南臺科技大學校園網路管理及流量管制要點

Southern Taiwan University of Science and Technology Campus Network Management and Traffic Control Guidelines

民國 97 年 1 月 30 日 行政會議通過

Adopted by Administrative Meeting on January 30, 2008

民國 101 年 4 月 30 日 行政會議修正通過

Revised and Adopted by Administrative Meeting on April 30, 2012

一、南臺科技大學(以下簡稱本校)因應教育部與區網中心加強對學術網路之管理要求，特依據本校「校園網路使用規範」訂定本要點。

Article 1 Southern Taiwan University of Science and Technology (hereinafter referred to STUST) develops the guidelines in accordance with the STUST "Campus Network User Instructions" in response to the management requirement for academic network from the Ministry of Education and Local Network Center.

二、本要點所稱之校園網路包含學校行政區、教學區及學生宿舍區之網路。所稱之流量係指校園網路與校外網路(含 TANet 線路及商網線路)間之流量進出總和。

Article 2 The campus network addressed in the Guidelines includes the network in school administrative zones, instructional zone and student dormitories. The so-called traffic refers to the total incoming and outgoing traffic between campus network and off-campus network (including TANet lines and commercial network lines).

三、本校網路流量管制措施如下：

(一) 校園有線網路每一網路位址單日流量超過上限，即限制該網路位址之網路頻寬至隔日零時。

(二) 校園無線網路每一使用者單日流量超過上限，即限制該使用者及該無線網卡之無線網路網路頻寬至隔日零時。

(三) 如因教學或學術研究之原因而有超大流量之需求者，於需求日三個工作日之前填寫「特殊流量申請單」，經單位主管簽核後，送交計算機與資訊網路中心(以下簡稱計網中心)申請。

網路流量之單日流量上限及限制網路頻寬授權計網中心規範，並公告於計網中心網站，流量統計數據以計網中心之流量軟體統計為準。

Article 3 STUDT network traffic control measures are described below:

(1) In case one network IP address of campus wired network exceeds the limit, the network bandwidth of the IP address will be limited until 24:00A.M of the next day.

(2) In case one user exceeds the limit for single-day traffic in wireless campus internet, the user and the wireless network bandwidth of the wireless network card shall be limited until 24:00A.M of the next day.

(3) The applicant in need for big traffic due to instructional reasons or academic research shall need to complete the “Special Traffic Application” in 3 working days before the day of requirement. The application shall be signed by department supervisor for approval before submitting to the Computer and Information Network Center (hereinafter referred to as the Computer Network Center) for application.

The Computer Network Center is authorized to regulate the single-day traffic limit for network traffic and restriction of network bandwidth with announcement published on the website of Computer Network Center. The traffic statistics are subject to the traffic software statistics at the Computer Network Center.

四、使用者對個人所擁有或管理之電腦設備，有責任防止其感染電腦病毒或木馬並避免任何破壞網路之行為。有下列情形之電腦，即視為中毒電腦，計網中心可進行必要之處理，以免影響他人使用網路之權利：

(一) 疑受病毒、Worm、木馬感染，會經由網路擴散，有送出病毒封包之行為。

(二) 有掃描網路埠或網路位址的行為。

(三) 有連線數(flow)超過計網中心公告限制之行為。

(四) 教育部電算中心、區網中心或其他使用者通知有異常行為，並經查證屬實。

中毒之電腦將被立即停止網路使用權，若有需要可要求使用者親自至計網中心說明。中毒之電腦須先完成各項防護措施後，方能提出網路復用申請。一個月內中毒超過十次者，停用網路使用權三十天。

Article 4 Users are responsible for preventing the computer equipment owned or administered with computer virus or trojans to avoid any conducts that will sabotage the network. Computers with the following conditions are considered virus computer and the Computer Network Center may take necessary measures to prevent the right for others to use network:

(1) Conducts suspected of virus, worm and trojans infection that will diffuse via internet and send out virus packet.

(2) Conducts that scan the network ports or network address.

(3) Conducts with flow exceeding the restriction announced by the Computer Network Center.

(4) The abnormal conducts notified by the Department of Information and Technology Education, Ministry of Education, local network center or other uses that have been verified true.

Computers infected with virus shall be suspended of right to use internet. Users may visit the Computer Network Center to explain in person if necessary. Computer infected with virus shall first complete the various protection measures before proposing the application of internet recovery. Persons with more than 10 times of virus infection in 1 month shall be suspended for right to use the internet for 30 days.

五、有下列行為者視為蓄意違規，將被停用網路使用權三十天：

(一)冒用他人網路位址或使用未經授權之網路位址者。

(二)違反校園網路使用規範經勸導未改善者。

前項第一款除停用網路使用權三十天外，並通知單位主管處理，累犯者則依校規論處。

Article 5 The following conducts are deemed as deliberate violation and shall be suspended for right to use the internet for 30 days:

(1) Use other's network address or use unauthorized network address.

(2) Persons violating user campus network instruction and such persons have not shown improvement after advice.

Apart from the 30-day suspension of right to use internet in Paragraph 1 of previous article, the department supervisor shall be notified and recidivism will be punished in accordance with STUST regulations.

六、為加強資訊安全及尊重與保護智慧財產權，除以下原因外，校園網路禁止使用 P2P 類型之軟體：

(一) 計網中心公告認可之 P2P 軟體。

(二) 因教學或學術研究之需求必須以 P2P 軟體下載，需填寫「P2P 軟體使用申請表」，經單位主管簽可後，送交計網中心申請。

Article 6 To strengthen information security and respect and protect intellectual property, the following P2P software is prohibited to use on campus network with the exception of the following reasons:

(1) P2P software announced and recognized by Computer Network Center.

(2) P2P downloads due to instructional reason or academic research. The applicant must fill out the "P2P Software Use Application" which will be authorized by the department supervisor before submitting to the Computer Network Center for application.

七、本校師生須以合法方式使用本校電子資源，不得有下列行為：

(一) 使用程式不正常大量下載資料。若涉及侵犯智慧財產權或損及電子資源廠商合約之情事，須自負民法、刑法、著作權法等相關法令之追訴責任。

(二) 將個人連線電子資料庫之帳號、密碼提供校外人士使用。一經查證，立即取消連線之權利，並須負相關之責任。

Article 7 STUST faculty and students shall use STUST electronic resources through legitimate approach without engagement of the following conducts:

(1) User program with abnormally massive data download. In case the user involves with infringement of intellectual property or damage the contract with suppliers of electronic resources, the user shall be held for litigation responsibilities related to civil code, criminal code, and copyright act.

(2) Provide personal account and password connected to electronic database to non-STUST user. Once verified, the user shall be cancelled with the right to connection in addition to being held liable for relevant responsibilities.

八、發現網路智慧財產權疑似被侵權時，依下列程序處理之：

(一) 接獲教育部、區網中心或其他單位以電子郵件或書面檢舉，有疑似侵害智慧財產權情事時，接獲單位應通報計網中心處理。

(二) 計網中心立即將被檢舉之網路位址做斷線處理。

(三) 通知該網路位址之使用人，告知侵權法律責任，並要求立即停止疑似侵權行為。計網中心將該網路位址列入追蹤名單，至少追蹤 3 個月。

(四) 依情節之需要，通知學務處及相關單位主管協助處理。

(五) 若網路位址重覆被檢舉且情節重大者，移請相關單位依校規論處。

(六) 將處理情形回覆檢舉單位。

Article 8 In case of discovering suspected infringement of online intellectual property, process according to the following procedures:

(1) In the event the Ministry of Education, Local Network Center or other departments have received email or written report suspecting infringement of intellectual property, the notified department shall inform the Computer Network Center for processing

(2) The Computer Network Center shall cut the line for the network address to be reported immediately

(3) Notify the user of the said network address and notify him/her of legal rights of infringement in addition to immediately requesting the user to suspend the suspected infringement conduct. The Computer Network Center shall list the network address into follow-up list for at least 3 months.

(4) Depending on the condition, the Office of Student Affairs and relevant department supervisor shall assist with the handling.

(5) In case the network address is repeatedly reported with major gravity, the case will be transferred to relevant department for disciplines by STUST conducts.

(6) Reply the processing status to the reporting department.

九、發現有資安事件時，依下列程序處理之：

(一) 接獲教育部、區網中心或其他單位以電子郵件或書面舉報，有疑似本校設備遭受他人攻擊或攻擊他人情事時，接獲單位應通報計網中心處理。

(二) 計網中心立即將被舉報之網路位址做斷線處理。

(三) 通知該網路位址之管理人員進行處理，並副知單位主管。管理人員於處理完畢後，應填寫「資訊安全事件報告單」，經單位主管簽核後送交計網中心。

(四) 計網中心依「教育機構資通安全通報應變流程」進行通報作業。

Article 9 In the event of information security incident, follow the procedures below for process:

(1) In the event the Ministry of Education, Local Network Center or other departments have received email or written report suspecting STUST equipment being hacked or is

hacking others, the notified department shall inform the Computer Network Center for processing.

(2) The Computer Network Center shall cut the line for the network address to be reported immediately.

(3) The administrator of network address should be notified with copy notice to the department supervisor. The administrator shall complete the “Information Security Incident Report” after completion and submit to the department supervisor for verification before submitting to the Computer Network Center.

(4) The Computer Network Center shall report in accordance with “Educational Institutions Information and Communication Security Reporting and Response Process.”

十、 網路使用權之復用流程一律依計網中心網站之「網路復用申請流程」相關規定辦理。

Article 10 The recovery process for right to use internet shall be processed in accordance with the relevant provisions of “Internet Recovery Application Process” on the Computer Network Center.

十一、 本要點經行政會議通過，陳請校長核定後公佈實施，修正時亦同。

Article 11 The Guidelines shall be adopted by the Administrative Meeting and submitted to the President for approval before announcement and implementation. The same procedures apply to revision.