國立虎尾科技大學人事服務電子（e）報

114 年 3 月　　國立虎尾科技大學人事室編製

「人事服務電子報」(簡稱人事ｅ報)，內容涵蓋教職員喜訊、每月新知、法令宣導、人事動態、環保節能、生活知識、各類活動訊息等。各單位如有須同仁瞭解事項，都可透過本報轉知，本報為溝通之橋樑，每月透過電子郵件傳送全體同仁參考，如有任何訊息，歡迎來信提供及指教。(來信信箱：personel@nfu.edu.tw)

壹、每月新知

一、公務人力發展學院與國內公私立大學簽訂英語學習合作備忘錄，提供公務人員進修語言課程優惠方案。(公告於人事室網頁最新消息)

二、「114 年至 117 年全國公教員工及其親屬長期照顧保險方案」經公開徵選由國泰人壽保險股份有限公司獲選賡續承作。(公告於人事室網頁最新消息)

貳、法規訂定或修正

一、行政院修正「行政院表揚模範公務人員要點」第 9 點、第 10 點，並自 114 年 2 月 26 日生效。(公告於人事室網頁最新消息)

參、人事動態

異動情形	服務單位	職稱	姓名	生效日期	備註
辭職	文理學院 農業科技系	產學攜手專班約用人員	鄧宇涵	114.03.01	產學攜手專班計畫人員
到職	農業科技系	研究組員	鄧宇涵	114.03.01	
離職	農業科技系	研究組員	黃泳潔	114.03.01	
離職	研究發展處	辦事員	黃逸寧	114.03.03	
離職	工業管理系	研究佐理員	林潔宜	114.03.03	
到職	電機資訊學院	研究副管理師	陳靜美	114.03.03	
新進	管理學院 工業管理系	產學攜手專班約用人員	林潔宜	114.03.03	產學攜手專班計畫人員
離職	多媒體設計系	研究佐理員	陳思穎	114.03.10	
離職	主計室	組員	吳明展	114.03.18	

肆、114 年度續聘外聘心理諮商師為本校同仁服務

一、本校為加強對教職員工協助，聘僱 1 名心理諮商師於 114 年度 2 月、3 月及 4 月第一週及第三週的週一(即 2/3、2/17、3/3、3/17、4/7 及 4/21)上午 9:00 至 12:00 到校駐點為教職員工服務，諮詢地點為本校學生輔導諮商中心 。

二、若教職員有特殊需求，亦可至本校特約診所雲晴心理諮商所諮商。

伍、職場霸凌防治宣導

一、重申本校對於職場霸凌(職場不法侵害)採取零容忍原則，職場霸凌係指在工作環境中，個人或團體對於上司、同事或下屬進行不合理的欺凌行為，包含言語、非言語、生理、心理上的虐待或羞辱，使被霸凌者感到受挫、被威脅、羞辱、被孤立及受傷，進而折損其自信並帶來沉重的身心壓力外，並影響單位工作氛圍及頇隊合作，各單位應建立一個尊重與包容的友善職場，在處理公務上應就事論事，本開放、誠意及善意溝通，在與同仁互動過程切勿有職場霸凌情事發生。

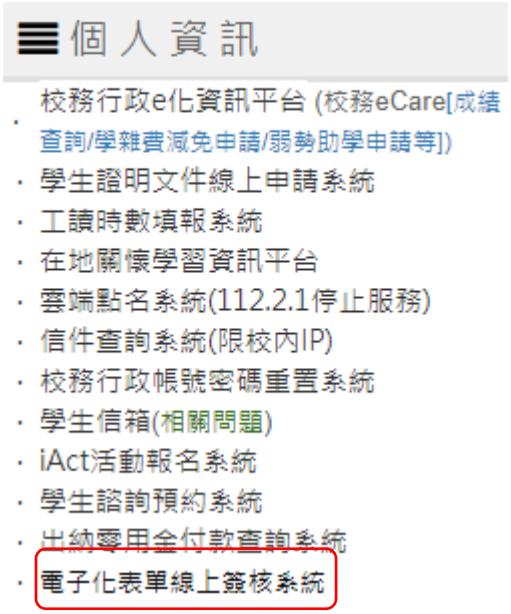
二、本校受理職場霸凌事件之專責單位為環保及安全衛生中心，另亦可至行政院人事行政總處職場霸凌通報平台(https://gov.tw/s4s 或人事總處全球資訊網首頁/常用捷徑/職場霸凌案件通報平臺)，並選擇以「無 eCPA 帳號由此進入」管道進行通報。

陸、資安宣導事項：

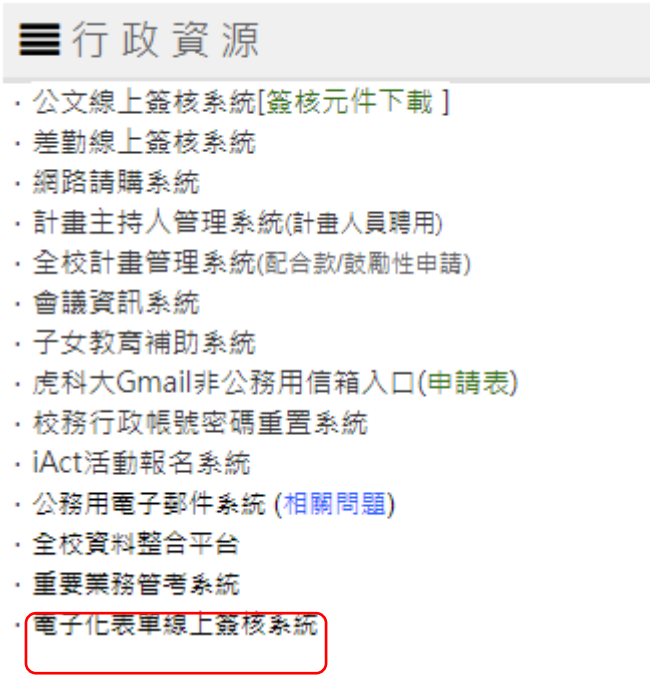
一、校內資安暨個資保護宣導訊息：

（一）本校電子化表單線上簽核系統申請網址(https://eisms.nfu.edu.tw)，登入方式使用本校 AD 帳號

1.本校首頁→使用者入口列(在校學生)→個人資訊→電子化表單線上簽核系統



2.本校首頁→使用者入口列(教師)→行政資源→電子化表單線上簽核系統



3.本校首頁→使用者入口列(職員)→全校行政專區→電子化表單線上簽核系統

（二）個人電腦安全檢查表及設定說明書宣導**(連結)**，若有問題可洽詢電算中

心#5057

（三）「資通安全責任等級分級辦法」限制使用危害國家資通安全產品**(連結)**

1.依「資通安全責任等級分級辦法」限制使用危害國家資通安全產品，將限制使用危害國家資通安全產品列入各級機關應辦事項。參考「資通安全管理法」第三條用詞，通訊產品包含軟體、硬體、服務等項。另外，具連網能力、資料處理或控制功能者皆屬廣義之資通訊產品。

2.大陸廠牌資通訊產品（含硬體、軟體及服務）禁止使用於公務環境：

- 公務用之資通設備不得使用中國大陸廠牌，且不得安裝非公務用軟體。
- 個人資通設備不得處理公務事務，亦不得與公務環境介接。
- 已使用或採購之中國大陸廠牌資通訊設備不得與公務環境介接。
- 如屬公告招標案件請於財物或勞務明細表『注意事項』中註明相關規定。
- 透過委外契約或場地租借使用規定，要求對外出租場域不得使用大陸廠牌資通訊產品。

（四）依臺教資(四)字第 1100122001 號函，學校使用資通系統或服務蒐集及使用個人資料注意事項，服務蒐集之個人資料者，應注意資料蒐集最小化、存取控制最小權限原則、雲端資通服務不宜使用共同編輯、傳輸之機密性、資料儲存安全並加密與訂定個人資料保存期限等事項。

（五）依據行政院院授科會前字第 1120059686 號函文，為使各機關使用生成式 AI 提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險，特就各機關使用生成式 AI 應注意之事項，訂定本參考指引。本參考指引包含總說明及 10 點規定，相關規定請參閱**(連結)**

二、資安通報事件與情資：

（一）7-Zip 驚爆嚴重漏洞！恐遭駭客繞過 Windows 安全機制

(資料來源：https://www.techbang.com/posts/121113-7-zip-windows)

本報導指出，7-Zip 以其高效的壓縮率、免費開源的特性以及支援多種壓縮格式等優勢，在全球 Windows 用戶中擁有廣大的使用者群。無論是個人用戶還是企業組織，都經常使用 7-Zip 來壓縮、解壓縮檔案。然而，近日 7-Zip 卻爆出了一個嚴重漏洞（CVE-2025-0411）。這個漏洞允許攻擊者繞過 Windows 的重要安全功能「網路標記」（Mark of the Web，簡稱 MotW），進而在使用者解壓縮惡意檔案時，不知不覺地執行惡意程式碼，對電腦系統造成嚴重威脅。7-Zip 的開發者 Igor Pavlov 已於 2024 年 11 月 29 日迅速發布了 24.09 版本，及時修復了這個安全漏洞。但由於 7-Zip 並沒有自動更新的功能，許多使用者可能仍然在使用舊版本，因此強烈建議所有 7-Zip 用戶儘快手動更新

到**最新的 24.09 版本**，以確保系統安全，遠離潛在的威脅。

（二）Veeam 修補本地端與雲端備份軟體漏洞，駭客可用中間人攻擊伎倆破壞系統

(資料來源：https://ithome.com.tw/news/167241)

本報導指出，備份與資料保護軟體廠商 Veeam，於2月4日揭露影響6款備份軟體的重大漏洞，並釋出修補。這個編號為 CVE-2025-23114的漏洞，存在 Veeam 備份產品使用的 Veeam Updater 元件，攻擊者可趁機透過中間人攻擊的手法，以 root 權限在受影響伺服器上執行任意程式碼，嚴重性等級達到9.0。Veeam 旗下使用 Veeam Updater 元件的產品，總共有6款備份軟體，目前只有 Veeam Backup for Salesforce 的3.1版與後續版本，仍受此漏洞影響，解決漏洞的辦法是將內含的 Veeam Updater 元件更新到7.9.0.1124版，用戶只需透過控制臺介面的 Checking for Updates 選項，讓系統自動執行更新即可。至於其他5款產品都是舊版本才含有這個漏洞，但新版本已完成修補，包括：

✓Veeam Backup for Nutanix AHV：6.0以後版本用不受影響，5.0與5.1版用戶須更新到新版本。

✓Veeam Backup for AWS：8.0以後版本不受影響，6a 與7版用戶須更新到新版本。

✓Veeam Backup for Microsoft Azure：7.0以後版本不受影響，5a 與6版用戶須更新到新版本。

✓Veeam Backup for Google Cloud：6.0以後版本不受影響，4與5版用戶須更新到新版本。

✓Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization：5.0版以後版本不受影響，3、4與4.1版用戶須更新到新版本。

（三）DeepSeek 的 AI 服務隱私防護遭質疑！資安業者指控恐將用戶輸入資料傳至中國國營電信業者

(資料來源：https://www.ithome.com.tw/news/167289)

本報導指出，中國 AI 工具 DeepSeek 號稱以低成本建置匹敵效能 ChatGPT 引起全球關注，並標榜開源、免費而受到歡迎，但背後由中國企業開發而可能隱含的資安風險也引起研究人員注意，繼有數家資安業者警告 DeepSeek R1模型能被輕易越獄而能用於助長犯罪，最近有資安業者提出新的發現，指出 DeepSeek 疑似與中國國營電信業者串連，而有可能讓中國政府直接存取相關資料。資安業者 Feroot Security 執行長 Ivan Tsarynny 接受媒體採訪時指出，他們的研究團隊於網頁版 DeepSeek AI 聊天機器人進行調查，發現這家公司在登入網頁嵌入重度混淆的程式碼相當不尋常，經過他們的解析，確認有隱藏功能，可將使用者的資料傳送到中國移動（China Mobile）的帳號登入網站 CMPassport.com。Ivan Tsarynny 進一步表示，雖然他們並未在嘗試登入的過程裡，看到 DeepSeek 明目張膽地直接將用戶資料傳送到中國移動，但他們無法完全排除 DeepSeek 會暗中進行傳輸的可能。此外，他們找到 DeepSeek 將使用

者資料傳送至中國伺服器的證據，雖然無法確定這些伺服器是否與中國移動有關，但已有資料流入其他中國 IT 平臺，其中一個是百度的廣告追蹤器。

三、智慧財產權新知：

經濟部智慧財產局變更「專利主題網」、「著作權主題網」及「智財活動通」等網站網址。

(資料來源：https://www.tipo.gov.tw/copyright-tw/cp-434-979992-a280f-301.html)

經濟部智慧財產局調整下列網站之服務網址：

1.「專利主題網」：https://www.tipo.gov.tw/patents-tw/

2.「著作權主題網」：https://www.tipo.gov.tw/copyright-tw/

3.「智財活動通」：https://www.tipo.gov.tw/act/

4.「商標主題網」：https://www.tipo.gov.tw/trademarks-tw/