DC 與 Document Cloud 服務總覽

Adobe Acrobat DC 將最新的 Acrobat 桌面軟體與 Acrobat Reader 行動應用程式和 Adobe Document Cloud 線上服務的進階功能相結合，在確保所有裝置之間安全性的同時，協助各組織滿足用戶對任何裝置連線及生產力的需求。客戶使用 Adobe Acrobat DC 和 Document Cloud 服務就能將內容轉換成電子文件與他人分享，還能輕鬆產生、管理及轉換來自任何 Adobe 雲端服務、桌面應用程式或行動應用程式的 PDF 檔案。

Acrobat 文件安全性功能

密文

Adobe Acrobat DC 內含一組密文工具，可協助客戶保護敏感或機密資訊，包括在發布前永久刪除文件中的文字和圖像。此外，用戶還能根據模式（例如電話、信用卡號碼和電子郵件地址）搜尋和標記密文。標記密文的資訊會從檔案中完全移除，不像其他工具或方法只是遮蔽而已。客戶還可使用「文件淨化」功能來移除隱藏資訊和非圖形物件，例如可能顯示於 PDF 的中繼資料。

檔案分享

所有儲存在雲端的 Document Cloud 檔案都會自動加上「私人」標籤，表示只有上傳該內容的用戶能看到內容。用戶必須採取明確的操作來分享該內容，否則內容會保持私人狀態。所有 Document Cloud 的內容分享都是藉由電子郵件、簡訊或任何協作軟體將 Document Cloud 內容連結傳送給收件者的方式完成。

Document Cloud 服務的用戶可透過兩種選項分享檔案：「僅檢視」或「審核」。如果用戶傳送「僅檢視」限制的連結，收件者就只能以唯讀文件的情況下檢視內容。或者，若用戶傳送的文件為可審核狀態，則收件者可在文件上加上注釋，但不能以任何方式編輯或修改文件。

資產設定和分享限制

資產設定能讓組織控制員工在組織外部分享資產的方式。IT 管理員可選擇限制設定，藉此限制員工使用 Document Cloud 內的特定分享功能，包括限制只能對已宣告、受信任以及已列入安全清單的網域中的收件者採用邀請的方式分享。設定此規定後，用戶就無法與不在允許網域清單中的外部用戶分享組織擁有的資產。

Admin Console 中的資產設定

Microsoft 資訊保護 (MIP)

使用 Acrobat DC 或 Acrobat Reader DC 開啟受 Microsoft 資訊保護 (MIP) 解決方案 (包括 Azure 資訊保護 (AIP) 和使用 Microsoft Office 365 的資訊保護) 所保護檔案的客戶，請參閱此文件。

Acrobat Reader DC 中的保護模式

惡意程式碼會利用 PDF 格式來寫入或讀取電腦的檔案系統；為了協助保護客戶不受此威脅，Adobe 提供沙盒技術的實作，這項技術已在 Adobe Reader X 中採用，稱為「保護模式」。

沙盒是一項安全性方法，會建立受限制的執行環境，以便在其中利用低權限來執行程式。沙盒協助保護用戶的系統，不受包含可執行程式碼之未受信任文件傷害。在 Acrobat Reader DC 環境中，未受信任的內容可能是任何 PDF 檔案，以及它可能叫用的處理程序。Acrobat Reader DC 將所有 PDF 檔案都視為可能發生損毀，並將 PDF 檔案叫用的所有處理程序侷限於沙盒。

「Acrobat Reader DC 保護模式」能協助防禦嘗試在電腦系統上安裝惡意程式碼的駭客，同時支援組織防範惡意人士從其網路存取及擷取敏感性資料和智慧財產。當用戶啟動 Acrobat Reader DC 時，「保護模式」會預設為啟用，並且會限制授予程式的存取權等級，確保執行 Microsoft Windows 之系統的安全，以避免惡意的 PDF 檔案寫入或讀取電腦的檔案系統、刪除檔案或修改系統資訊。

Windows 8 和更新版本中的「保護模式」也可在 Windows AppContainer 中執行，藉此為啟用「保護模式」的客戶提供更加穩固的鎖定環境。

Acrobat DC 中的保護檢視

「保護檢視」類似 Acrobat Reader DC 的「保護模式」，是 Acrobat DC 豐富功能集的沙盒技術實作。在 Acrobat DC 中，Adobe 擴充了「保護模式」功能，不僅封鎖嘗試使用 PDF 檔案格式在電腦系統上執行惡意程式碼的寫入式攻擊，另外也會封鎖嘗試透過 PDF 檔案竊取敏感性資料或智慧財產的讀取式攻擊。

如同「保護模式」，「保護檢視」會將不受信任程式 (例如，任何 PDF 檔案和它所叫用的處理程序) 的執行侷限於沙盒，以避免使用 PDF 格式的惡意程式碼寫入或讀取電腦的檔案系統。「保護檢視」假設所有 PDF 檔案都是潛在惡意檔案，並將處理侷限於沙盒，除非用戶明確指出檔案受信任。

用戶在 Acrobat DC 獨立應用程式和在瀏覽器中開啟 PDF 文件的這兩種情況下都支援「保護檢視」。Windows 8 和更高版本中的「保護檢視」一律都在 AppContainer 中執行。如此可為啟用「保護檢視」的客戶提供更加穩固的鎖定環境。

當用戶在「保護檢視」中開啟不受信任的檔案時，Acrobat DC 會在檢視視窗頂端顯示訊息列。訊息列會指出檔案不受信任，並提醒用戶現正處於「保護檢視」，藉此停用許多 Acrobat DC 功能及限制檔案內的用戶互動。基本上，檔案為「唯讀」模式，而且「保護檢視」會防禦內嵌或標記 (tag-along) 內容竄改系統。

若要信任檔案及啟用所有 Acrobat DC 功能，用戶可以按一下訊息列中的「啟用所有功能」按鈕。此動作會結束「保護檢視」，並透過將檔案加入至 Acrobat 授權位置清單的方式，提供檔案的永久信任。後續每次開啟受信任的 PDF 檔案，都會停用「保護檢視」限制。

Document Cloud 服務架構

Adobe Document Cloud 服務包括：

- 整理 **PDF** — 插入、刪除、重新排序或旋轉 PDF 頁面
- 建立 **PDF** — 將 Word、Excel 和 PowerPoint 文件以及影像或照片轉換成 PDF 檔案
- 匯出 **PDF** — 輕鬆將 PDF 轉換成可編輯的 Microsoft Word、Excel、PowerPoint 或 RTF 檔案

- **編輯 PDF** — 輕鬆編輯來自行動裝置或筆記型電腦的現有 PDF
- **合併 PDF** — 將多個檔案合併成單一 PDF 檔案，並可隨處組合文件套件
- **傳送及追蹤** — 傳送、追蹤文件，並確認傳送狀態
- **Adobe Scan** — 擷取任何內容並轉換成可搜尋的高品質 PDF
- **Adobe Sign** — 在任何裝置上準備及傳送需要安全、受信任且具法律效力之電子簽名的文件

Document Cloud 服務安全性

權益和身分管理

IT 管理員利用 Adobe Admin Console 中的指名用戶授權，授與用戶存取 Adobe Document Cloud 服務的權益。Acrobat Document Cloud 支援三 (3) 種不同類型的用戶指名授權：

- **Adobe ID** — 適合個人用戶所建立、擁有及控制，並由 Adobe 代管的用戶管理帳戶。Adobe ID 帳戶只有在 IT 管理員啟用存取權的情況下，才能存取 Acrobat Document Cloud 服務。
- **Enterprise ID** — IT 管理員從客戶的企業組織建立及控制，並由 Adobe 代管的企業管理帳戶選項。組織擁有且能管理這些用戶帳戶及所有相關的資產。
- **Federated ID** — 企業管理的帳戶，其中所有身分設定檔是由客戶的單一登入 (SSO) 身分管理系統所提供，並且為客戶的 IT 基礎架構所建立、擁有及控制。Adobe 與大多數符合 SAML 2.0 的身分提供者整合。

倘若電子郵件地址位於公司網域內，大多數的企業組織會為其員工、承包商和自由工作者使用 Enterprise ID 或 Federated ID，如此一來就能讓組織同時控管代表該 ID 所儲存的權益和使用者產生的內容 (UGC)。如需各身分類型的詳細資訊，請參閱 Adobe 客戶支援網站。

Adobe ID 和 Enterprise ID 密碼儲存均運用 SHA-256 雜湊演算法結合密碼封存及大量的雜湊反覆運算。Adobe 會持續監控由 Adobe 代管的帳戶是否有異常或不當的帳戶活動，並評估這項資訊以協助迅速減輕對安全性的威脅。Adobe 不會管理 Federated ID 帳戶的用戶密碼。如需詳細資訊，請參閱 Adobe 身分管理服務安全性總覽。

電子簽名和數位簽名

Document Cloud 服務中有兩種不同的工具可供用戶選擇，以便安全地使用簽名：

- 填寫及簽署工具 — 由 Adobe Sign 提供支援，可讓用戶管理端對端簽署流程，其設計有助於遵循美國、歐盟及全球大多數工業化國家的電子簽名法律。用戶可使用此工具來向他人索取簽名、追蹤簽署流程，以及自動封存已簽署文件和稽核記錄。整個過程都採用安全性措施，而且文件與稽核記錄會經由 Adobe 認證並加上防竄改封印。

無法在行動裝置上進行追蹤。如需 Adobe Sign 及其安全性功能的詳細資訊，請參閱 Adobe Sign 技術總覽。

- 認證工具 — 可讓用戶使用 Adobe 認可的信任清單 (AATL) 或歐盟信任清單 (EUTL) 中所列的信任服務提供者核發的認證式數位簽名來簽署文件。使用受信任第三方認證授權機構 (CA) 所核發的認證 ID 來簽署，是公認對文件進行電子簽署的安全方法。此 ID 只會與簽署者本人連結，並且可以識別其身分。簽署者的認證會在簽署階段使用唯有該簽署者持有的私密金鑰，以密碼編譯方式繫結至文件。

  Acrobat DC 會自動與認證授權機構連線，以驗證簽署者的簽名，以及其簽署之文件的真實性。此類型的簽名符合 PDF 電子簽名標準，包括 PDF 進階電子簽名 (PAdES) 第 2、3 和 4 部分，以及美國國防部聯合互通測試司令部 (JITC) 使用密碼編譯及公開金鑰基礎結構 (PKI) (採 AES-256、RSA-4096、SHA-512 及 RSA-PSS 演算法) 的方式。此認證工具也可讓用戶在文件上加入時間戳記，並提供防竄改封印以資證明。

Document Cloud 服務內容儲存空間

雖然管理員透過 Adobe Admin Console 分配 Enterprise ID 和 Federated ID 帳戶的個人雲端儲存空間，但是無法直接存取用戶 Document Cloud 服務儲存空間中的任何檔案。若刪除含現有共享服務儲存空間的 Enterprise ID 或 Federated ID，會導致用戶無法存取雲端儲存空間內的任何資料，且該用戶的資料將在 90 天後遭到刪除。

管理員也可以使用 Admin Console 分配儲存空間給 Adobe ID 帳戶。雖然管理員無法刪除 Adobe ID 帳戶，但是可以撤銷授與的企業儲存空間額度，以及應用程式和服務存取權。與這些帳戶相關聯的資料將在 90 天後遭到刪除。

Adobe Document Cloud 服務使用多租用戶儲存空間。客戶內容經過 Amazon Elastic Compute Cloud (Amazon EC2) 實例處理後，會儲存在結合多個 Amazon Simple Storage Services (Amazon S3) 貯體的位置，並透過 MongoDB 實例儲存於 Amazon Elastic Block Store (Amazon EBS)。內容本身會儲存在 Amazon S3 貯體中，而有關內容的中繼資料則透過 MongoDB 儲存在 Amazon EBS 中 — 這些全都受到該 Amazon Web Services (AWS) 地區內身分識別與存取管理 (IAM) 角色的保護。

儲存在 Amazon EBS 的中繼資料和支援資產使用 AES 256 位元加密，該加密方法採用美國聯邦資訊處理標準 (FIPS) 140-2 核准的密碼編譯演算法，並遵循美國國家標準與技術局 (NIST) 800-57 的建議。

資料都是以備援方式儲存在多個資料中心和各個資料中心的多部裝置上。所有網路流量都會經過有系統的資料驗證與總和檢查碼計算，以避免發生損毀並確保完整性。最後，儲存的內容將會自動同步複寫到該客戶所在地區的其他資料中心設施，如此一來，即使兩個地點中有任何的資料遺失，仍能維持資料完整性。

如需基礎 Amazon 服務的詳細資訊，請參閱：

- MongoDB
- Amazon S3
- AWS Key Management Service (KMS)
- Amazon EC2 服務

專屬加密金鑰

Amazon S3 中所儲存內容和資產的預設加密方式為 AES 256 位元對稱安全性金鑰，每位客戶及每位客戶宣告的網域都擁有專屬的金鑰。如果管理員希望為其組織內的部分或所有網域增加一層額外控管與安全性，可以使用 AWS KMS 所管理的專屬加密金鑰，此金鑰每年自動更換一次。

管理員也可透過 Admin Console 撤銷此專屬加密金鑰，如此會導致用戶無法存取該金鑰加密的所有資料，藉此防止上傳和下載內容，直到再次啟用加密金鑰為止。

注意：雖然 Adobe Document Cloud 檔案可以使用專屬加密金鑰進行加密，但是中繼資料無法使用此金鑰加密。

如需管理使用專屬金鑰之加密的詳細資訊，請參閱下列 Adobe 說明頁面：

- 管理加密
- 專屬加密金鑰常見問答

Amazon Web Services

如前面所述，Adobe Document Cloud 服務的所有元件都託管於美國的 AWS 上，包括 Amazon EC2 和 Amazon S3。Amazon EC2 是一項 Web 服務，在雲端提供可自動擴充的運算容量，讓網路規模的運算更容易。Amazon S3 是公認高度可靠的資料儲存基礎架構，可用於儲存和擷取任何資料量。

AWS 平台會根據業界標準的做法提供服務，並且通過一般業界公認的認證與稽核。如需有關 AWS 和 Amazon 安全性控制項的詳細資訊，請前往 AWS 雲端安全性網站。

AWS 和 Adobe 的營運責任

AWS 負責操作、管理及控制各種元件，上至 Hypervisor 虛擬化層，下至 Adobe Document Cloud 服務運作所在設施的實體安全性。而 Adobe 則負責及管理客體作業系統 (包括更新和安全性修補程式) 和應用程式軟體，以及配置 AWS 提供的安全性群組防火牆。

AWS 也會操作 Adobe 使用的雲端基礎架構，以佈建各種不同的基本運算資源，包括處理和儲存。AWS 基礎架構包括設施、網路和硬體，以及支援佈建和使用這些資源的作業軟體 (例如，主機作業系統、虛擬化軟體等)。Amazon 是根據業界標準的做法及各種不同的安全性合規標準來設計及管理 AWS。

安全管理

Adobe 使用安全殼層 (SSH) 和安全通訊端層 (SSL) 做為管理 AWS 基礎架構的管理連線。

AWS 網路上客戶資料的地理位置

所有上傳到 Document Cloud 的 UGC 都儲存在 AWS 美國東部 (維吉尼亞州) 的地區資料中心。內容會在每座資料中心內以及地區內的其他資料中心進行備份，以達到負載平衡和備援的目的。

AWS 網路上身分資料的地理位置

身分資料儲存在多個地區負載平衡的 AWS 資料中心，位於維吉尼亞州 (美東)、奧勒岡州 (美西)、愛爾蘭 (西歐) 及新加坡 (亞太東南)。身分資料會複寫到所有資料中心。Adobe 遵循與跨界資料傳輸有關的適用法律，相關資訊詳述於 https://www.adobe.com/tw/privacy/eudatatransfers.html。

客戶資料分離 / 客戶隔離

AWS 使用強大的租用戶隔離安全性與控制功能。AWS 是一種虛擬化的多租用戶環境，除了實作安全性管理程序之外，還會實作其他專為隔離 AWS 客戶所設計的安全性控制。Adobe 使用 AWS 身分識別與存取管理 (IAM) 進一步限制對運算和儲存空間實例的存取權。

安全網路架構

AWS 採用網路裝置 (包括防火牆和其他邊界裝置) 來監視和控制網路外部邊界的通訊，以及網路內重要內部邊界的通訊。這些邊界裝置採用規則集、存取控制清單 (ACL) 及設定來強制執行前往特定資訊系統服務的資訊流程。每一個受管理的介面上都有 ACL (或流量流程政策)，用於管理和強制執行訊務流量。

Amazon Information Security 核准所有 ACL 政策，並使用 AWS ACL 管理工具自動將政策推送至每一個受管理介面，如此有助於確保這些受管理介面強制執行最新的 ACL。

網路監視和保護

AWS 使用各種自動化監視系統提供高水準的服務效能與可用性。監視工具有助於偵測異常或未經授權的活動，以及輸入和輸出通訊點的狀態。AWS 網路所提供的保護機制能有效抵禦傳統的網路安全性問題：

- 分散式阻斷服務 (DDoS) 攻擊
- 中間人 (MITM) 攻擊
- IP 詐騙
- 連接埠掃描
- 其他租用戶進行的封包探查

如需網路監視和保護的詳細資訊，請參閱 AWS 雲端安全性網站。

入侵偵測

Adobe 使用符合業界標準的入侵偵測系統 (IDS) 和入侵防禦系統 (IPS) 主動監視 Adobe Document Cloud 服務。

記錄

Adobe 會在伺服器端記錄 Adobe Document Cloud 服務客戶活動，藉此診斷服務中斷、特定客戶問題及回報的錯誤。記錄只會儲存 Adobe ID 以協助診斷特定客戶問題，不會包含用戶名稱 / 密碼組合。只有經授權的 Adobe 技術支援人員、主要工程師及特定幾位開發人員能夠存取記錄，用於診斷可能發生的特定問題。

服務監視

AWS 會監視電子、機械及生活支援系統與設備，以協助立即找出服務問題。為了維持設備持續運轉，AWS 會進行持續的預防性維護。

資料儲存與備份

Adobe 會將所有 Adobe Document Cloud 服務的資料儲存在 Amazon S3 中，以提供具高度耐用性的儲存基礎架構。為協助提供耐用性，Amazon S3 PUT 和 COPY 作業會同步將客戶資料儲存到多個設備上，並將物件儲存到 Amazon S3 地區內多個設備的多部裝置上做為備援。

Amazon S3 會計算所有網路流量的總和檢查碼，以便偵測在儲存或擷取資料時資料封包損毀的情形。Amazon S3 資料物件的資料複寫作業是在地區叢集內部進行，不會複寫到其他地區的資料中心叢集。

中繼資料會以拍攝 Amazon EBS 磁碟區的快照進行複寫，並以類似 Amazon S3 的方式儲存。如需 AWS 安全性的詳細資訊，請參閱 AWS 雲端安全性網站。

變更管理

AWS 會根據類似系統的業界標準，授權、記錄、測試、核准及記載現有 AWS 基礎架構中的例行、緊急和設定變更。Amazon 會以排程方式更新 AWS，以盡可能減少對客戶的影響。當會對服務的使用情形造成不良影響時，AWS 會透過電子郵件或 AWS Service Health Dashboard 與客戶溝通。Adobe 亦會針對 Adobe Document Cloud 維護 Adobe 系統狀態。

修補程式管理

AWS 會負責維護支援 AWS 服務傳遞的補丁系統，例如 Hypervisor 和網路服務。Adobe 則負責修補其在 AWS 中執行的客體作業系統 (OS)、軟體和應用程式。需要修補程式時，Adobe 會提供預先強化的全新作業系統和應用程式實例，而非實際的修補程式。

AWS 實體與環境控制

AWS 實體與環境控制已明確概述於 SOC Type 1 和 SOC Type 2 報告中。下一節將概述全球 AWS 資料中心採行的一些安全性措施與控制。如需有關 AWS 安全性的詳細資訊，請參閱 AWS 雲端安全性網站。

實體設備安全性

AWS 資料中心採用業界標準的架構與工程方法。AWS 資料中心位於外表毫不起眼的設施當中，且 Amazon 在周邊與建築物出入口設置了專業的保全人員、監視攝影機、IDS 及其他電子措施來實際管制進出。經授權的人員必須至少通過兩次雙重驗證才能進出資料中心樓層。所有訪客和承包商均須出示證件及簽名才能進入，且需有授權人員持續隨行。

AWS 僅對業務上確實需要進出資料中心的員工和承包商提供資料中心通行權限與資訊。當員工業務上不再需要該權限時，即使該人員仍為 Amazon 或 AWS 的員工，仍會立即撤銷其權限。AWS 員工所有進出資料中心的記錄都會予以保存，並進行例行稽核。

消防

AWS 在所有 AWS 資料中心安裝了火災自動偵測與消防設備。所有資料中心環境、機械與電子基礎架構空間、冷卻器機房及發電機設備機房中的火災偵測系統均使用煙霧偵測感應器。這些區域均配有消防管線、雙重互鎖預動式或氣體灑水系統作為保護。

受控環境

AWS 採用氣候控制系統以維持伺服器和其他硬體的恆溫作業環境，預防過熱及減少服務中斷的可能性。AWS 資料中心的大氣條件均維持在最佳水平。AWS 人員與系統會監控溫度與濕度，使資料中心維持在合適的狀態。

備用電力

AWS 資料中心的電力系統採可全天候完整備援及維護的設計，且維護時不會影響資料中心的運行。不斷電電源供應 (UPS) 裝置會在重要的必備負載設備發生電力故障時提供備用電力。資料中心使用發電機以提供整座設備的備用電力。

重大損毀復原

AWS 資料中心具備高度可用性，可承受小規模的系統或硬體故障影響。所有資料中心建置於全球不同地區的叢集內，保持全年無休 24 小時的連線狀態為客戶提供服務，也就是說，資料中心決不「停擺」。若發生故障，自動化程序能將客戶的資料移出受影響的區域。

核心應用程式部署於 N+1 組態中，這樣一來當某一座資料中心故障時，就有足夠的容量能將流量傳輸至其餘站點，以達到負載平衡。如需有關 AWS 重大損毀復原流程的詳細資訊，請參閱 AWS 雲端安全性網站。

Adobe 風險與弱點管理

Adobe 致力於確保風險與弱點管理、事件回應、防護及解決程序能靈活敏捷且精準。我們持續監視威脅趨勢，與世界各地的安全性專家共享知識，在事件發生時迅速解決，並且將這些資訊回饋給我們的開發團隊，以協助讓所有 Adobe 產品與服務達到最高層級的安全性。

深入測試

Adobe 認可領先的第三方資安公司並與其合作，共同進行深入測試以找出可能的安全性弱點，並提升 Adobe 產品與服務的整體安全性。收到第三方提供的報告後，Adobe 會記載這些弱點、評估嚴重性與優先順序，接著建立防護政策或補救計劃。Adobe 每年進行一次完整的深入測試，並於每月進行弱點掃描。

在內部，Adobe Document Cloud 安全性團隊於每季及每次發行前，都會進行所有 Document Cloud 元件和服務的風險評估。Document Cloud 安全性團隊會與技術營運和開發主導人員合作，協助確保每次發行前消除所有的高風險弱點。如需 Adobe 深入測試程序的詳細資訊，請參閱 Adobe 安全工程設計總覽。

事件回應與通知

隨著新弱點與威脅不斷進化，Adobe 也致力於回應和消除新發現的威脅。除了訂閱產業整體弱點公告清單 (包括 United States Computer Emergency Readiness Team (US-CERT)、Bugtraq 和 SANS) 之外，Adobe 還訂閱了由主要安全性廠商發佈的最新安全性警示清單。

如需 Adobe 事件回應與通知程序的詳細資訊，請參閱 Adobe 事件回應總覽。

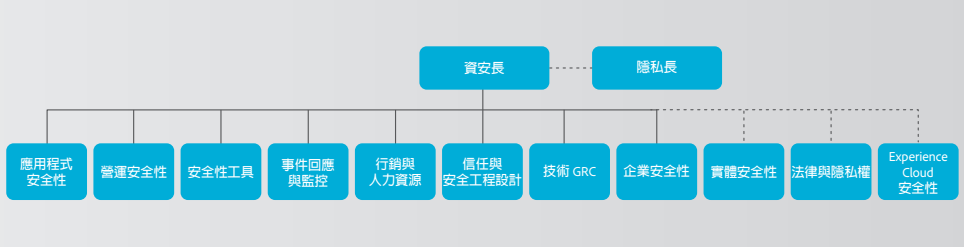
鑑識分析

Document Cloud 團隊遵循 Adobe 鑑識分析程序來進行事件調查，此程序當中包括對受影響的電腦進行完整影像擷取或記憶體傾印、安全保存證據，以及保管鏈錄影。

Adobe 安全性組織

Adobe 的資安長 (CSO) 負責協調所有安全工作，這是我們對產品和服務安全性的承諾。CSO 部門負責協調所有產品和服務的安全計劃，以及 Adobe 安全產品生命週期 (SPLC) 實作。

CSO 也管理 Adobe 安全軟體工程團隊 (ASSET)，此安全專家組成的中央專責團隊擔任關鍵 Adobe 產品和營運團隊的顧問，包括 Adobe Document Cloud 團隊在內。ASSET 研究人員與個別 Adobe 產品和營運團隊合作，致力於達成產品和服務所適用的安全性級別，並在安全性實務上指導這些團隊，以執行開發、部署、作業和事件回應的清楚與可重複流程。



Adobe 安全性組織

Adobe 安全產品開發

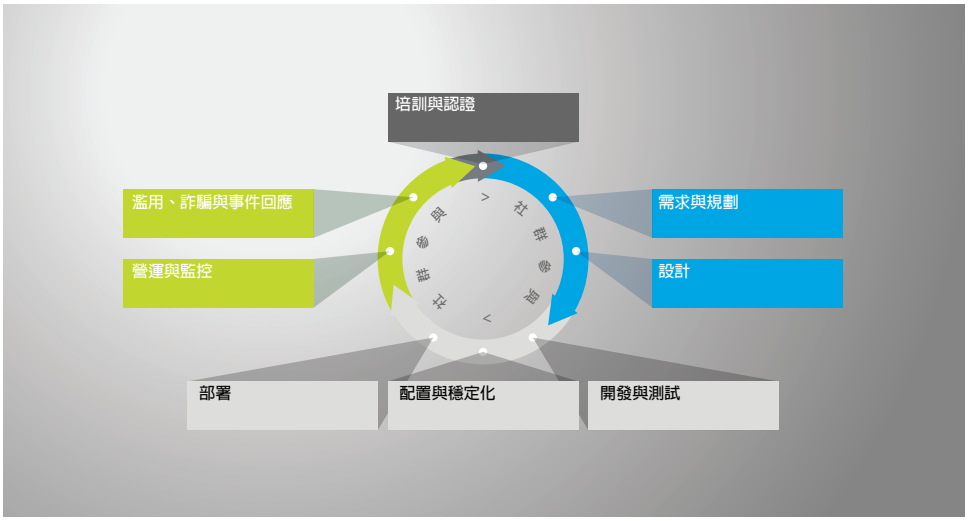
就如其他關鍵的 Adobe 產品和服務組織，Adobe Document Cloud 組織同樣採用 Adobe SPLC 流程。Adobe SPLC 是一套由數百種特定安全性活動組成的嚴謹流程，橫跨軟體開發慣例、流程和工具，其整合進產品生命週期的多個階段，涵蓋範圍從設計和開發，到品保、測試與部署。ASSET 安全性研究人員會根據可能的安全性問題進行評估，為每一項產品或服務提供專屬的 SPLC 指南。輔以持續的社群參與，Adobe SPLC 得以在技術、安全性慣例與威脅景況變化的環境中，不斷進化並保持最新狀態。

Adobe 安全產品生命週期

依特定 Adobe Document Cloud 元件而定，Adobe SPLC 活動包括以下部分或全部的建議最佳做法、流程及工具：

- 產品團隊的安全性訓練和認證
- 產品健全狀況、風險及威脅景況分析

- 安全編碼指南、規則及分析
- 引導 Adobe Document Cloud 安全性團隊的服務藍圖、安全性工具及測試方法，有助於因應 Open Web Application Security Project (OWASP) 的 10 大關鍵 Web 應用程式安全性風險，以及 CWE/SANS 的 25 項最危險的軟體錯誤
- 安全性架構審核與深入測試
- 原始碼審核，有助於消除可能導致弱點的已知瑕疵
- UGC 驗證
- 應用程式和網路掃描
- 完整應對審核、回應計劃及發行開發人員教材



Adobe 安全產品生命週期

Adobe 軟體安全性認證課程

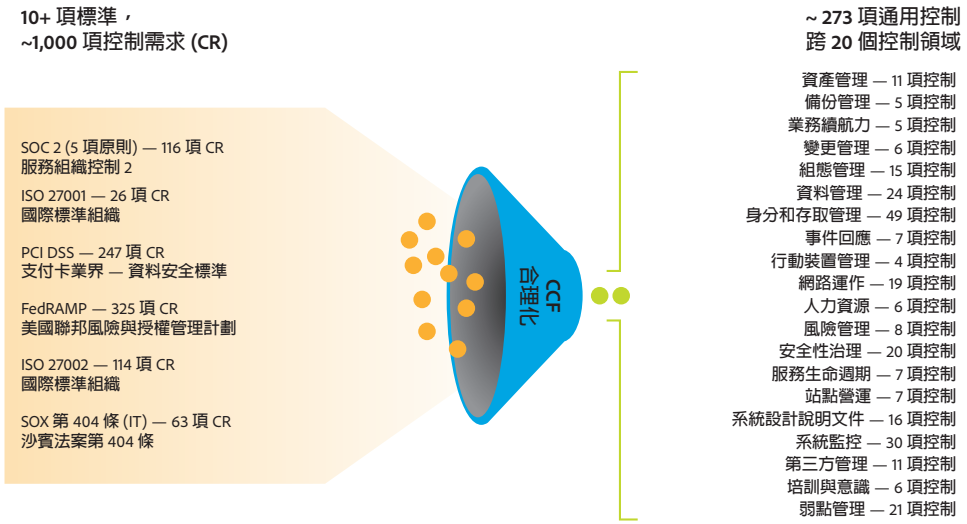
Adobe SPLC 當中涵蓋了 Adobe 在開發團隊內持續進行安全性訓練，藉此強化全公司的安全性知識，並提升我們產品和服務的整體安全性。參加 Adobe 軟體安全性認證課程的員工可藉由完成安全性專案獲得不同的認證等級。如需產品安全性做法的詳細資訊，請參閱 Adobe 安全工程設計總覽。

如需 Adobe 軟體安全性認證課程的詳細資訊，請參閱 Adobe 安全性文化白皮書。

Document Cloud 服務合規性

Adobe 通用控制框架 (CCF) 是我們在產品營運團隊內，以及基礎架構和應用程式團隊中不同部分所實施的一套安全性活動和合規性控制。

建立 CCF 的過程中，Adobe 分析了雲端架構業務最常見的安全性認證準則，並合理處理超過 1,000 項需求，涵蓋對應約數十種業界標準的 Adobe 專屬控制。



Adobe 通用控制框架

Adobe Document Cloud 服務的最新法規和合規性

SOC 2 是一套安全性原則，訂定了與安全性、機密性及隱私權相關的領先做法控管。Adobe Document Cloud 服務合乎 SOC 2 Type 2 (安全性和可用性) 的規範。

ISO 27001 是一套全球採行的標準，概述了嚴格的安全性需求並提供系統化的方法，用於管理客戶資訊的機密性、完整性及可用性。Adobe Document Cloud 服務符合 ISO 27001:2013。

支付卡業界資料安全標準 (PCI DSS) 是處理支付卡資訊 (如信用卡號碼) 的組織專屬的資訊安全標準。Adobe 身為符合 PCI DSS 的服務提供者，能夠協助客戶符合 PCI 對安全處理持卡人相關個人身分資料的需求。

金融服務業現代化法 (GLBA) 要求金融機構保護其客戶的個人資料。Adobe Document Cloud 服務已符合 GLBA 的規範，能夠讓我們的金融機構客戶符合 GLBA 對於使用服務提供者的需求。

美國聯邦風險與授權管理計劃 (FedRAMP) 是一項官方計劃，提供標準化的方法對雲端產品和服務進行安全性評估、授權及持續監控。Adobe Document Cloud 服務是為 FedRAMP 量身打造，能夠讓我們的客戶符合 FedRAMP 的需求。

美國家庭教育權利與隱私法案 (FERPA) 是專為保護美國學生教育記錄和目錄資訊的機密性所設計的法案。依據 FERPA 的規範，Adobe 能夠透過合約方式同意在處理受管制的學生資料時擔任「校方負責人」，讓我們的教育機構客戶符合 FERPA 的需求。

SAFE-BioPharma 標準說明身分驗證或數位簽署所需的標準化身分信任需求。Adobe Document Cloud 通過認證，符合 SAFE-BioPharma 的數位識別標準。Adobe Acrobat DC 可在遵循 SAFE-BioPharma 工作流程的範圍內安全使用。此外，Adobe Document Cloud 服務和 Adobe Sign 合乎 SOC 2 Type 2 的規範。

如需 Adobe Sign 現行合規性情形的詳細資訊，請參閱 Adobe Sign 技術總覽。

最後，客戶須負責確保合乎其法律義務之規範，並確認我們的解決方案合乎其合規性需要，並受到適當的方式保護。

Adobe 員工

Adobe 的員工與辦公室遍佈全球各地，並於公司上下實施下列流程和程序來保護公司免於遭受安全性威脅。

員工對客戶資料的存取權

Adobe 將 Adobe Document Cloud 的開發和生產環境保持區隔，採用技術控管的方式限制對實際生產系統的網路和應用程式層級存取。員工擁有特定授權可存取開發和生產系統，而沒有正當業務目的的員工則無法存取這些系統。

背景審查

Adobe 基於聘僱目的取得背景審查報告。通常 Adobe 所需的特定報告性質與範圍包含有關教育背景、工作經歷及法院記錄的查詢，包括犯罪記錄，以及向專業和個人相關人士取得的參考資料，這些資料均在適用法律允許之下取得。這些背景審查需求適用於美國地區一般新進員工，包括將負責管理系統或能夠存取客戶資訊的人員。美國地區的新進臨時機構工作人員須經由合適的臨時機構，依 Adobe 背景過濾指南進行背景審查。在美國以外地區，Adobe 依據 Adobe 背景審查政策與當地適用法律對特定新進員工進行背景審查。

終止聘僱

Adobe 員工離職時，其主管會送出一份現有工作人員表。經核准後，Adobe 人力資源部門便會展開電子郵件工作流程，通知相關利益者在該名員工離職日之前採取特定行動。若是 Adobe 主動終止聘僱，Adobe 人力資源部門會傳送類似的電子郵件通知相關利益者，包括聘僱終止的特定日期和時間。

Adobe 公司安全部門接著安排以下行動，協助確保員工離職當天即不再擁有存取 Adobe 機密檔案以及進出辦公室的權限：

- 移除電子郵件存取權
- 移除遠端 VPN 存取權
- 辦公室和資料中心識別證失效
- 終止網路存取

若有提出要求，主管可請大樓保全人員護送離職員工離開 Adobe 辦公室或大樓。

設備安全性

所有 Adobe 公司辦公室所在地現場都有聘僱警衛全天候保護場所安全。Adobe 員工須攜帶 ID 識別感應卡才能進出大樓。訪客須從正門進出，且出入均須於接待處簽名，並出示臨時訪客 ID 識別證，以及由員工陪同。Adobe 一律將所有伺服器設備、開發電腦、電話系統、檔案和郵件伺服器，以及其他敏感性系統鎖在環境管制的伺服器機房內，只有經適當授權的人員才能接觸。

病毒防護

Adobe 會掃描所有內送和外寄的公司電子郵件當中是否有已知的惡意程式碼威脅。

客戶資料機密性

Adobe 一律將所有客戶資料視為機密處理。除非依照 Adobe 與客戶簽訂之合約所允許以及 Adobe 使用條款和 Adobe 隱私權政策中所規定，否則 Adobe 不會代表客戶使用或分享所收集的資訊。

總結

本白皮書中說明 Adobe 主動實施的安全性和嚴格的程序，有助於保護 Adobe Acrobat DC、Acrobat Reader DC 和 Document Cloud 服務，以及您機密資料的安全。在 Adobe，我們非常重視您數位體驗的安全性。我們持續監視不斷演進的威脅趨勢，以隨時掌握惡意活動，並協助確保客戶資料的安全性。

若需詳細資訊，請造訪 Adobe 信任中心。

Adobe Inc.
香港銅鑼灣希慎道 33 號
利園大廈 4102 室
www.adobe.com/tw

5/19