各單位使用物聯網設備之資安管理注意事項

物聯網設備係指具網路連線功能並連線於網路上之嵌入式系統設備(內建小型作業系統)，常見如印表機、監視器、交換器、無線網路 IP 分享器、NAS 網路儲存設備(QNAP、Synology)、智慧電表、智慧 UPS 等。

所有類型設備

1. 若如監視器無連校外或從校外連入之需求，可詢問計網中心承辦人是否可使用 10.116 開頭之 IP 位址(僅限校內瀏覽)，避免使用 140.116 開頭之 IP 位址。
2. 更改出廠預設密碼或網路上搜尋的到的密碼，密碼複雜度應至少達 8 碼以上，至少含英文大小寫數字三種。
3. 帳號密碼若是請廠商設定，單位使用人也應跟廠商索取帳號密碼，確保有完整的設備存取權限。
4. 關閉設備不需要或使用不到之服務或協定，如 SSH、Telnet、SNMP、DNS、NTP 等。
5. 透過設備本身提供防火牆或存取控制功能(ACL)來限制只有同網段辦公室同仁才可連線該設備。
6. 定期進行設備軟韌體更新，建議可設定為自動更新。

印表機

1. 印表機掃描功能建議採用持隨身碟直接連接印表機掃描儲存使用。
2. 印表機掃瞄功能若有需要在電腦端架設 FTP 軟體：ftp utility  ，不可使用匿名登入：anonymous，請務必設定額外的帳號密碼。
3. 若使用匿名可登入之 FTP，可能被駭客放置病毒，如 info.zip、payment.scr，點下去電腦可能就被加密勒索了。
4. 請更改印表機網站管理頁面登入之預設密碼。
5. 以印表機本身內建防火牆或存取功能限制可列印之來源 IP 位址。

監視器

1. 更改預設密碼。
2. 限制可觀看監視器之來源 IP 位址。
3. 定期校時，確認時間正確。
4. 定期更新韌體。

NAS 網路硬碟－QNAP、Synology

1. 更改預設帳號密碼。
2. 限制可存取管理網頁之來源 IP 位址。
3. 定期更新韌體。
4. 建議可利用快照、備份等功能，將資料額外備份。或將資料另外備份至別處。
5. 網路儲存設備 NAS 經常因為定期更新韌體，又開放校外可存取頁面，發生被駭客入侵後，資料全部被加密。

IP 分享交換器

1. 更改預設帳號密碼，且不要開放外網也可連線到管理頁面。