

IST 文件加密系統的資安對策



對內整合後端
文管應用系統

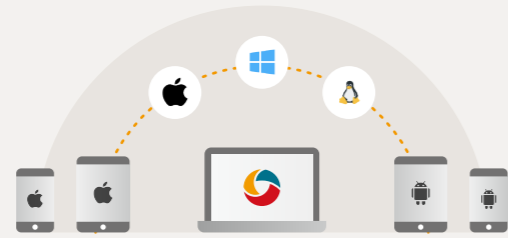
文件分級分區
使用授權明確

對外必須通過
外發審核機制

支援多種作業系統 - 電腦、手機、平板都適用

IST 文件加密系統支援跨平台應用，以因應趨多元的企業電腦類型，無論是習慣使用 Windows 的行政部門、傾向使用 Mac 的設計部門，或是以 Linux 為主的重要伺服器，都能獲得安全保障。

此外，IST 也提供支援 Android、iOS 等行動裝置的加密用戶端 App，使用者在手機或平板上就能直接執行文件加解密功能，應用彈性更高、更便利。



優勢特色

- 隨身碟加密用戶端
授權用戶端安裝於隨身碟中
打造移動式加密安全環境
- 分級分區
可指定機密等級與安全存取區域
只看該看的文件
- 郵件白名單
寄/收件者皆符合設定條件
收件者收到的附件智慧解密
- 手機加密用戶端
支援 Android 及 iOS
可於手機或平板執行加解密
- 外發審核流程
機密文件須提出申請並獲得核准
才能產生外發加密檔
- 即時備援/備份
備援伺服器於意外發生時接手
穩定中確保機密資料安全
- 自訂授權軟體
支援各類型應用軟體
未獲授權無法取得加密內容
- 外部讀取加密檔
專用閱讀器搭配外發授權機制
為文件安全把關
- 整合後端系統
IST 安全閘道器整合後端系統
免客製，穩定性高

導入效益

安全管理

內外部流通皆受管控

靈活應用

手機與平板均可適用

操作簡便

自動背景執行加解密

系統整合

免客製整合文管系統

系統需求

安裝模組	軟體需求	最低硬體需求
資料庫	MS SQL Server 2005 SP1 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019	Pentium 4 雙核心處理器 4GB RAM 硬碟可用空間 120GB
伺服器	Windows 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022	
控制台	Windows 7 / 8.x / 10 / 11 Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022	Pentium 4 處理器 2GB RAM 硬碟可用空間 4GB
用戶端	Windows 7 / 8.x / 10 / 11 Windows Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022 Linux、Mac OS (詳細版本支援請來電洽詢)	

實際硬體需求及儲存空間用量，以評估客戶環境需求後之建議規格為主。

安和科技

安和科技集結來自不同領域的端點安全專家，從產品研發、功能創新與改善，到針對各產業特殊需求而設計的應用方案，以全方位的技術能量，打造更符合企業應用的「IST端點安全系統」與「IST文件加密系統」，不只協助企業即時解除內部安全危機，更可及早察覺潛在風險，同時也承諾透過持續更新、不斷進化的功能，全力為用戶守護資訊資產。

安和科技有限公司 www.ist.tw

11491 台北市內湖區陽光街321巷56號5樓
5F., No.56, Ln.321, Yangguang St., Neihu Dist.,
Taipei City 11491, Taiwan (R.O.C)

+886 2 7732-0668 TEL
+886 2 7732-0699 FAX
+886 2 7732-0669 技術支援專線

sales@ist.tw
support@ist.tw

第三方公司名稱或商標為其所有人擁有



IST 文件加密系統

自文件新增儲存的瞬間即自動加密
無論在企業內外部都同樣受到保護

文件加密不限檔案格式
與外部交換文件安全便利
支援Windows, Mac, Linux, Android, iOS

www.ist.tw

機密資料遺失、遭竊的風險，公司承受得起嗎？

在企業引進各種安全技術以因應資安問題的同時，資料外洩事件仍持續發生，除了無所不在的外部攻擊、永遠補不完的漏洞，內部人員和相關第三方更是主要關鍵，無論是無心的人為疏忽，或是惡意竊密，都可能對企業造成極大傷害。

各種企業機密，例如設計圖、原始碼、研究資料、獨家配方等智慧資產，以及透過數據分析後而成為公司 know-how 的機敏資料，一旦外流或遭到惡意刪除，究竟會對企業造成多大的營運風險，不僅難以估算，更是無法承擔。

研發部門
程式碼、配方、研究測試報告...

設計部門
產品設計圖、新機圖形介面...

採購部門
物料成本、供應商資料...

行銷部門
新品規格、上市時程、銷售策略...

製造部門
製程文件、生產計畫、機台佈局...

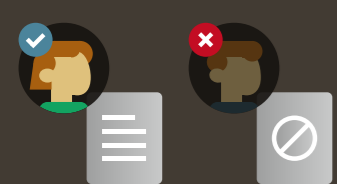
業務部門
客戶資料、報價單、訂單...

財務部門
財務報表、資金規劃...

法務部門
各式合約、訴訟資料...

依需求設定檔案使用權限，強化機密資料保護

直接限定
授權使用者



通過審核流程
才能外發加密文件



各別指定
可讀取的機密等級



符合郵件白名單
附件智慧解密



依職務賦予
不同加密授權模式



外發限制讀取時間
及操作權限



禁止複製、禁止列印、
限制次數...

加解密權限

滿足各種職務需求，無須改變操作習慣

四種加密授權模式

管理者可根據各員工的職務需求，為其預設適用之授權，待用戶端電腦執行加密檔時，便自動啟用預設模式，實際操作與執行一般檔案無異，使用習慣一如以往，有助企業順利推動加密安全政策。



自訂授權軟體

獲得授權才能存取加密文件

軟體類型不受限

IST 控制台已預設辦公軟體、文字處理、二維／三維工程設計、電子電路設計、圖形圖像設計、程式設計開發等常用軟體類型，以及數十種應用程式；當然，企業也可依需求自訂各種授權軟體。

單一介面同時管理

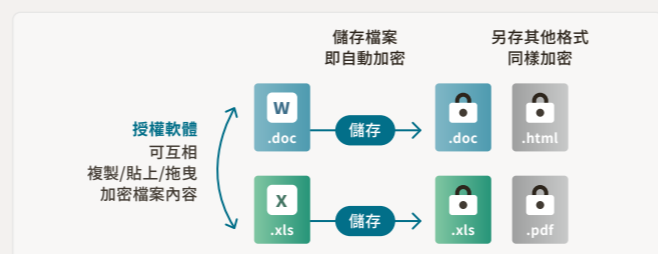
Win、Mac、Linux 授權軟體

管理者透過 IST 控制台的文件加密管理介面，即可同時查看與管理 Windows、Mac、Linux 等作業環境下的授權軟體。

控制軟體		
Win	Linux	Mac
全部授權軟體		
自動授權軟體		
文書處理		
程式開發		
圖形圖像設計		

授權軟體自動執行加解密

可授權指定軟體存取加密文件，即便使用者將加密文件轉存為其他檔案格式，該文件仍會以加密狀態轉存。



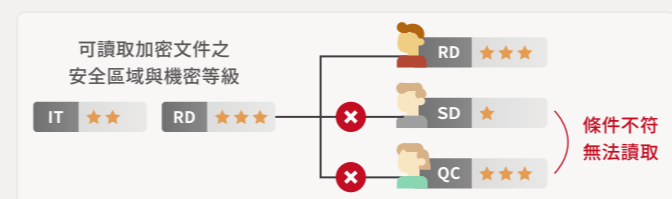
非授權軟體
無法開啓加密檔

分級分區授權

只能依規定存取該看的文件

文件分級分區

預先指定加密文件的機密等級與可讀取的安全區域（例如某部門），唯有符合該授權條件者才能讀取內容，確保資料安全不外洩。



行動加解密

以行動裝置執行文件加解密

手機加密用戶端App

IST 手機加密用戶端支援 Android 及 iOS，使用者透過手機或平板就能依權限檢視、編輯加密文件，如常執行文件加解密功能。

IST 手機加密用戶端 App
支援 Android 及 iOS



檔案外部流通

分享加密文件安全又方便

通過審核才能外發加密文件

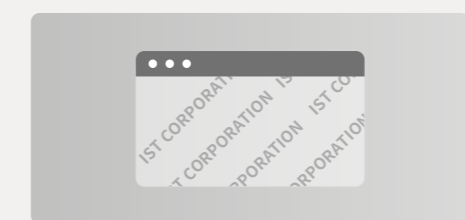
外發機密文件之前，必須向管理員提出申請，並可事先指定授權對象，核准後才能產生加密文件，供外部合作廠商使用。

外發授權、浮水印 確保文件在外安全

外發授權項目多元，例如：是否允許列印／虛擬列印、螢幕擷取、執行剪貼簿複製、修改、文件編輯等，亦可限制檔案的開啓次數、有效期限，或要求同步標準時間、進行密碼認證。

外發視窗浮水印

可在外部電腦開啓外發加密文件的視窗中顯示螢幕浮水印，一旦外部使用者以拍照方式留存文件內容、洩漏機密資料，即可藉由浮水印上的資訊追查洩密來源。



可在用戶端電腦的加密文件視窗中顯示浮水印

系統容災、備援與檔案備份

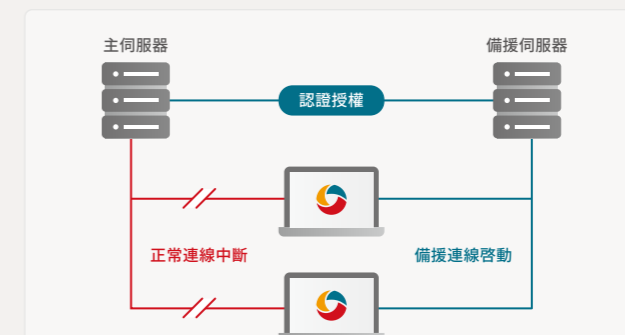
穩定中確保機密資料安全

系統容災時間

只要預設容災時間，即使網路或伺服器發生異常或故障等狀況，導致用戶端與伺服器之間無法正常連線，用戶端仍可在預設時間內，正常的依既定權限執行文件加解密操作。

加密備援模式

當 IST 主伺服器發生問題，預設之備援伺服器將自行啓動進入備援模式，以維持系統正常運作。



檔案備份機制

加密文件可選擇以明文（未加密）、密文（加密）或原文（維持原檔案的加解密狀態）等方式備份到檔案備份伺服器，以確保企業重要文件的內容完整保留！

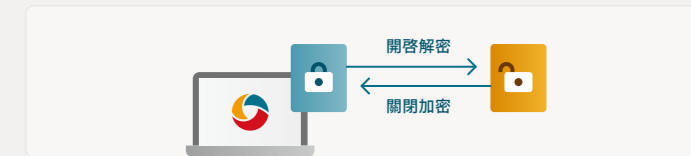


外部使用者免安裝用戶端

方式 1 | 加密文件整合專用閱讀器

加密文件與 IST 專用閱讀器整合成一個外發檔案，直接點擊檔案就能開啓加密文件，關閉該檔案即回復加密狀態。

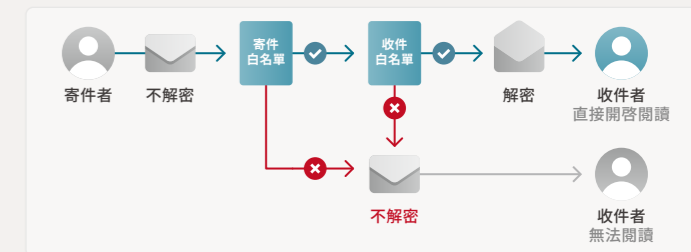
■ 適用對象：出差員工、下游廠商



方式 2 | 郵件白名單，附件智慧解密

郵件寄送加密檔案時，只要寄件者與收件者都在白名單列表內，IST 會在郵件傳輸過程中解密附件，收件者將收到解密的檔案。

■ 適用對象：原廠、上游廠商



離線辦公保護

不在辦公室也能持續加密運作

申請臨時 / 長期離線授權

臨時或長期離線，用戶端必須向管理員提出申請並通過審核。

隨身碟加密用戶端

打造移動式的安全加密環境，將已安裝授權 IST 用戶端的隨身碟插入任一電腦，便可遵循企業所賦予之權限，存取或編輯加密文件。



免客製整合後端系統

無縫整合既有系統與加密機制

IST 加密閘道器(另購)

專為 IST 文件加密系統所打造，達成加密檔案上傳至後端系統，如：ERP、CRM、PLM/PDM 等伺服器時自動解密，檔案從前述伺服器下載至合法用戶端電腦時自動加密的安全機制。

上傳至後端系統的檔案以明文儲存，不影響伺服器檔案管理。

