國立高雄師範大學物聯網設備安全原則

113 年 11 月 20 日 113 學年度第 1 次資安、個資暨智財保護管理審查會議通過
113 年 12 月 18 日 113 學年度第 4 次行政會議通過

一、依據教育部 110 年 9 月 22 日臺教資(四)第 1100128345 號函規定及臺灣學術網路危機處理中心團隊製之 IoT 設備資安防護指南等相關規定，為降低物聯網設備(IoT 設備)造成資通安全威脅，特訂定本安全原則。

二、本原則所稱物聯網設備係指處理公務具網路連線功能之設備，包含無線網路基地台/無線路由器、網路攝影機、網路印表機、門禁設備、環控系統、數位播放器、無人機等。

三、單位應建立物聯網設備管理清冊，並至少每年更新一次。

四、單位應訂定物聯網設備安全性更新機制，以維持設備之整體安全性。

五、單位應確認所屬物聯網設備皆具備身分驗證機制，且禁止使用廠商預設帳密及弱密碼，密碼長度應配合中央主管機關規定，且應包含英文字母大小寫、數字與特殊符號要素之組合，並配合本校資安政策定期更換密碼。

六、單位應管制設備連線範圍，僅允許申請內部 IP 使用，不開放校外連線。惟若因業務需求需開放校外連線，應填寫 ISP-04-018-001 防火牆規則變更申請單，經圖書資訊處審核後始得開放連線。

七、若無法落實本原則第四、五、六點之安全控管規範，應建立補償性管控機制，如：限制網際網路連線能力、加強存取控制或進行網路連線行為監控等。若設備存在已知弱點且無法修補或更新，應訂定汰換期程。

八、依行政院規定，禁止使用大陸廠牌資通訊設備。

九、設備於採購前，應依據本原則進行評估。

十、採購物聯網設備時，應優先採購取得資安標章之物聯網設備，且應與設備供應商簽訂資訊安全相關協議，其內容應包含服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案等事項，以明確約定相關責任。

十一、　針對本校出租場域，應於委外契約或場地租借使用規定，明訂不得使用危害國家資安之產品（如大陸廠牌軟體、硬體及服務）。

十二、　本原則經資安、個資暨智財保護管理審查會議、行政會議通過，陳請校長核定後實施，修正時亦同。