國立臺北科技大學校園網路使用規範

97 年 6 月 10 日第 2 學期計算機與網路發展指導委員會議通過
97 年 7 月 1 日第 2 學期第 10 次擴大行政會議通過
100 年 6 月 14 日第 2 學期計算機與網路發展指導委員會議修正通過
100 年 7 月 19 日第 2 學期第 10 次擴大行政會議修正通過
108 年 1 月 17 日 107 學年度第 1 學期計算機與網路發展指導委員會修正通過
108 年 4 月 2 日 107 學年度第 2 學期第 3 次行政會議修正通過
110 年 12 月 7 日 110 學年度第 1 學期第 7 次行政會議修正通過

一、目的：

國立臺北科技大學（以下簡稱本校）為充分發揮本校校園網路功能、普及尊重法治觀念，並提供網路使用人及管理人可資依循之準則，以促進教學及研究，特依據「教育部校園網路使用規範」訂定本規範。

二、適用範圍：

使用本校網際網路位址（IP Address）或在校園範圍內上網之資訊設備皆為本校校園網路之一部份，前項所指資訊設備包含電腦伺服器、個人電腦、網路設備等，利用上述設施之個人或單位皆為本校校園網路之使用對象。

三、實施要點：

（一）本校校園網路之建立，係以提供全校教職員工生，從事教學輔助、學術研究、行政業務等相關活動為目標。

（二）校園網路上各項活動皆應遵守本規範及教育部訂定之「台灣學術網路使用規範」。

（三）校園網路使用者應隨時注意在使用資訊設備時，不得影響他人生活及共同使用者之權益。

（四）校園網路之使用者禁止於網路上從事下列活動：

1、除因公務需要且經單位主管核可外，禁止在公務電腦使用點對點(P2P)軟體下載侵權檔案或提供違法分享。

2、傳送違反著作權法及違反相關法律規章之資訊。

3、以任何方式偷窺、竊取、更改、干擾、破壞他人資訊。

4、蓄意散佈電腦病毒或其他未經授權資訊。

5、侵入未經授權使用的電腦系統。

6、將個人登入身份識別帳號及密碼借予他人使用。

7、盜用或冒名使用他人身份申請登入識別帳號或網際網路位址。

8、蓄意破壞或不正當使用資訊設備（電腦伺服器、個人電腦、網路設備等）。

9、使用校園網路散佈廣告信、販售違禁品、非法軟體或資料。

10、 任何未經授權許可之商業行為。

11、 散佈不實文字、毀謗他人名譽。

12、 危害或干擾系統安全或網路通信安全。

13、 其他國家及本校相關法律規章明訂違法者。

（五）校園網路使用者若違反本規範或涉嫌侵害他人權益時，除送校方相關單位議處外，需自負刑事與民事責任。

（六）任何單位或個人若發現校園網際網路位址之資訊設備發生不正當行為時，可檢附相關行為證明資料予計算機與網路中心，計算機與網路中心於查明該不當資訊設備來源並發現其行為確有不當時，得轉知該資訊設備所屬單位網管人員及使用者處理或網路停權；情節重大者，得移送校方相關單位處理。

（七）校外單位若有偵查犯罪之必要，應正式來函，負責單位依規定簽請校長核定後，配合提供相關資料。

（八）校園網路使用者應善盡自身資訊設備資安保護及帳號密碼強度提升之責任。

（九）校園網路管理者應尊重網路隱私權、不得任意窺視其他網路使用者之個人資料或有侵犯隱私權之行為，但有下列情形之一者，不在此限：

1、為維護或檢查系統安全。

2、依據合理之懷疑，認為有違反校規情事發生時，為取得證據或調查不當行為。

3、為配合司法機關之調查。

4、其他依法令執行之相關網路管理行為。

（十）校園網路之公用電腦管理者應善盡下列管理責任：

1、保管並維護管理者之身份識別帳號及密碼。

2、保管並維護公用電腦使用者之身份識別帳號及密碼。

3、保管並維護使用者之個人資料。

4、公用電腦服務之維護。

5、公用電腦安全系統之維護。

6、保存期限內公用電腦使用者存取紀錄或系統紀錄之維護。

7、公用電腦系統及使用者重要資料備份之維護。

8、對不當使用系統資源者在公告相關管理規則後予以停權或適當處分。

9、配合校方處理爭議或偵查犯罪，提供相關資料。

（十一）　校園網路之網路設備管理者應善盡下列管理責任：

1、維護管理相關校園網路資訊設備中之網路設備及相關資訊設備。

2、保管並維護網路設備之管理者身份識別帳號及密碼。

3、對不當使用網路資源者在公告相關管理規則後予以停權或適當處理。

(十二)為使校園網路使用頻寬合理化及減少校園網路資訊安全事件發生，實施下列措施：

1、對網路服務埠進行管制。

2、對網路應用程式進行管制。

3、本校校園網路之使用對象，其使用之資訊設備若有其他需另行開放之服務埠，需填寫防火牆服務埠新增/異動申請表，經核可後，即可開放。

4、為落實網路使用者登記與管理制度，對於連入校園網路之裝置應逐一配發本中心核定之 IP，除經專案核定外，嚴禁

使用具有網路位址轉換之功能設備，如 IP 分享器、路由器或以其他任何形式共用 IP 進而影響學術網路穩定性與安全性；為保障本校無線網路頻段品質避免射頻干擾影響其穩定性，未經本中心核可不得安裝或使用與無線區域網路(802.11)網路相同無線射頻頻段之設備。

(十三)本校教職員工生未經本中心與本校資安長同意，於本校校址內不得以下列形式規避本校之資通安全管理監測機制或將資通電訊產品接入校園內。

1、使用非學術網路之線路。

2、將非學術網路之線路接入校園。

3、將本校資通電訊產品介接非本校之網路。

4、如資通電訊產品為公務使用時，不得進行網路區隔、位址轉譯或其他任何形式隔離，應直接接入校園網路並配予合規之 IP 位址，以配合稽查。

5、自建之資通電訊產品應符合本校 ISMS 規範；委外資通電訊產品應符合本校委外資訊系統標準作業流程及本校 ISMS 規範，方能接入校園網路。

上述列舉之情事如有未列之部分將以本中心最新公告為主，不另修改規範。若經稽查發現將要求限期改善，未於時限內限期改善者，本中心得中斷該空間之網路並依獎懲辦法相關法規進行懲處。

(十四)為降低資安風險，遠端存取採「原則禁止、例外允許」方式辦理，從校外連線校內主機者必須透過 VPN 方式進行連線。若需開放不特定、非校內人士或自校外等連入存取者，則將其方式視為伺服器主機連線，請依系統向上集中管理原則向本中心申請虛擬主機，並依「雲端虛擬主機租用管理要點」及「校園伺服器管理要點」辦理。

四、獎懲辦法：

(一) 本校教職員工生若有符合資通安全管理法「公務機關所屬人員資通安全事項獎懲辦法」內任一情形者，將協助收集相關資料建請相關單位依法敘獎。

（二） 本校教職員工生若經主管機關通報或裁定，發生第一級資通安全事件者，依本中心最新公告說明以情節輕重封鎖至少 1 至 30 日或取消其使用權；發生第二級(含)以上資通安全事件，即影響全校及附屬單位核心業務者，除依上述第一級方式處理外，本中心將提供佐證資料檢送相關單位依法懲處。

（三） 為保護公務機密、敏感資料與個人資料，若主動發現系統漏洞者，可依循本校資安事件通報之正常程序通報，或以業界公認可靠之第三方漏洞平台進行系統漏洞通報，並依法進行資通安全情資分享，防止資通安全事件之發生或擴大並降低其損害。本中心將依相關辦法提報敘獎或頒發相關證明以茲獎勵；反之若通報者洩漏或利用該漏洞情資，以致發生網路或系統遭到竄改、破壞或竊取之情形，本中心將提供佐證資料檢送相關單位依法懲處；如造成機關或他人權益損害時，本中心亦將協助受害機關、人提供相關佐證資料供檢調單位後續民、刑事責任之判定。

五、 本規範經行政會議通過後實施，修正時亦同。