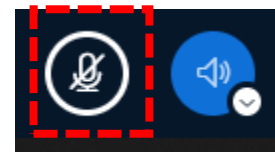




ISMS與資通安全 全校推動說明

請於聊天室簽到 例如：王大明簽到

請參加者關閉麥克風



國立暨南國際大學/計算機與網路中心

報告人：資通安全推動工作小組

**日期：111/05/11
111/05/16**

前言

本中心將於111年開始導入 資訊安全管理系統制度 (ISMS) ，以下會摘錄各程序書內較具體的事項，以及表單撰寫方式，請各位同仁務必遵守。



導入期程

111年ISMS第一階段導入：行政單位

112年ISMS第二階段導入：教學單位

教育訓練 5月11日下午、5月16日早上（各3小時）

教育訓練測驗5/20日前完成

本次行政單位需進行資訊系統盤點及IoT盤點

5/16日後計中會陸續和各單位約時間帮大家看盤點情形，再進行後續導入



只要做資安就不會有資安事件？

只要綁安全帶就不會出車禍？

降低風險和損失



資安事件發生時

發現人員應通報單位主管及計網中心



面對稽核人員

他們是不太熟的～友好朋友

友善、據實回答、不發散問題



ISMS具體事項宣導-資安政策

- 本校已於110年成立資通安全推動委員會，由主秘擔任資通安全長，一級主管擔任委員，計網中心主任擔任執行秘書。
- 第一階段將導入全校行政單位，由一級單位推派人員擔任資安窗口
- 本校資訊安全政策，宣告全校同仁及委外廠商，應請廠商簽署「[PIMS-2-015-03委外廠商人員保密切結書](#)」
- 雲端硬碟網址<https://reurl.cc/q5Nk13>
(資訊安全政策、委外廠商人員保密切結書)



ISMS具體事項宣導-雲端硬碟登入方式

登入雲端硬碟



和webmail一樣的帳號、密碼



The screenshot shows the 'Cloudmail - 教職員工及公務' login page. The URL 'mail.ncnu.edu.tw' is prominently displayed. Below the header, there are navigation tabs: 'home', 'webmail 說明', 'cloudmail 說明', 'nopam 說明', and '問題集'. The main content area is titled '暨大教員工及公務Cloudmail郵件系統(Google Mail)'. It features a login form with fields for 'Login name/教職員公務帳號:' and 'Password/密碼:', followed by a 'Login/登入' button. A red box highlights the login fields. Below the form, there are three reminders: (1) First-time login requires enabling the account and changing the password; (2) If unable to login after 180 days, refer to the 109 academic year email account password policy; (3) For account security, users should check their device and login time. At the bottom, there are links for '首次登入(Enable Account)', '忘記密碼(Forgot Password)', and 'Email故障報修(Fault Report)'. On the right side, there is a '相關連結' (Related Links) section with a link to '設定第二信箱' (Set up second mailbox) and other useful links. The footer includes the NCNU logo and copyright information.

Cloudmail - 教職員工及公務
mail.ncnu.edu.tw

home webmail 說明 cloudmail 說明 nopam 說明 問題集

暨大教員工及公務Cloudmail郵件系統(Google Mail)

Login name/教職員公務帳號: @ncnu.edu.tw

Password/密碼: Login/登入

提醒(1):首次登入請點選下方的"首次登入"超連結啟用帳號及變更密碼
提醒(2):自2020/08/01起,若您超過180天以上沒變更密碼以致無法登入,請參考109學年電子郵件帳號密碼部分之資安新措施!!+Q and A
提醒(3):為維護cloudmail 帳號安全,請以手機或PC隨時查看最近使用過的裝置及登入時間點!!
[首次登入\(Enable Account\)](#)|| [忘記密碼\(Forgot Password\)](#)|| [Email故障報修\(Fault Report\)](#)

If this is your first time logging in, please click the "Enable Account" hyperlink below to enable your account and change your password.

相關連結

- [設定第二信箱](#)
- [郵件啟用\(Enable Account\)](#)
- [忘記密碼\(Forget Password\)](#)
- [故障報修\(Fault Report\)](#)
- [暨大電子郵件服務網](#)
- [暨大校園保護智慧財產權專區](#)
- [暨大首頁](#)

國立暨南國際大學
National Chi Nan University
© Copyright 國立暨南國際大學 計算機與網路中心諮詢組

ISMS具體事項宣導-資產管理

- 建立單位資訊系統清冊（有資訊系統者）
- 建立單位IoT設備清冊
- 設備報廢，硬碟資料需進行抹除或實體破壞
 - 可自行處理或請計中協助
- 如何填寫清冊下堂課會說明，
- 後續由計中同仁至各單位各別協助



ISMS具體事項宣導-人員管理

- 本校同仁任職需簽訂「[NCNU-ISMS-D-045-人員個人資訊暨資訊安全保密切結書](#)」，且服務期間皆應遵守本校規範，於業務上所獲知之機密資訊，非經授權不得對外透露。
- 人員離（調）職時需移除相關資源之存取權限
- 委外廠商，應簽署「[PIMS-2-015-03委外廠商人員保密切結書](#)」
- 各項文件由各單位自行妥善保管
- 雲端硬碟網址<https://reurl.cc/q5Nk13>



ISMS具體事項宣導-教育訓練

- 一般使用者及主管：

每人每年接受三小時以上之一般資通安全教育訓練

- 為確保教育訓練執行之成效，可採行隨堂抽問、案例討論、習題演練、
隨堂測驗...等方式進行成效評估
- 所以我們也有隨堂測驗喔！在下節課



ISMS具體事項宣導-教育訓練

- 其他課程資源

E等公務園-學習平台 提供線上課程、評量 可作為教育訓練時數

https://elearn.hrd.gov.tw/mooc/course_share.php?code=d29c0100e87607b16ee886f603f9fd17

https://elearn.hrd.gov.tw/mooc/course_share.php?code=f418946aa77c88bf821b61fa96dd0250

https://elearn.hrd.gov.tw/mooc/course_share.php?code=d29c0100e87607b16ee886f603f9fd17

https://elearn.hrd.gov.tw/mooc/course_share.php?code=6e4e4a213d8679ce7736d02a21560faa

https://elearn.hrd.gov.tw/mooc/course_share.php?code=be5a62bfddedaf68288facab3acb8b8d

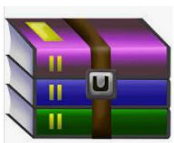
https://elearn.hrd.gov.tw/mooc/course_share.php?code=728ddd32406273363179f9a3c7b250f5



ISMS具體事項宣導-辦公環境

- 禁止使用或下載未經授權或與業務無關之軟體。

破解版WinRAR



- 使用者發現電腦中毒、勒索軟體、不明惡意軟體，請通知計中

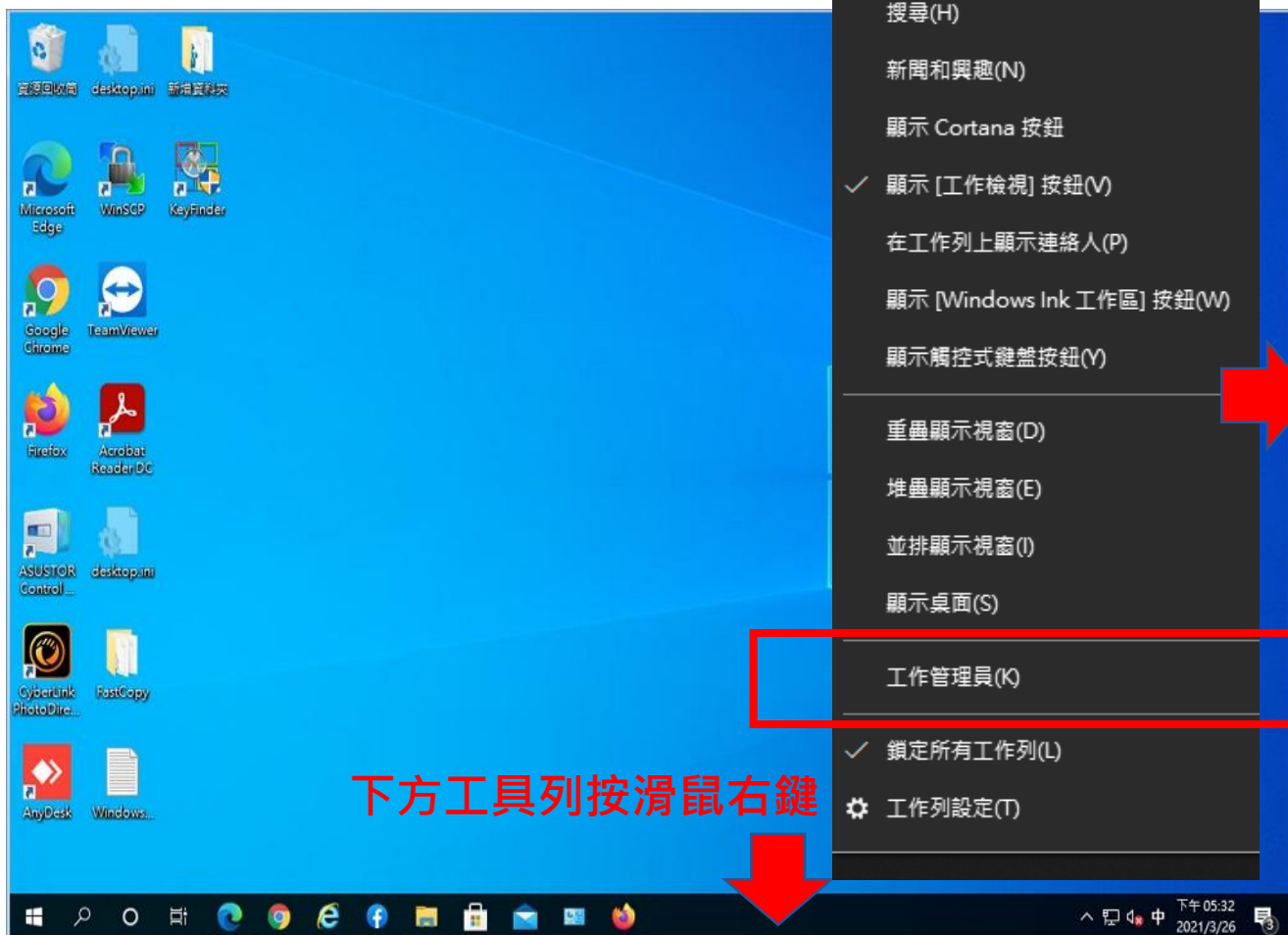
電腦中毒常見現象

- 電腦變慢卡卡的
- 瀏覽網頁時跳出奇怪的視窗
- 電腦開機速度變慢
- 檔案突然無法開啟



ISMS具體事項宣導-辦公環境

電腦變慢卡卡的？



工作管理員

檔案(F) 選項(O) 檢視(V)

處理程序 效能 應用程式歷程記錄 開機 使用者 詳細資料 服務

名稱	狀態	16% CPU	78% 記憶體	0% 磁碟	0% 網路	3% GPU	GPU 引擎	電源用量
> 工作管理員		1.3%	30.4 MB	0 MB/秒	0 Mbps	0%		非常低
桌面視窗管理員		1.3%	87.4 MB	0 MB/秒	0 Mbps	2.3%	GPU 0 - 3D	非常低
> Runtime Broker		0%	1.9 MB	0 MB/秒	0 Mbps	0%		非常低
> Runtime Broker		0%	3.9 MB	0 MB/秒	0 Mbps	0%		非常低
> Microsoft Text Input Application		0%	6.0 MB	0 MB/秒	0 Mbps	0%		非常低
> Cortana (2)		0%	0.7 MB	0 MB/秒	0 Mbps	0%		非常低
> Google Chrome (10)		0%	541.0 MB	0.1 MB/秒	0 Mbps	0%		非常低
> Windows 殼層體驗主機		0%	0 MB	0 MB/秒	0 Mbps	0%		非常低
> LINE (32 位元) (5)		0.2%	78.1 MB	0 MB/秒	0 Mbps	0%		非常低
> Runtime Broker		0%	1.9 MB	0 MB/秒	0 Mbps	0%		非常低

較少詳細資料(D) 結束工作(E)



ISMS具體事項宣導-辦公環境

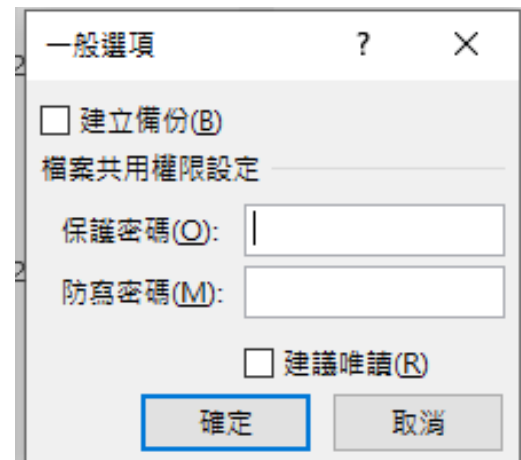
- 定期(至少14天內)清理個人電腦的資源回收筒，以確保已經刪除的重要資料不會因為遺留在資源回收筒未清理，而遭未經授權之使用。
- 避免將具有個資文件放置在桌面(實體或電腦桌面)
 - 檔案加密



ISMS具體事項宣導-辦公環境

文件如何加密？

- 將本來的 Word 或 Excel 檔案另存新檔



ISMS具體事項宣導-辦公環境

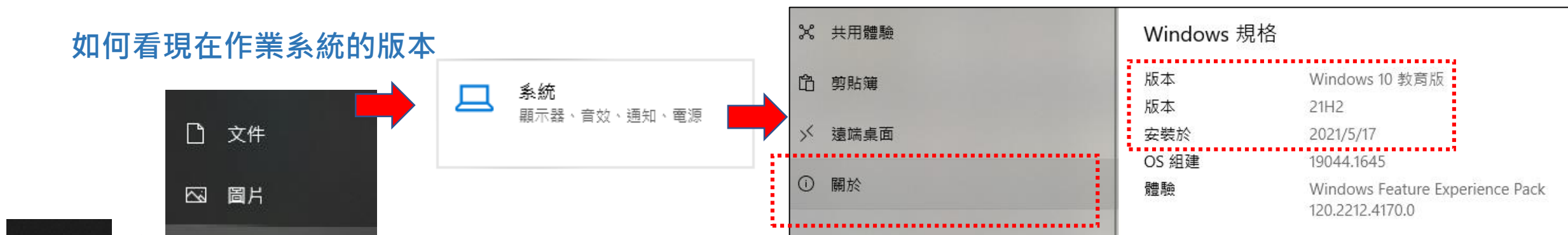
- 電子郵件（外部圖片關閉、社交工程）
- 關閉電子郵件預覽功能方式請參考「[社交工程攻擊-郵件預覽關閉文件](#)」，文件中有 Gmail、webmail、Outlook 的關閉方式
- 個人電腦、伺服器、筆電，需採用密碼保護（登入），不使用或離開座位時應鎖定、登出 (加入CCSERVER網域就已經有設定)
- 雲端硬碟網址 <https://reurl.cc/q5Nk13>



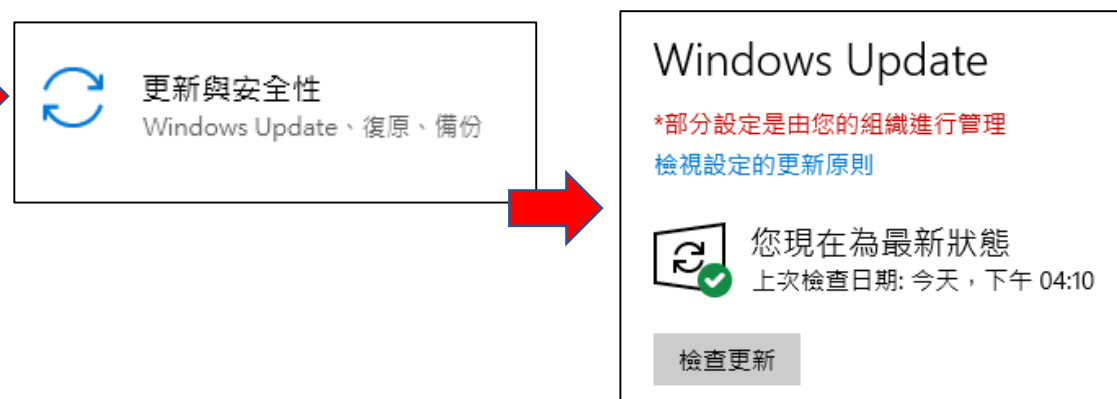
ISMS具體事項宣導-辦公環境

- 作業系統應更新至原廠支援版本(目前最低為Win10-20H2版本)

如何看現在作業系統的版本



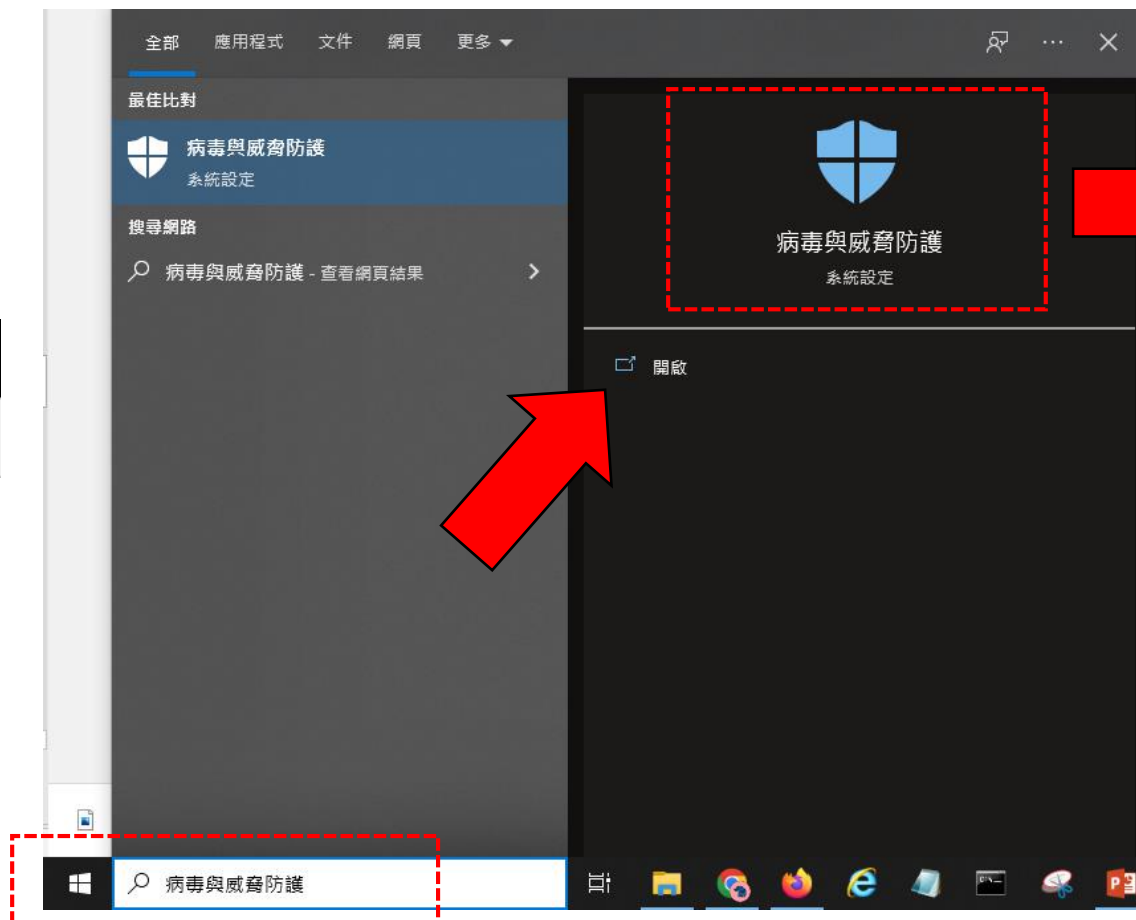
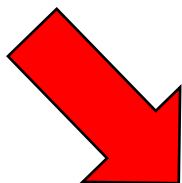
如何看作業系統的更新狀態



ISMS具體事項宣導-辦公環境

- 應安裝資安防護軟體，並定期更新。(本校防毒資源)

放大鏡-搜尋



McAfee



Sophos



F-Secure

ISMS具體事項宣導-遠端作業

- 內部人員如有遠端連線作業需求，應告知並經單位主管同意
- 外部人員連線前應填寫「[NCNU-ISMS-D-044-外部人員遠端連線申請表](#)」
- 遠端連線軟體不可常駐於系統，僅可於約定之連線時間開啟
- 外部人員進行遠端連線作業時，業務負責人應於電腦前監看其操作，必要時應介入
- 開放外部人員使用遠端連線軟體時應設定專屬帳號及一次性密碼，專屬帳號僅於約定時間開啟



ISMS具體事項宣導-帳號及權限管理

- 使用權限請以執行業務及職務所必要的**最低資源存取授權為限**
- 伺服器主機及網路設備應指定負責人，負責人無法進行管理時應由代理人負責
- 視狀況授與適當存取權限，並**避免共用帳號**
- 新購置設備，安裝完成後應立即**更新預設之密碼**，並**刪除或關閉不必要之帳號**
- 密碼設置，至少**8碼**，且應符合**密碼設置原則**，並避免使用記錄密碼功能



ISMS具體事項宣導-帳號及權限管理

密碼總是強度不夠？太難又記不起來？

- 密碼123456 弱密碼
- 一個密碼打天下
- 本校密碼原則8碼以上+英文+數字+特殊符號

123456 → 1 23 456 → 12 345 6

1@23 # 456 → A1@23 # 456B

數字拆成不同組合
加上特殊符號及英文





中場休息



物聯網(IoT)設備及資訊系統 盤點說明

國立暨南國際大學/計算機與網路中心

報告人：資通安全推動工作小組

日期：111/05/11

物聯網(IoT)設備說明



物聯網設備相關指引-何謂物聯網 (IoT)

- 裝置可以自行透過網路去做資訊的讀取及傳遞，也可透過網路接收資訊並執行某些動作。
 - 網路印表機/多功能事務機：可聯上網路之列印、影印及掃描設備。
 - 網路攝影機/聯網監視系統：可聯上網路之攝影機、監視系統。
 - 門禁/刷卡系統：提供門禁開關、刷卡識別身份之聯網裝置。
 - 環控系統：提供監控環境狀態，如溫度、濕度或發電量等聯網設備。
 - 無線基地台/無線路由器：提供無線網路分享及聯網功能。
 - 多媒體控制器/聯網電視：提供即時字幕或影片播放，或提供聯網功能之電視機（牆）。
 - 網路儲存裝置（NAS）：提供自建網路磁碟機或其他網路服務之整合設備。
 - 其他：上述未列入但有透過無線或有線網路聯網之裝置。



物聯網設備相關指引-物聯網設備的生命週期

- 規劃：
 - 依需求進行相關評估及規劃。
- 採購：
 - 應配合國家政策，優先採購物聯網資安認證2星標章之產品。
 - 依資訊設備採購相關規範進行採購。（目前規範**不得**採購大陸廠牌產品）
- 安裝：
 - 設備安裝前應申請固定IP位址，不得使用動態主機設定協議（DHCP）。
 - 固定IP位址非必要不得使用公用IP位址（Public IP）。
 - 設備安裝施工需遵守相關場域安全規範。



物聯網設備相關指引-物聯網設備的生命週期（續）

- 設置：
 - 設備第一次啟用，需進行密碼變更，不得使用預設密碼；如設備可變更管理者帳號，宜同時變更預設帳號。
 - 密碼規則需符合本校資安要求。
 - 如物聯網設備需連線控制主機，則物聯網設備及控制主機之預設密碼皆須變更。
 - 檢視設備是否有相關資訊安全弱點，如有相關更新，需更新到可運作之最新版本。
 - 設備宜控管非必要連線之IP，非必要之服務宜關閉。



物聯網設備相關指引-物聯網設備的生命週期（再續）

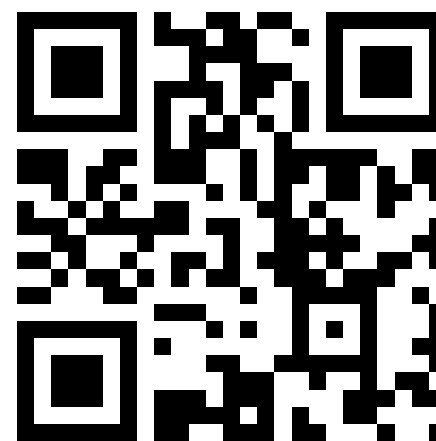
- 使用：
 - 具有掃描傳送功能之設備，優先設定使用電子郵件進行掃描文件傳遞。
 - 如掃描至公務用電腦內，需於該公務用電腦內設定僅允許設備IP位址連線至該服務。
 - 物聯網設備每年至少應進行一次盤點作業，並於新增、異動或移除設備時進行物聯網設備盤點表維護。
 - 定期檢視物聯網設備安全性更新。
- 報廢：
 - 設備中含有可存放資料之裝置時，需進行資料抹除或時破壞之動作。



物聯網設備相關指引-物聯網設備盤點表

編號	類別	設備廠牌	廠牌國別	設備型號	IP或網址	韌體/系統版本	放置地點/單位代碼	管理人 / 財產保管人	是否使用預設密碼
1	<p>網路印表機/多功能事務機</p> <p>網路攝影機/聯網監視系統</p> <p>門禁系統</p> <p>環控系統</p> <p>無線基地台/無線路由器</p> <p>多媒體控制器/聯網電視</p> <p>網路儲存裝置</p> <p>其他</p>	<p>類別</p> <p>網路印表機/多功能事務機：可聯上網路之列印、影印及掃描設備。</p> <p>網路攝影機/聯網監視系統：可聯上網路之攝影機、監視系統。</p> <p>門禁/刷卡系統：提供門禁開關、刷卡識別身份之聯網裝置。</p> <p>環控系統：提供監控環境狀態，如溫度、濕度或發電量等聯網設備。</p> <p>無線基地台/無線路由器：提供無線網路分享及聯網功能。</p> <p>多媒體控制器/聯網電視：提供即時字幕或影片播放，或提供聯網功能之電視機（牆）。</p> <p>網路儲存裝置（NAS）：提供自建網路磁碟機或其他網路服務之整合設備。</p> <p>其他：上述未列入但有透過無線或有線網路聯網之裝置。</p>							

- 物聯網設備盤點表：<https://reurl.cc/KbMbDy>



資訊系統盤點說明

- 資訊系統盤點清冊：<https://reurl.cc/ErGpxv>



資訊系統盤點

1.系統名稱 (例：校務系統、電子郵件系統) *

簡答文字

2.系統屬性 *

☐ 行政

☐ 業務

☐ 兼具行政/業務

- 行政類：

指機關內部輔助單位之業務,如：人事、薪資等

- 業務類：

指機關內部業務單位之業務,如：對外的報名系統、自建單位網頁

- 兼具行政/業務:

如:教務系統



資訊系統盤點

3.建置方式 *

- ☐ 本機關委外開發
- ☐ 本機關租用服務
- ☐ 本機關購置套裝軟體
- ☐ 本機關自行開發
- ☐ 主管/上級/其他機關提供
- ☐ 其他 (請填寫3-1題)

3-1.建置方式補充說明：第3題選填『其他』者才需填寫

簡答文字

- 建置方式：
本機關自行開發
購置
租用



資訊系統盤點

4.系統主管機關（例：國立暨南國際大學、教育部等..）*

簡答文字

.....

5.系統管理者(部門/單位 例：計算機與網路中心/網路組))*

簡答文字

.....

6.系統使用者(部門/單位 例：圖書館、註冊組、全機關)*

簡答文字

7.主機是否設置於機關內*

☐ 是

☐ 否



資訊系統盤點

8.是否含機敏資訊 *

- ☐ 是
- ☐ 否 (第9題請選"無機敏資訊")
- ☐ 其他機關維運 (本校以外的機關)

9.機敏資訊以非明文方式儲存 ? (是/否/無機敏資訊/其他機關維運) *

- ☐ 是
- ☐ 否
- ☐ 無機敏資訊

10.機敏資訊類別(例：身份證字號、學號、等個人資料，無則填寫"無" *

簡答文字

機敏資訊：個人資料



資訊系統盤點

11.是否與民生權益相關(民生權益係指考試、福利、醫療等) *

- ☐ 是
- ☐ 否
- ☐ 其他機關維運 (本校以外的機關)

12.防護需求等級-機密性 *

普-發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。

中-發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。

高-發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。

資訊系統盤點

13.防護需求等級-完整性 *

選擇

普-發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竊改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。

中-發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竊改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。

高-發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竊改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。

選擇

資訊系統盤點

14.防護需求等級-可用性 *

選擇

普-發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。

中-發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。

高-發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。

資訊系統盤點

15.防護需求等級-法律遵循性 *

普-其他資通系統設置或運作於法令有相關規範之情形。

中-如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。

高- 如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。

資訊系統盤點-何謂防護需求等級

防護需求等級是以

「機密性」、「完整性」、「可用性」、「法律遵循性」四個構面下去評估，
每個構面分為普、中、高三種等級，取四個構面中最 "高等級為系統安全等級"

16.防護需求等級 (請填寫12-15題中最高等級)

☐ 普

☐ 中

☐ 高

資訊系統盤點

17.建置廠商（系統建置方式為 本校自行維運者請填「國立暨南國際大學」，「主管/上級/其他機關」者請填「其他機關維運」，為「本機關購置套裝軟體」者請填「套裝軟體」 *

簡答文字

18.維運廠商（系統維運方式為 本校自行維運者請填「國立暨南國際大學」，「主管/上級/其他機關」者請填「其他機關維運」，為「本機關購置套裝軟體」者請填「套裝軟體」， *

簡答文字

資訊系統盤點

19.最大可容忍中斷時間(單位"小時"請填數字)，請自行評估該系統對於機關之最大可容忍中斷時間 *

簡答文字

20.系統是否對外（係指以網際網路即可連線檢視或使用之系統） *

☐ 是

☐ 否

課後測驗

- 需完成課後測驗，才算取得資訊安全時數
- 請於5/20日前完成測驗

測驗連結：<https://reurl.cc/e3W0ZK>

