國立體育大學

國立體育大學
資訊安全基本認知

編輯者:王永彰
第六版修編日期:113.8.16
資訊中心審查日期：113.8.16
資訊發展暨安全管理委員會審查日期:113.8.21

一、宗旨

為維護本校資訊安全，特收錄每位同仁皆應注意之重點資訊安全行政規定，彙整為本基本認知，以利同仁遵循。根據本校資訊安全政策，推廣是「資訊安全人人有責」。這代表每位同仁都需具備資訊安全的基礎認知，遵守相關的網路與資訊安全法規，以確保校內資訊相關設備和系統得到有效的安全防護。我們的目標是共同努力，確保每個人都承擔起維護校內資訊安全的責任。

二、資訊安全目標

(一) 資訊安全事件每年發生次數不得**超過三次**。

(二) 每人每一年應接受三小時以上資訊安全通識教育訓練。

(三) 各單位有資訊系統外包之承辦人員，應接受資安專業訓練。

三、資訊設備使用管理

(一)公務配發之可攜式設備(筆記型電腦、行動裝置等)及儲存媒體(行動硬碟、隨身碟、網路儲存裝置等)應妥適保管，非因公務需要不得攜出辦公處所。

(二)公務配發之可攜式設備不得透過公開(無需認證)之無線網路傳輸敏感性資料，若有連結外部網路或設備之情形，該設備於攜回或連結校務資訊作業環境前，應進行掃毒或系統還原。

(三)私人之資訊設備不得連結校務資訊作業環境及處理機密或敏感性公務資料。

(四)使用者離開電腦時，應關閉螢幕電源或啟動電腦鎖定功能；電腦應設定超過**十五分鐘**未使用，進入螢幕密碼保護或強制登出。

(五)電腦名稱修改：全校電腦名稱需修改為(分機-帳號)，例如：1427-ismc9853。

四、電腦軟體使用管理

(一)資訊設備所需軟體，安裝前應確認已取得合法授權。

(二)電腦可以下載使用正版通訊軟體(如LINE)，但不得用於傳送公文等公務，僅用於聯繫窗口或回覆加密密碼的異地通知之用，用畢收回。

(三)未經各單位主管核准，不得使用私有、免費或共享軟體；經核准使用之軟體已逾授權期限者，應立即刪除。

(四)資通安全弱點通報系統(VANS)安裝：依據「資通安全責任等級分級辦法」之「資通安全責任等級C級之公務機關應辦事項修正規定」，安裝VANS程式以便將個人電腦軟硬體版本資訊，定期上傳數位發展部，以便確保全國所有政府學校機關之軟硬體符合資訊安全要求。

五、資料管理

(一)保管機密或敏感性之電腦資料或檔案者，應將檔案加密或置於設有加密保護之資料夾。

(二)機密或敏感性之資料及記載電腦檔案相關資訊等文件，不得隨意放置，下班時應上鎖或以其他方式妥為收存。

(三)定期備份重要資料及檔案。

(四)因業務需要於公務電腦建立之個人資料檔案，應**每年至少一次檢視**有無保留之必要。

(五) 機密性資料不應透過網路上傳輸，對於敏感性檔案，應在傳輸之前進行加密處理

(六)使用線上表單(如GOOGLE)收集個資時，需先寫明**個資宣告**用途(如:此筆資料僅於此次活動保險使用，活動結束後銷毀)。

(七) 使用線上表單(如GOOGLE)收集個資時，盡量**最小化收取的資料內容**，避免個人資料保存之責任。

六、網路使用管理

(一)公務電腦(含筆記型電腦/平板電腦)及物聯網的相關設備(附錄)若因業務需求更改固定式IP 位址，需經**各單位主管核准後，並向資訊中心申請及備查。**(網路服務申請表)

(二)公務電腦(含筆記型電腦/平板電腦/可攜式電腦儲存媒體) 及物聯網的相關設備需架設無線網路等相關對外連線設備，若有業務需求應規劃防護措施並單位主管核准。並送資訊中心申請及備查。

(三)不得使用點對點（Peer-to-Peer, P2P）分享軟體

(四)各單位承辦人需定期盤點單位內(含實驗室)公務電腦以及物聯網相關設備資訊（數量、IP位址)，造冊後單位主管覆核，並送資訊中心備查。(相關表單請參閱附錄二）

七、帳號及密碼管理

(一)密碼應設定八碼以上，且至少自英文大寫、英文小寫、數字及特殊符號，擇取三類依複雜性原則組成，並**避免**設定與使用者相關資料（生日、身分證字號、單位簡稱、電話號碼、車牌等)。

(二)密碼應至少**每年更換一次**。

(三)使用者識別碼及密碼應妥善保管，不得張貼於公務電腦、螢幕或其他容易洩密之場所。

(四)系統或瀏覽器**應取消密碼自動記憶功能**，避免密碼遭擷取或竊用。

八、病毒及駭客防範

(一)防毒軟體之病毒碼應為最新版本（日期最長不得超過一週，如有問題立即聯絡資訊人員）。

(二)不得開啟及下載來路不明之連結或檔案，以避免遭受木馬或病毒軟體植入。

(三)使用儲存媒體前，應先執行病毒掃瞄檢查，以防駭客藉由儲存媒體植入後門程式。

(四)公務電腦(含筆記型電腦)及伺服器應關閉USB儲存裝置自動執行設定(Auto Run)，以防駭客藉由USB儲存裝置植入後門程式。

(五)防毒軟體安裝:校內電腦皆需安裝指定之防毒軟體(eset，資訊中心/常用免費軟體下載)

九、電子郵件管理

(一) 同仁收發公務所需資訊應使用公務電子信箱，不得使用非公務信箱。

(二) 公務名片所載電子信箱聯絡資訊，應以公務信箱為準。
(三) 非因業務需要不得設定自動傳送電子郵件讀取回條。
(四) 收取電子郵件規定如下：
1.來路不明郵件(非公務郵件)勿任意開啟，應逕行刪除。
2.關閉自動預覽再開啟郵件閱讀。
3.以純文字讀取模式開啟郵件。
4.傳送敏感性資料，應啟動加密機制。
5.收信時應先確認發信者電子郵件帳號是否遭偽冒，必要時應直接聯繫發信者確認。

十、資訊安全事件通報：資訊中心發現或察覺可疑資安事故、異常事件或安全弱點等情事，應**立即向本校資安通報窗口(資訊中心)通報**。

十一、附錄

附錄一 物聯網設備介紹

物聯網設備(直接使用RJ45進行連線之設備與本身有無線網路卡)

1.網路印表機	提供紙張輸出功能 (範例:印表機、多功能事務機、影印機等)
2.網路攝影機	提供影像錄製功能 (範例:攝影機)
3.門禁設備	提供門禁開關功能 (範例:指紋機、指掌靜脈機、門禁卡機等)
4.無線網路基地台/無線路由器	提供無線網路分享功能 (範例:無線網路基地台、無線路由器)
5. 環控系統	提供監控機房溫度或濕度功能 (範例:機房溫度監控伺服器)

附錄二 物聯網設備盤點表

國立體育大學 電腦及物聯網設備盤點表

盤點單位:

※請填覆單位內所有的「公務電腦」、「網路印表機」、「門禁設備」、「網路攝影機」、「無線網路基地台/無線路由器」、「環控系統」等物聯網設備，項次不足請自行增加。
※檢測標的為下列可直接使用RJ45或無線網路卡進行連線之設備:

□ 公務電腦:提供業務需求(筆記型電腦、個人電腦)

□ 印表機:提供紙張輸出功能 (範例:印表機、多功能事務機、影印機等)

□ 網路攝影機:提供影像錄製功能 (範例:攝影機)

□ 門禁設備:提供門禁開關功能 (範例:指紋機、指掌靜脈機、門禁卡機等)

□ 無線網路基地台/無線路由器:提供無線網路分享功能 (範例:無線網路基地台、無線路由器)

□ 環控系統:提供監控機房溫度或濕度功能 (範例:機房溫度監控伺服器)

編號	設備類別	無此類設備	項次	設備名稱	網址/IP	廠牌型號	作業系統	設備放置位置
範例1	公務電腦		1	個人電腦	192.168.1.1			行政405辦公室
範例1	網路印表機	□	1	HP網路印表機	192.168.5.101	HP LaserJet 4300		行政405辦公室
			2	HP網路印表機	192.168.5.102	HP LaserJet 4400		行政405辦公室
	網路攝影機	□	1	AXOO網路攝影機	192.168.10.11	AXOO P1354		行政405辦公室
			2	AXOO網路攝影機	192.168.10.12	AXOO M1033_W		行政405辦公室
	門禁設備	□	1	OO科技門禁卡機	192.168.20.11	OO科技 KEEP-301		行政405辦公室
			2	OO科技門禁卡機	192.168.20.12	OO科技 KEEP-301		雲五館3樓討論室二

	無線網路基地台/無線路由器	■						
	環控系統	■						

編號	設備類別	無此類設備	項次	設備名稱	網址/IP	廠牌型號	作業系統	設備放置位置
範例2	網路印表機	□	1	HP網路印表機	192.168.5.101	HP LaserJet 4300		行政405辦公室
		□	2	HP網路印表機	192.168.5.102	HP LaserJet 4400		行政405辦公室
	網路攝影機	□	1	OOS網路攝影機	192.168.10.11	OOS P1354		行政405辦公室
			2	AOO網路攝影機	192.168.10.12	AXOO M1033_W		行政405辦公室
	門禁設備	■						
	無線網路基地台/無線路由器	□	1	ARUBA無線網路基地台	192.168.10.13	ARUBA AP-315		行政405辦公室
			2	ARUBA無線網路基地台	192.168.10.14	ARUBA AP-315		行政405辦公室
	環控系統	□	1	網路型溫濕度計	10.5.1.217	T&D TR-72W		行政405辦公室
			2	網路型溫濕度計	10.5.1.218	T&D TR-72W		行政405辦公室

編號	設備類別	無此類設備	項次	設備名稱	網址/IP	廠牌型號	作業系統	設備放置位置

1								
		□						

附錄三 資通系統盤點表

分級說明	機密性 C	數值1:一般:此資訊資產無特殊之機密性要求 數值2:限閱:此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位使用 數值3:敏感:此資訊資產僅供內部相關業務承辦人員存取 數值4:機密:此資訊資產所包含資訊為組織或法律所規範的機密資訊
	完整性 I	數值1:資產本身完整性要求極低 數值2:資產本身具有完整性要求，但是完整性被破壞不會對組織造成傷害 數值3:資產具有完整性要求，且完整性被破壞會對組織造成傷害，但不至於太嚴重 數值4:資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止
	可用性 A	數值1:資訊資產容許失效≧3天 數值2:8小時≦資訊資產容許失效＜3天 數值3:4小時≦資訊資產容許失效＜8小時 數值4:資訊資產容許失效＜4小時
	單位承辦人	(請在左邊簽名，用自己的帳號輸入名字就可以)
	單位主管	(請在左邊簽名，用自己的帳號輸入名字就可以)

以資訊中心為例:

流水號	對外網路位址IP	資通系統名稱	業務單位	機密性	完整性	可用性	資產價值	備註
1	192.83.181.6	SQLServer資料庫	資訊中心	1	2	2	2	限閱，僅供學校內部人員使用
				2	2	2	2	單位自評
2	192.83.181.11	憑證主機	資訊中心	1	1	1	1	
				1	1	1	1	單位自評
4	192.83.181.16	MRTG	資訊中心	1	1	1	1	
				1	1	1	1	單位自評

★會將各處室需要資通系統盤點的部分，寄至承辦人與主管信箱。

附錄四 核心資通系統盤點表

資通系統安全等級評估表

安全等級	普	中	高
分類	1-2	3	4
機密性	若未經授權之資訊揭露，在機關營運造成有限負面影響	若未經授權之資訊揭露，在機關營運造成嚴重負面影響。	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響
完整性	若未經授權之資訊修改或破壞，在機關營運造成有限負面影響	若未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響	若未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響
可用性	若資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之有限負面影響	若資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響	若資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響
法律規章遵循性	若系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之有限負面影響	若系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之嚴重負面影響	若系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之非常嚴重或災難性負面影響

參考資料：資通安全責任等級分級辦法-附表九-資通系統防護需求分級原則

以資訊中心為例:

文件等級：內部使用

國立體育大學核心資通系統安全等級評估表

「資訊中心 NTSUONE/AD/校務行政資訊系統」

業務屬性：□學術專案類■行政類□業務類　　填表日期：112/11/09

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	中	中	中	中
		資訊系統安全等級：		中

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	若未經授權之資訊揭露，在機關營運造成嚴重負面影響。
	異動		
2. 完整性	初估	中	若未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響。
	異動		
3. 可用性	初估	中	若資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響。
	異動		
4. 法律遵循性	初估	中	若系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之嚴重負面影響。
	異動		

資訊中心		資通安全長
承辦人	主管	簽章
技士王永彰	資訊中心主任黃雲龍 11/17	國立體育大學副校長黃東治 11/21

★會將各處室需要的核心資通系統盤點的部分，寄至承辦人與主管信箱。

資通安全內部稽核表第11、12項資通教育訓練時數，為幫助各單位同仁查找訓練時數方便，特出此教學手冊，請參閱。

P1.開啟學校ee-class→登入→點選我的首頁

ee-class入口:https://eeclass2.ntsu.edu.tw/

點選資訊安全與個人資料保護實務→

一般教職人員的資安通識課每年加總3小時↓

課程活動

標題	期限	完成條件	學習成果	完成
一、資安管理與個資保護通識教育				
主管、同仁、教師				
1. 全校落實資通安全管理之優先執行策略	-	閱讀 1 次	08:03	
2. 20230829_國體大-資訊安全通識教育part1(全校)	-	閱讀 1 次	02:29	
3. 20230829_國體大-資訊安全通識教育part2(全校)	-	閱讀 1 次	25:35	
4. 資安管理-單位主管責任(業務單位主管)	-	閱讀 1 次	09:28:00	
5. 資安管理-系統委外承辦人員責任(業務單位)	-	閱讀 1 次	03:21:27	

專業資安人員(各處室資安窗口需加上)的專業教育訓練每兩年加總3小時↓

二、資安管理專業教育訓練

資訊人員(資通系統業務單位與委外承辦人、資訊系統管理與開發)				
1. 20230919-資安稽核實務-謝棟梁副主任-(資訊人員)	-	閱讀 1 次	00:25	
2. 教育體系資安稽核重點 - 策略面(資安長必讀)	-	閱讀 1 次	03:09:28	
3. 高教深耕資安專章評核項目提報佐證重點(資安委員)	-	閱讀 1 次	-	-
4. 教育體系稽核重點 - 內稽執行(資安專職)	-	閱讀 1 次	16:59:17	
5. 教育體系稽核重點 - 管理面與技術面(資安專職)	-	閱讀 1 次	09:16:26	
6. 安全系統發展生命週期SSDLC- (系統開發與管理專業)	-	閱讀 1 次	13:54:24	
7. 資安風險評鑑方法- (系統開發與管理專業)	-	閱讀 1 次	18:18:54	

接下頁，有第二種方式

P2.進入學校首頁→教職員→校務資訊系統→登入→點選歷程系統暨課程地圖新功能統

校務資訊系統入口:https://one.ntsu.edu.tw/portal/

點選報表統計

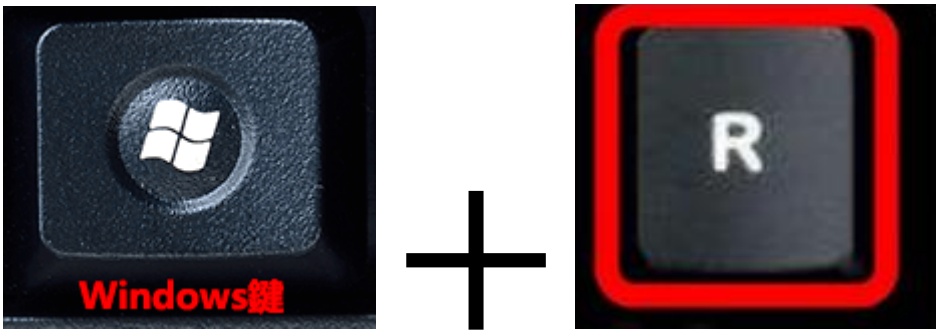
點選活動與參與清單

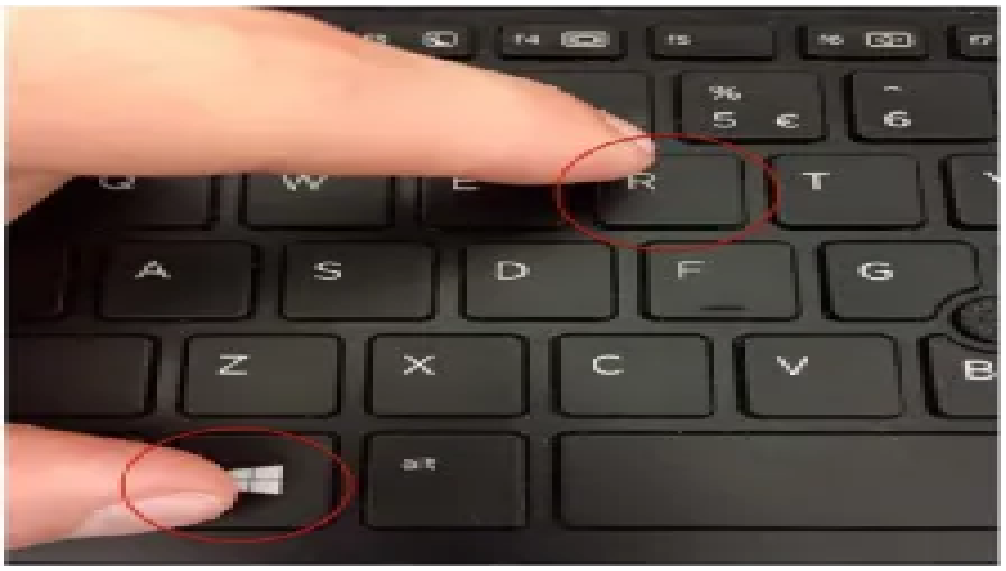
如下圖選取搜索欄位

按匯出即可看到時數

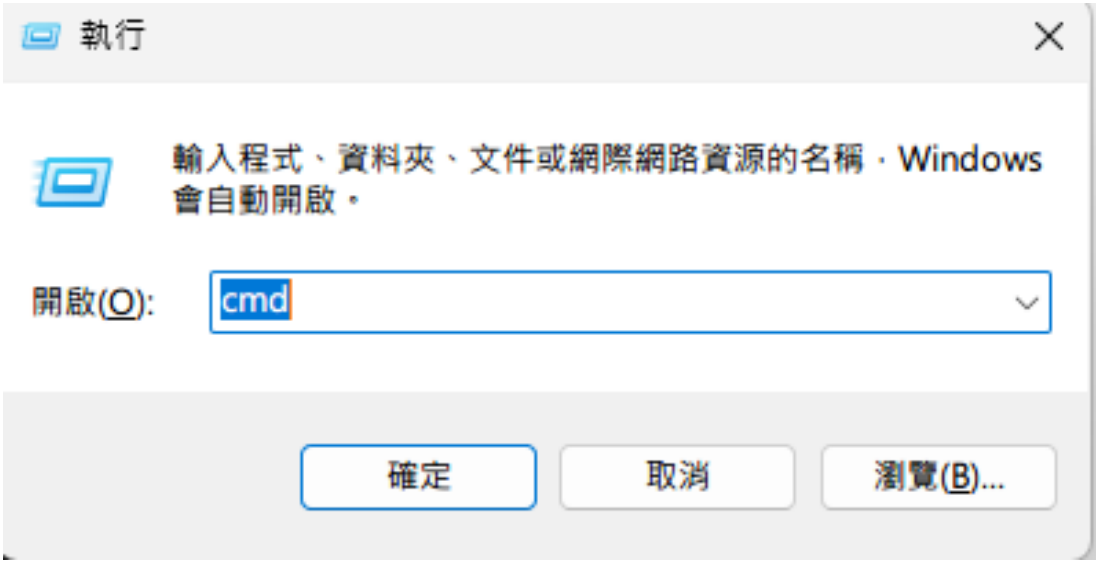
資通安全內部稽核表第13項資通系統、物聯網設備定期盤點，為幫助各單位人員盤點時，查找電腦IP，特出此教學手冊，請參閱。

Step1：從鍵盤同時按下這兩個鍵。

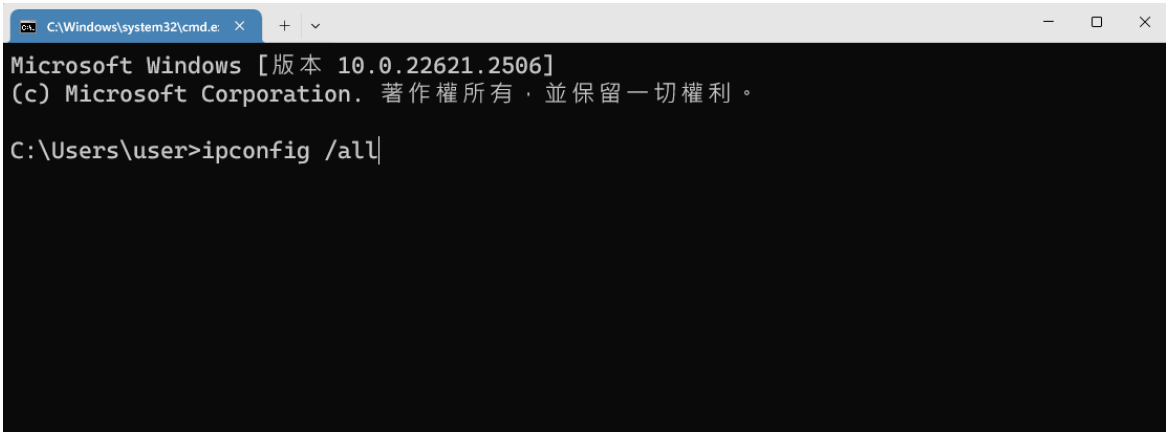




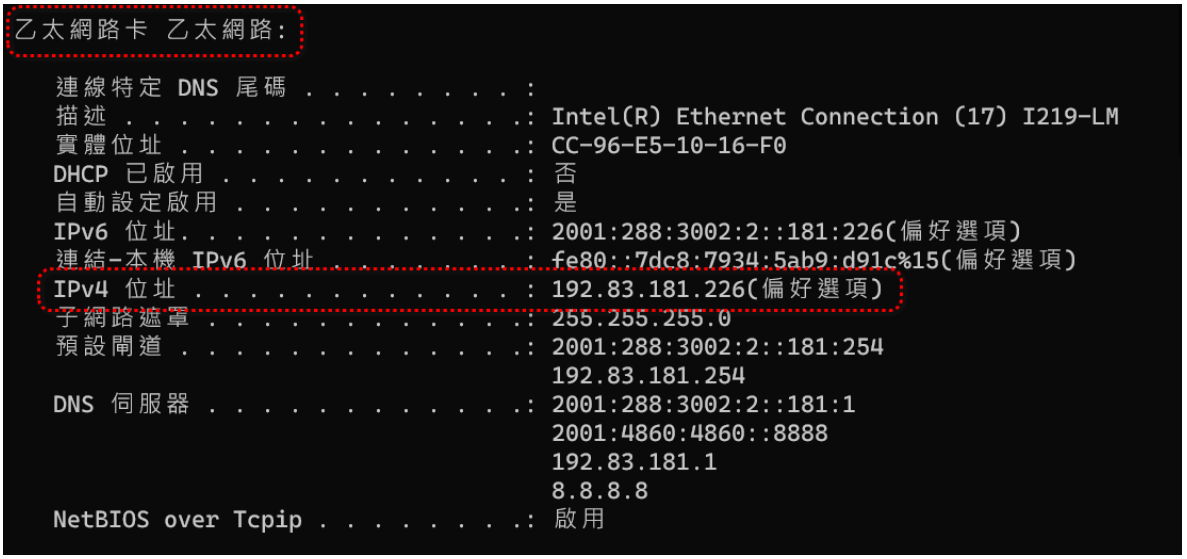
Step2：開啟以下這個[執行]的視窗後，請輸入cmd，再按下確定。



Step3：出現[命令提示字元]視窗後，請輸入ipconfig /all，按下Enter。



Step4：會出現乙太網路卡乙太網路中的[IPv4位址]。


乙太網路卡 乙太網路:
連線特定 DNS 尾碼 . . . . . :
描述 . . . . . : Intel(R) Ethernet Connection (17) I219-LM
實體位址 . . . . . : CC-96-E5-10-16-F0
DHCP 已啟用 . . . . . : 否
自動設定啟用 . . . . . : 是
IPv6 位址. . . . . : 2001:288:3002:2::181:226(偏好選項)
連結-本機 IPv6 位址 . . . . . : fe80::7dc8:7934:5ab9:d91c%15(偏好選項)
IPv4 位址 . . . . . : 192.83.181.226(偏好選項)
子網路遮罩 . . . . . : 255.255.255.0
預設閘道 . . . . . : 2001:288:3002:2::181:254
192.83.181.254
DNS 伺服器 . . . . . : 2001:288:3002:2::181:1
2001:4860:4860::8888
192.83.181.1
8.8.8.8
NetBIOS over Tcpip . . . . . : 啟用

資訊安全基本認知宣導簽名單

_____人員簽名表　　學生助理:

組別	姓名	分機	備註

單位承辦人核章　　單位主管核章