

「護數守設 安全之道」



守護 AI 時代下的 香港 K12 教育生態

網絡安全、數據私隱
合乎道德的 AI 應用

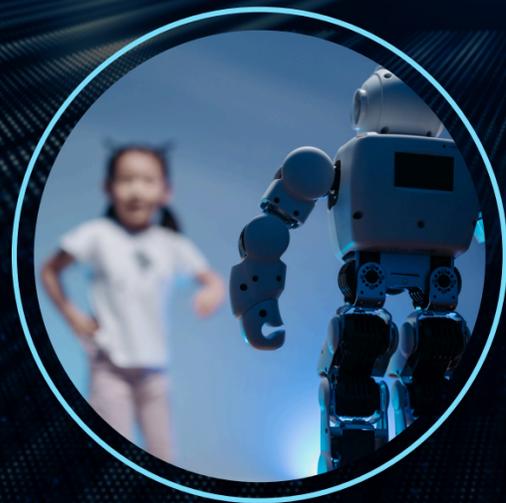


Ken Chung
K-Solve Global



K12 教育中的 AI 網絡安全與數據安全

教育領域的AI應用：機遇與風險



香港K12機構面臨的主要威脅

案例研究與經驗總結



保障AI系統安全的最佳實踐

K12教育中的 AI 網絡安全 與數據安全簡介



K12教育中的 **AI** 網絡安全與數據安全簡介

隨著人工智慧 (**AI**) 技術在教育領域的快速普及，
K12教育機構正經歷數位化轉型的浪潮。

從智慧教室到個性化學習平臺，**AI**應用顯著提升了教學效率與學生體驗。

技術的深度整合也伴隨著新型網絡安全威脅與數據隱私風險。

尤其是K12教育機構，因其服務對象為未成年人，
且涉及大量敏感個人數據（如學生身份、學習記錄、家庭資訊），
使其成為網絡攻擊的高風險目標。如何平衡AI技術的創新應用與安全防護，
已成為全球教育機構的關鍵挑戰。

探討**AI**在教育中的雙面性，並聚焦香港K12機構面臨的具體威脅與解決方案。

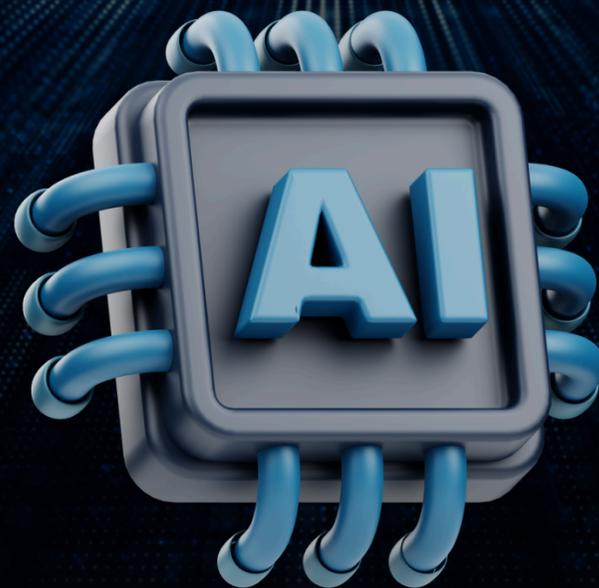
K12教育中的 **AI** 網絡安全與數據安全簡介

數碼校園的雙重防線 - 安全與私隱

定義：

AI 網絡安全： 保護系統、網絡、設備免受攻擊、破壞或未經授權存取。

AI 數據安全： 確保學生、教職員敏感信息（如成績、身份資料）的保密性、完整性。



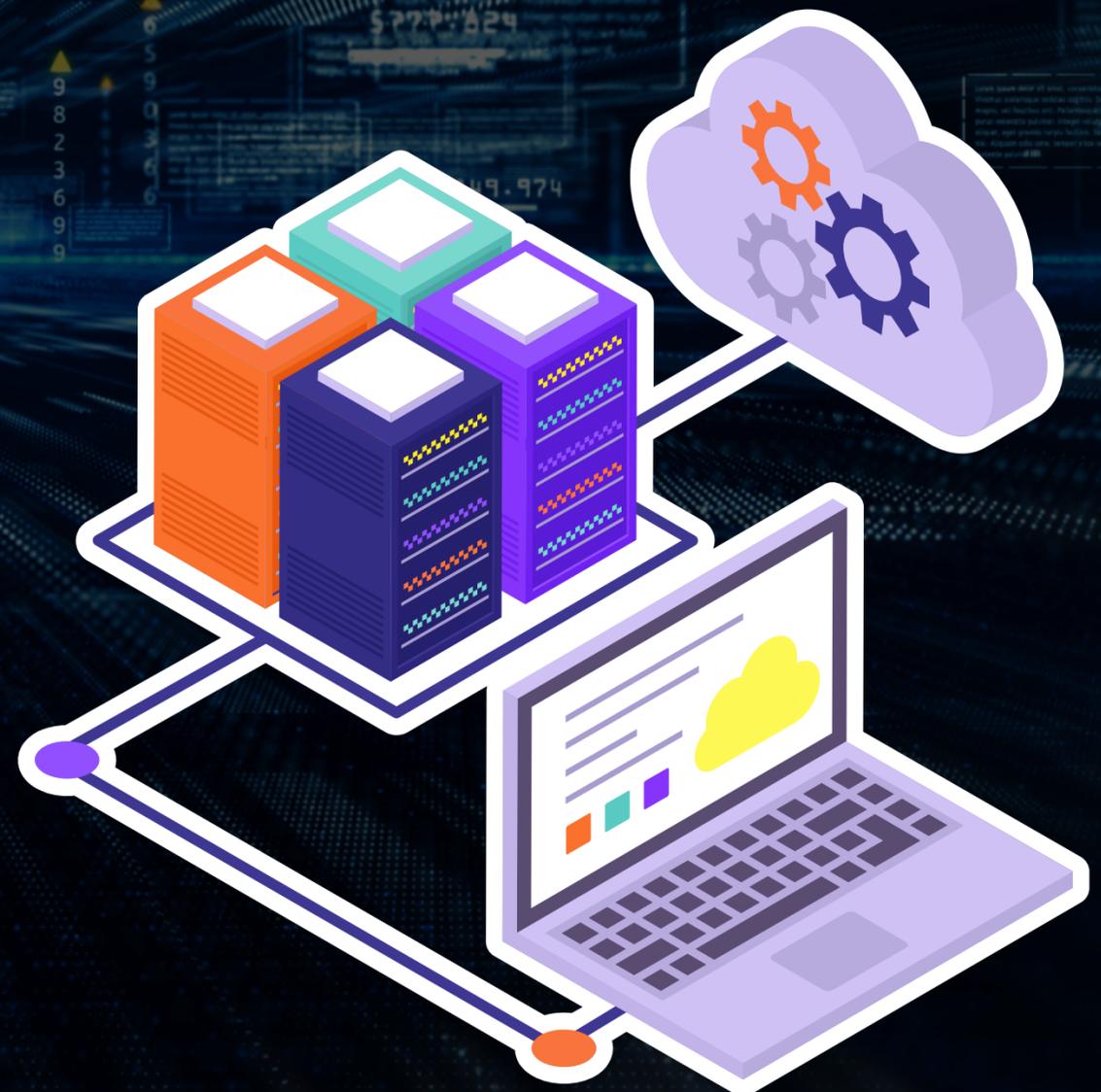
K12教育中的 AI 網絡安全與數據安全簡介

數碼校園的雙重防線 - 安全與私隱

香港教育現狀：

97%學校使用雲端教學平台（教育局數據）

BYOD政策普及→設備管理複雜化



K12教育中的 AI 網絡安全與數據安全簡介

數碼校園的雙重防線 - 安全與私隱

為何重要：

合規要求：違反《私隱條例》最高罰款100萬港元

信任基礎：家長對數據處理透明度的期待



關於公署 | 私隱條例 | 資訊及活動 | 執法報告 | 常見問題 | 審查及執法 | 「起底」罪行 | 數據安全新 | 防騙貼士 | 投訴 | 教育及培訓 | 資源中心 | 聯絡我們

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

關鍵字搜尋

主頁 > 私隱條例 > 《個人資料(私隱)條例》

RSS A A A Eng

私隱條例

《個人資料(私隱)條例》

- 六項保障資料原則
- 實務守則 / 指引
- 《2021年個人資料(私隱)(修訂)條例》
- 2012年條例修訂
- 當值律師服務
- 其他刊物
- 歡迎《通用數據保障條例》
- 內地《個人信息保護法》

《個人資料(私隱)條例》

《個人資料(私隱)條例》(「條例」)在一九九五年通過,並於一九九六年十二月正式生效(個別條文除外),條例是亞洲區內最早全面保障個人資料私隱的法例之一,源自法律改革委員會在一九九四年八月發表題為「有關保障個人資料的法律改革」的報告書,該報告書建議以經濟合作及發展組織的一九八零年私隱指引¹為基礎,為私隱保障進行本地立法,以確保對個人資料有足夠的保障及落實有關人權的公約責任,保持香港作為國際商貿中心的地位,條例在二零一二年進行了主要的修訂,包括針對使用個人資料作直接促銷的新規定,並為應對私隱保障工作的新挑戰和公眾關注而加入更多保障,及至二零二一年,條例進行了另一次主要的修訂,旨在打擊侵犯個人資料私隱的「起底」行為,將「起底」行為列為刑事罪行,賦予個人資料私隱專員法定權力發出停止披露通知,要求停止或限制披露涉及「起底」內容,同時賦予私隱專員權力就「起底」個案進行刑事調查和檢控,以加強對「起底」個案的執法力度,按此瀏覽《個人資料(私隱)條例》

按此瀏覽《2021年個人資料(私隱)(修訂)條例》(刊憲日期:2021年10月8日)

按此瀏覽《2021年個人資料(私隱)(修訂)條例草案》(草案刊憲日期:2021年7月16日)

條例簡介

條例適用於公私營機構(包括政府),屬於科技中立及原則性的法例,條例附表一的保障資料原則,列出資料使用者應如何收集、處理及使用個人資料,此外條例亦有其他條文訂明更多的循規要求。

在講解條例的細節前,須先了解一些主要概念的定義:

- 個人資料是指與一名在世人士有關及可確定個人身份的資料,亦必須以可供查閱及處理的方式記錄下來。
- 資料當事人是指屬於相關個人資料的當事人的個人。
- 資料使用者是指控制個人資料的收集、持有、處理或使用的人,不論是獨自還是與其他人共同控制。
- 資料處理者是指非為本身目的而是代另一人(資料使用者)處理個人資料的人,資料處理者並不受條例直接規管,但資料使用者有責任透過合約規條或其他方式,確保他們的資料處理者符合條例相關的要求。

總括來說,保障資料原則是為了確保個人資料的收集方式是具透明度及公平,亦須盡量減低個人資料的收集;一經收集,應以安全的方式處理個人資料,而資料的保留時間不應超過達成原來的目的所需,個人資料的使用亦應限於或關乎原來收集目的;資料當事人有權查閱或改正自己的個人資料。

原則1 收集目的及方式

保障資料第1原則訂明,資料使用者須為直接與其職能或活動有關的合法目的,收集個人資料;收集的資料對該目的是必要及足夠的,但不超乎程度,而收集的方法應該是合法及公平的。

教育領域的AI應用： 機遇與風險



教育領域的AI應用：機遇與風險

AI革新教育——機會與暗礁並存

機遇

AI技術為教育帶來革命性突破：

個性化學習：

通過學習數據分析，AI可為學生提供適性化教材與即時反饋。

教學效率提升：

自動化評分、課堂管理工具減輕教師行政負擔。

教育普惠：

AI語言翻譯與輔助工具幫助少數族裔或特殊需求學生融入主流教育。



教育領域的AI應用：機遇與風險

AI革新教育—機會與暗礁並存

風險

數據隱私漏洞：

學生生物特徵（如人臉識別）、行為數據若遭洩露，可能被用於詐騙或定向攻擊。

算法偏見：

訓練數據不足可能導致AI推薦系統歧視特定學生群體。

系統濫用風險：

生成式AI（如ChatGPT）可能被學生用於作弊，或產生虛假教育內容。



香港K12機構面臨的 **AI**網絡安全主要威脅



香港K12機構面臨的主要 AI 威脅

香港學校的數碼 AI 防禦戰

威脅地圖

- **AI 外部攻擊：勒索軟件**（2023年教育界攻擊+40%）
- **內部疏失：教師,學生,家長誤開惡意郵件附件**（佔事故65%）



香港K12機構面臨的主要 AI 威脅

香港學校的數碼 AI 防禦戰

AI 放大風險：
深度偽造語音冒充校長詐騙（2024年香港某國際學校案例）
自動化攻擊工具降低黑客門檻

May 8, 2025 10:00 PM Eastern Daylight Time

根據《2025年Imperva惡意機器人報告》，人工智慧推動了難以偵測的機器人的增加，目前這類機器人產生的流量已占全球網際網路流量的一半以上

Share      

- 易於取得的AI工具的興起顯著降低了網路攻擊者的進入門檻，使他們能夠大規模建立和部署惡意機器人
- 自動化流量十年來首次超過了人類活動產生的流量，占所有網路流量的51%
- 針對應用程式介面(API)的攻擊在進階機器人流量中激增至44%，旅遊業整體上成為機器人攻擊的頭號目標



新聞 / 即時 / 港聞 / 有電騙集團假扮校長訛校工 警拘6人涉款52萬元

2025.03.16 16:12

商業罪案調查科訛騙組高級督察 陸鴻基
案情簡報 拘6人·涉串謀詐騙及洗黑錢

警方拘捕6人涉嫌「串謀詐騙」及「洗黑錢」等罪。(警方FB)

【點新聞報道】有詐騙集團招募非華裔人士開設傀儡戶口及登記電話卡，並以假冒身份進行電話騙案。警方於3月14至15日拘捕6人，涉嫌「串謀詐騙」及「洗黑錢」等罪，牽涉12宗電話騙案，涉及騙款約港幣52萬元。

警方指，該詐騙集團自去年11月起運作，調查發現該集團招募非華裔人士開設傀儡戶口及登記電話卡，並利用電話卡致電受害人時自稱同事，以假冒身份行騙，其中一些個案騙徒假扮學校校長或教職員，令不少校工中招。截至今年2月，警方接報不少有12人上線，受騙金額

熱門新聞

綜援生果金等人士今起陸續獲發「半糧」 即睇詳細金額

王楚欽奪冠後 致敬「星島報」 價值得他們 有多不容易

【有片】王楚欽奪冠後致敬馬龍樊振東：慢慢懂得他們有多不容易

【有片】團「粉」成功！孫穎莎奪冠後將國際奧委會主席拉入「朋友圈」

點觀香港 | 港鐵被罰1920萬設1日半價乘車 孫穎莎

AI模型逆向工程攻擊

黑客試圖竊取訓練數據或模型參數，尤其威脅使用本地化粵語數據集的AI教育設施。



邊緣設備漏洞

智慧教室的IoT設備（如AI監控鏡頭、電子白板）常因未更新韌體成為入侵突破口。



香港K12機構面臨的主要 AI 威脅

香港學校的數碼 AI 防禦戰

合規壓力：

- 跨境數據流動限制（如內地,外國《數據安全法》影響跨境平台）



中華人民共和國香港特別行政區政府
數字政策辦公室

關於我們 我們的工作 主要措施 最新消息 相關資源 聯絡我們

數據治理

主頁 > 我們的工作 > 數據治理 > 優化數據治理

數據安全保障方面

為確保政府資訊科技系統的推行和運作暢順，數字辦已於2024年2月向各局/部門推出一系列新措施，包括為大型及高風險資訊科技項目在推出前安排額外的獨立網絡安全測試，例如透過模擬實際入侵攻擊演練，有助局/部門及早發現和修補相關系統漏洞，並評估系統在應對網絡攻擊時的偵測及復原能力。

政府各局/部門須遵循《政府資訊科技保安政策及指引》所載的規定，而相關資訊保安原則基本上與私隱專員公署制訂的《資訊及通訊科技的保安措施指引》內所述的建議措施方向一致，包括須加密傳輸中和存儲中的資料；不可於公有雲平台存儲敏感及個人資料；以及各局/部門須定期為其資訊科技基礎設施、資訊系統及數據資產進行保安風險評估及審計等。《資訊及通訊科技的保安措施指引》亦已向外發布，供業界（包括公私營機構）參閱及按其情況制訂適用的資訊科技保安措施。

如《香港促進數據流通及保障數據安全的政策宣言》所述，數字辦已制訂《數據中心保安實務指引》，以加強數據中心基建安全。

數字辦加強局/部門的恆常資訊系統保安風險評估及審計工作、日常網絡檢測、抽查、遵行審計和員工培訓等，以提升政府資訊系統及網絡安全的監察和防禦能力。此外，數字辦會牽頭定期舉辦網絡安全攻防演練，測試和加強政府部門和公營機構的資訊系統安全。



中华人民共和国中央人民政府
www.gov.cn

首页 | 简 | 繁 | EN | 登录 | 邮箱 | 无障碍

中华人民共和国数据安全法

2021-06-11 08:37 来源：新华社 字号：默认 大 超大 | 打印 | 分享

新华社北京6月10日电

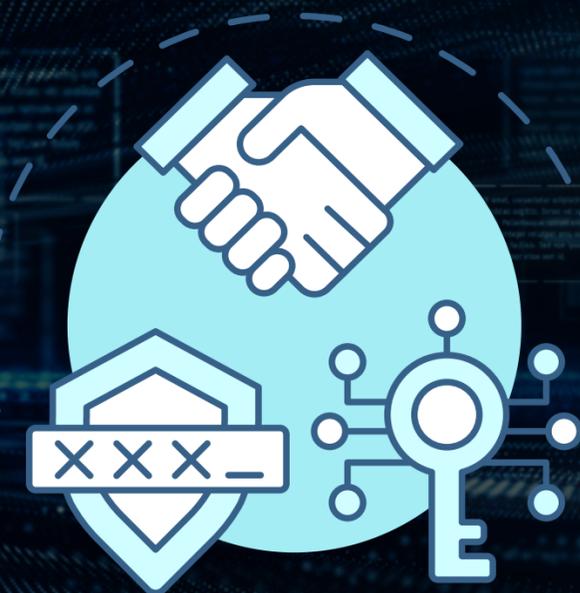
中华人民共和国数据安全法

（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）

目录

- 第一章 总则
- 第二章 数据安全与发展
- 第三章 数据安全制度
- 第四章 数据安全保护义务
- 第五章 政务数据安全与开放
- 第六章 法律责任
- 第七章 附则

跨境數據合規風險 使用境外AI服務（如中國內地或美國雲端平臺） 可能違反香港《個人資料（私隱）條例》。



跨境數據合規的本質是「法律管轄權競合」問題。香港K12機構應建立三層防護：

- 法律盡調：在使用內地AI服務前，要求供應商提供數據出境合規證明（如安全評估備案回執）；
- 技術隔離：通過數據脫敏、邊緣計算等方式減少原始數據出境；
- 透明度管理：向家長清晰說明數據跨境場景與權益保障措施，避免信任危機。

保障AI系統網絡安全的 最佳實踐



保障AI系統網絡安全的最佳實踐

從防禦到韌性 - AI時代的安全架構

技術層面：

數據最小化：僅收集必要資料（如匿名化課堂參與度數據）

加密雙保險：傳輸加密(TLS 1.3)+靜態加密(AES-256)

零信任架構 (Zero Trust)：將傳統資安實踐與AI專屬防護結合有效應對新型威脅
能在保護敏感資料、模型和基礎架構的同時，推動創新發展



保障AI系統網絡安全的最佳實踐

從防禦到韌性 - AI時代的安全架構

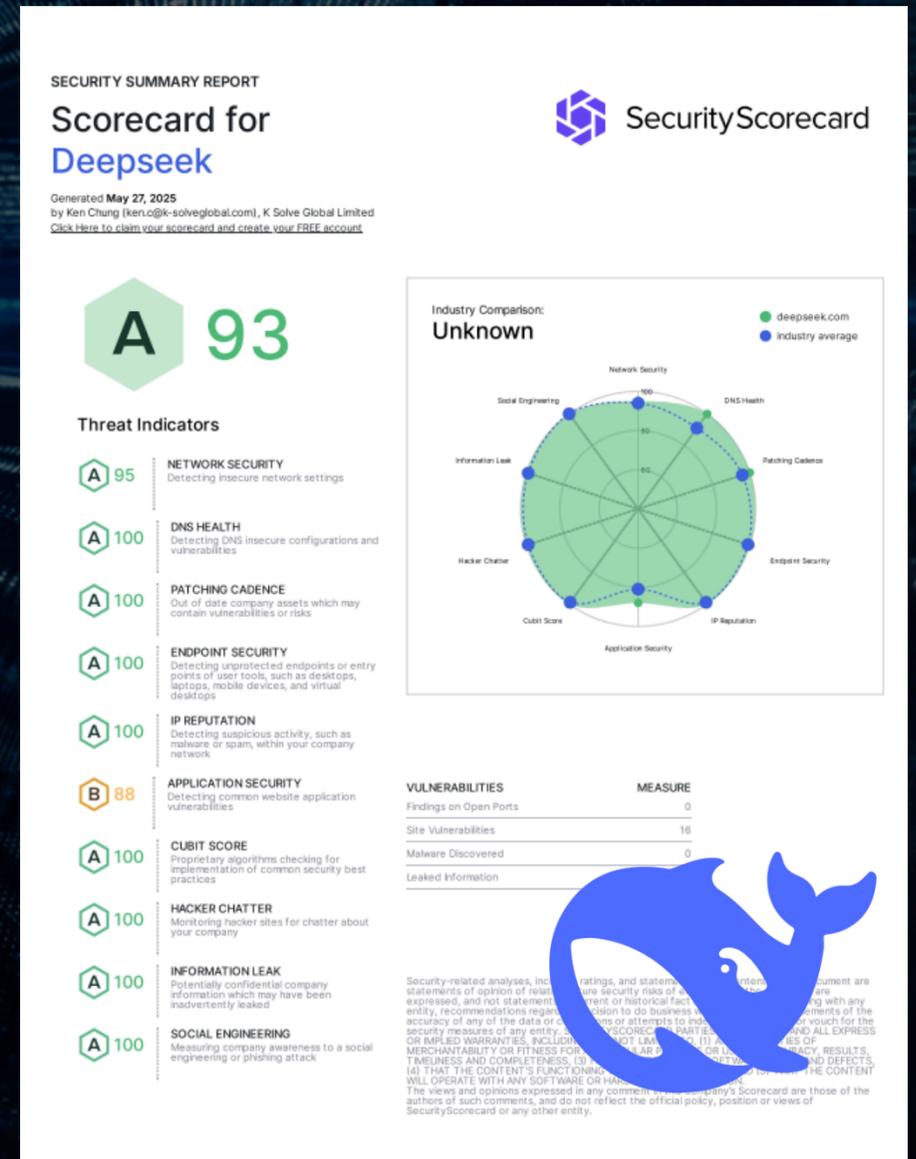
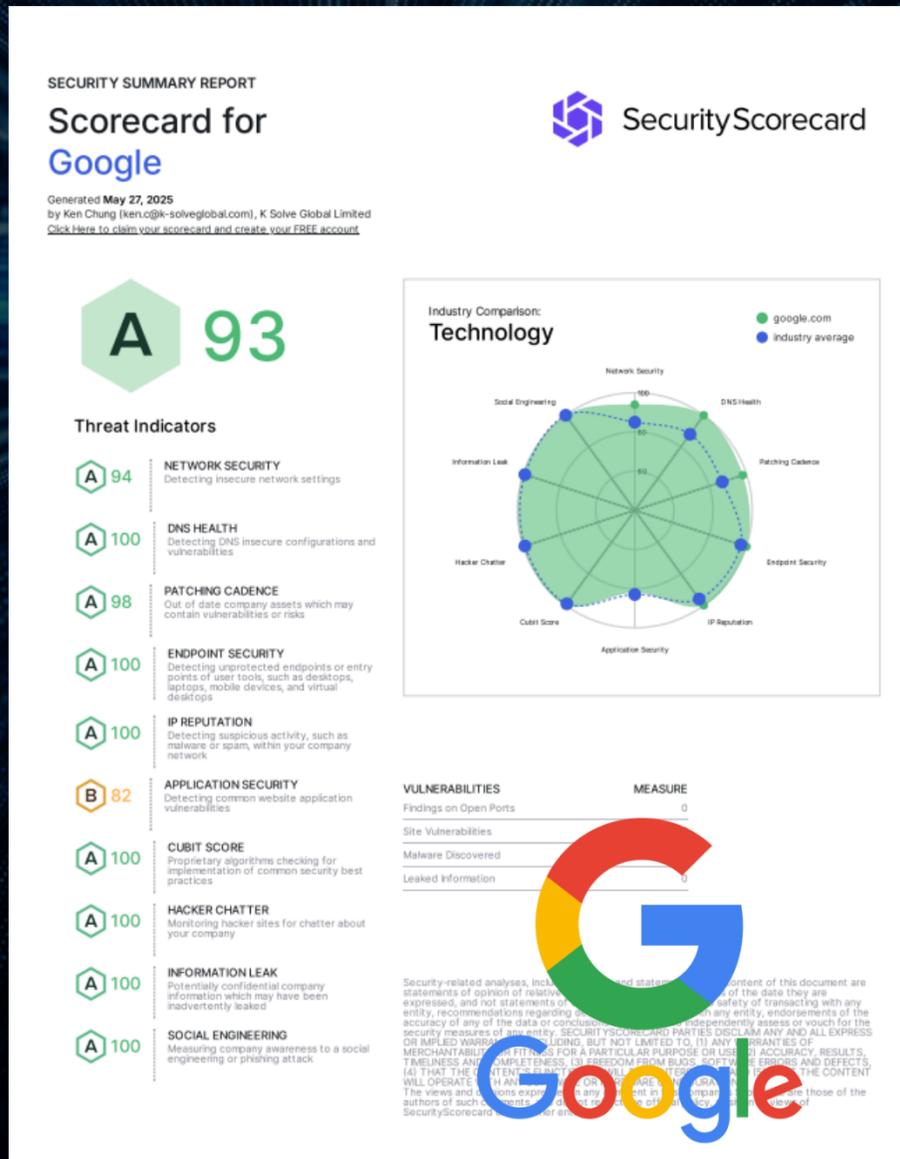
管理層面： 第三方風險評估表

[供應商名稱]

數據存儲地

ISO認證

年度滲透測試結果



2025 協作建立 第三方風險評估app

Grade	Company Name	Supplier CSRA	Certification	Total Company
D	ESET Hong Kong	2025 2024 2023	ISO27001	58
C	FUJIFILM Business Innovation Hong Kong Limited	2025 2024 2023	ISO27001	Grade A
B	Promethean Hong Kong	2025 2024 2023	ISO27001	13
B	Splashtop Hong Kong	2025 2024 2023	ISO27001	Grade B
C	Blackboard Hong Kong	2025 2024 2023	ISO27001	23
B	NEC Hong Kong	2025 2024 2023	ISO27001	Grade C
F	Konica Minolta Hong Kong	2025 2024 2023	ISO27001	11
A	Kodable Hong Kong	2025 2024 2023	ISO27001	Grade D
B	Seesaw for Schools	2025 2024 2023	ISO27001	6
F	eClass (Modern Education Research Society)	2025 2024 2023	ISO27001	Grade F
D	Tencent Education	2025 2024 2023	ISO27001	5
B	Canon Hong Kong	2025 2024 2023	ISO27001	
B	Ricoh Hong Kong	2025 2024 2023	ISO27001	
B	Lenovo Hong Kong	2025 2024 2023	ISO27001	
C	HKBN (Hong Kong Broadband Network)	2025 2024 2023	ISO27001	
F	IASPEC Education	2025 2024 2023	ISO27001	
B	VTech Education	2025 2024 2023	ISO27001	

保障AI系統網絡安全的最佳實踐

從防禦到韌性 - AI時代的安全架構

持續改進：

每學期「安全壓力測試」：模擬AI系統遭入侵場景

AI系統入侵應急響應流程報告

預演準備階段

攻擊遏制階段

系統恢復階段

入侵偵測階段

根因分析階段

事後復盤

案例研究與經驗總結



案例研究與經驗總結

全球教育AI安全實戰

學生學習平台

分析學生作業

自動化行政任務

智能溝通工具



虛擬助教

沉浸式學習

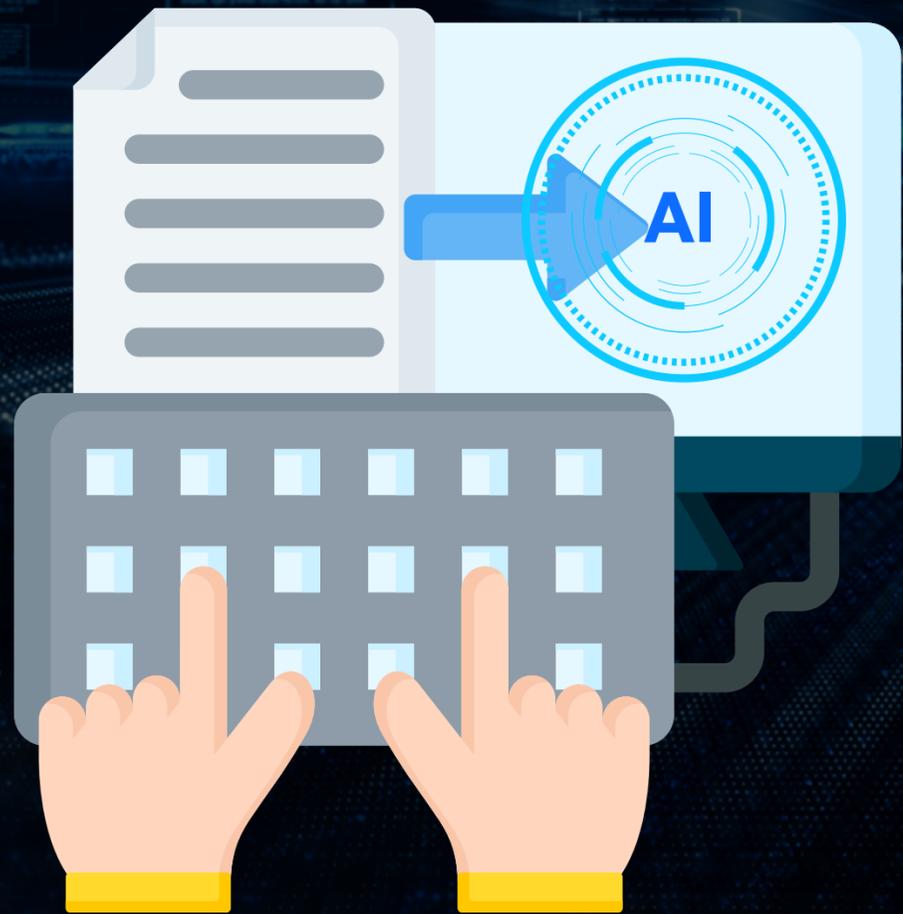
學習習慣分析

教學資源生成

教學分析與改進

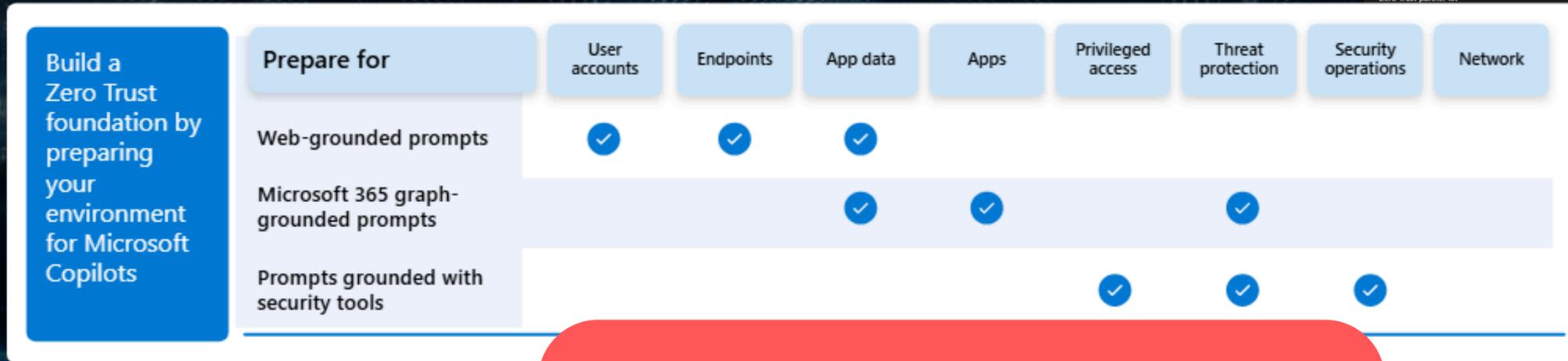
案例研究與經驗總結

用之前想一想



1. 學生個人身份資訊
2. 學業成績與評估紀錄
3. 健康與特殊需求資料
4. 家庭背景資訊
5. 行為紀律與輔導紀錄
6. 生物辨識資料
7. 地理位置與行蹤數據
8. 線上學習平台活動紀錄
9. 教職員人事資料

案例研究與經驗總結



零信任架構

Filter by title

- Zero Trust implementation guidance
- What is Zero Trust?
- Assessment and progress tracking resources
- Zero Trust partner kit

Get started with Zero Trust by preparing your environment for AI companions

You can build a Zero Trust foundation by preparing your environment for AI companions.

Category	Web-grounded prompts	User accounts	Endpoints	App data	Apps	Privileged access	Threat protection	Security operations	Network
Web-grounded prompts	✓	✓	✓	✓	✓	✓	✓	✓	✓
Microsoft 365 graph-grounded prompts	✓	✓	✓	✓	✓	✓	✓	✓	✓
Prompts grounded with security tools	✓	✓	✓	✓	✓	✓	✓	✓	✓

The following table summarizes the illustration and links to articles for implementing the recommended protections.

Prepare for	Protections	See these Zero Trust articles
Web-grounded prompts	User accounts, devices, and some app data.	Copilot Chat
Microsoft 365 graph-grounded prompts	Includes the previous protections plus more robust protection for app data and cloud apps. It also includes adding in threat protection.	Microsoft 365 Copilot
Prompts grounded with security tools	Focuses on tuning up least privilege access, a key principle of Zero Trust.	Microsoft Security Copilot

For more information on implementing Zero Trust, see the Zero Trust Guidance Center.

References

What Is Zero Trust?

Zero trust is a security model that implements continuous authentication and dynamic authorization for all users based on as many trust elements as possible, such as the identities of access subjects, network environments, and terminal status. Unlike traditional security models that evaluate entity risks through one-time verification and static authorization, the zero trust model performs continuous authentication and dynamic authorization.

Contents
Why Is Zero Trust Important?
Core Zero Trust Rules
Zero Trust Architecture
Methods Used to Implement Zero Trust

Why Is Zero Trust Important?

With the acceleration of digital transformation, enterprise information security is facing unprecedented challenges, since emerging technologies and innovative services break enterprises' existing security boundaries.

- The diversity and complexity of visitor identities and access terminals break network boundaries. In this case, traditional access control methods are too simple to meet requirements. For example, after initial user authentication, no further checks are performed to confirm the user's identity throughout the entire access process. Consequently, violations and abnormal behaviors during the access cannot be managed or controlled in real time.
- After services are migrated to the cloud, centralized data deployment breaks data boundaries and magnifies the risks involved in controlling static authorization, leading to increased potential for data abuse. Furthermore, mixing data of high and low security levels leads to permission pollution, passively increases the overall security requirements, and breaks the balance between security and service experience.
- Resource management is shifted from a distributed mode to a cloud-based centralized mode, and resources can be allocated on demand. Currently, security management and control policies are scattered, and the collaboration level is low. Once a cloud host is attacked, it is difficult to quickly mitigate the attack in a closed-loop manner.

什麼是零信任安全機制?

零信任是一種用於保護機構的安全性模型，其依據為不應預設信任任何使用者或裝置，即使對方已存在於機構的網路內。零信任機制會在整個網路上（而不只是在信任的範圍內）強制執行嚴格的身分驗證和授權，藉此移除隱含的信任。在這個模型中，所有存取資源的要求都會視為來自不受信任的網路，直到經過檢查及驗證為止。

Forrester Research 分析師 John Kindervag 在 2010 年首次提出零信任安全性模型。這標示了與傳統 IT 安全性模型不同的發展；傳統模型主要著重於在網路範圍中保護存取權，並假設內部的一切都值得信賴。

然而，如果攻擊者獲得網路存取權，則傳統做法幾乎沒有防禦機制。只要進入網路，攻擊者就能自由移動，並嘗試將入侵範圍擴展至高價值資料和資產，這種手法稱為橫向移動。如今，隨著資源和資料傳播，從單一位置實作網路的安全性控制變得困難，對現今的 IT 環境而言更是棘手。

零信任機制有助於公司強化 IT 環境的安全性，並限制或防範攻擊。

進一步瞭解 Google 如何實作 [BeyondCorp 零信任雲端安全性模型](#)，將存取權從網路範圍轉移至個別使用者和裝置。

免費試用

零信任的定義

案例研究與經驗總結



姓名	数学	语文	英语	总成绩	平均成绩
林明明	86	94	83	263	87.66666667
王进	79	78	79	236	78.66666667
杨柳书	94	81	84	259	86.33333333
刘小诗	82	98	91	271	90.33333333
刘诗琦	78	82	94	254	84.66666667
元星	80	86	75	241	80.33333333
李光	69	79	85	233	77.66666667
郭敏浩	58	83	76	217	72.33333333

新的聊天
DeepSeek-R1-FW

DeepSeek-R1-FW
由 @fireworksai
4876 名粉絲 · 600 點

歷史紀錄 費率

以低成本提供最先進的大型推理模型解題、數學和編程性能；解釋其思維鏈。您提供的數據不會用於訓練，且僅發送至美國公司 Fireworks AI。支援164k令牌的輸入上下文和文。

官方

敏感資料類型
繼續您與此應用程式的上次對話

試著說.....

Anne、Bob 和 Clara 三個人站成一排。已知 Anne 不在最前面，Bob 不在 Clara 後面，則三人順序為何？ →

池塘裡的睡蓮每天數量都會翻倍。假設第 8 天時池塘裡有 32 朵睡蓮，第幾天會達到 256 朵睡蓮？ →

訊息
+ 。

可信任平台?

案例研究與經驗總結

處理敏感數據



姓名	数学	语文	英语	总成绩	平均成绩
林明明	86	94	83	263	87.66666667
王进	79	78	79	236	78.66666667
杨柳书	94	81	84	259	86.33333333
刘小诗	82	98	91	271	90.33333333
刘诗琦	78	82	94	254	84.66666667
元星	80	86	75	241	80.33333333
李光	69	79	85	233	77.66666667
郭敏浩	58	83	76	217	72.33333333

姓名	数学	语文	英语	总成绩	平均成绩
001	86	94	83	263	87.66666667
002	79	78	79	236	78.66666667
003	94	81	84	259	86.33333333
004	82	98	91	271	90.33333333
005	78	82	94	254	84.66666667
006	80	86	75	241	80.33333333
007	69	79	85	233	77.66666667
008	58	83	76	217	72.33333333

案例研究與經驗總結

3. Section VIII_Appendix III_SOR_HKSP_INNO_018_25_Protected.xls

Copilot

The file [3. Section VIII_Appendix III_SOR_HKSP_INNO_018_25_Protected](#) contains the Schedule of Rates (SOR) for the provision of Yeeflow license subscription for InnoCell at Hong Kong Science Park for the service period from 12 August 2025 to 11 August 2026. Here are the key details:

Project Reference

- **Ref. No.:** HKSP/INNO/018/25
- **Project:** Provision of Yeeflow license subscription for InnoCell
- **Location:** Hong Kong Science Park

Key Items and Rates

1. Preliminaries

- **Scope:** Includes compliance with drawings, terms and conditions, insurance responsibility with other contractors, provision of utilities and equipment, debris removal, and provision of site access. **Amount:** Included (no specific monetary value listed)

2. Yeeflow License Subscription

Item	Description	Quantity
1	Yeeflow license	29
2	Delivery of 12,000	1

Summarize the key points in a document | Draft a response

Message Copilot

AI-generated content may be incorrect

Enterprise data protection in Microsoft 365 Copilot and Microsoft 365 Copilot Chat

Article • 03/13/2025 • 2 contributors

Feedback

In this article

- What is enterprise data protection in Microsoft 365 Copilot and Microsoft 365 Copilot Chat?
- Enterprise data protection for prompts and responses
- Privacy and security of web queries
- Agents in Microsoft 365 Copilot
- Footnotes

What is enterprise data protection in Microsoft 365 Copilot and Microsoft 365 Copilot Chat?

The use of Microsoft 365 Copilot and Microsoft 365 Copilot Chat, as used by organizations, are covered by the terms of the [Data Protection Addendum \(DPA\)](#) and [Product Terms](#), with Microsoft acting as a data processor.

Enterprise data protection (EDP) refers to controls^[1] and commitments, under the Data Protection Addendum (DPA) and Product Terms, that apply to customer data for users of Microsoft 365 Copilot and Microsoft 365 Copilot Chat. The use of the term EDP isn't meant to limit the benefits offered under the DPA and Product Terms.

SharePoint

[网络安全] 教育界

课程学习 | 课程 | 学习新语言 | 学习新技术 | 参与 | 编辑

Published 2025/2/3 | Share | Edit

永不学习 [Sample content]

领导课程 [Sample content]

学习新的语言 [Sample content]

学习新的技能 [Sample content]

职业发展课程 [Sample content]

其他资源 [Sample content]

帮助工具 | 文件库 | 寻找课程 | 表格 | 寻找课程 | 我的课程 | 寻找讲师

Welcome! Ask a question or get started with one of these prompts:

- Summarize any key highlights
- Create an FAQ based on these resources
- How can I use these resources?

Ask a question about this site

護數守設 安全之道



歡迎聯絡我