校園網路特殊需求開放申請單 The Application of the campus network service

ISPI-D-044，機密等級 Level of confidentiality：2限閱， 版　　本 Version：2.0

紀錄編號. / NO　　填表日期. / Date.

***單位 / 研究室**		**分機**	
***申請人 / 資通訊安全管理人員**			
***申請人的亞洲網路帳號** ***Asia Network ID；ANID**	**@asia.edu.tw**		
亞洲大學基於資通訊安全與個人資料保護管理之目的，並遵循「個人資料保護法」、「資通安全管理法」、「臺灣學術網路管理規範」辦理，蒐集單位、姓名、電話及電子郵件等個人資料，以在本校地區內，作為資通安全管理紀錄之用。您得以行使請求查閱、補充、更正；請求停止蒐集、處理、利用；請求刪除個人資料等權利。			
***用途** **(研究/計畫/服務，請填寫完整名稱)**			
***申請類型**	☐提供校外及校內網路服務 ☐提供校內網路服務 ☐僅校內教學研究需求，不提供網路服務		
在校內的資通訊設備 IP			
對點(校外)資通訊設備 IP			
***服務終止日期**(開通日起算)	☐ 7日　☐ 14日　☐ 30日　☐ 因課程需要至學期終了 ☐依計畫/合約日期辦理 (請檢附計畫/合約副本)		

***申請項目**

資通訊設備異動每日網路流量上限。

1. 本校目前僅統計下載流量，教學研究區域每日為20GB。
2. ☐ 申請期間內增加到每日_____GB (請提供期間內增加流量上限的佐證資料)。
3. ☐ 申請短期(30日內)流量上限增加，辦理教學行政業務 (業務內容如「用途」欄位)。

==========

網際網路服務及管制連接埠開啟

1. **進校傳輸：**由校外進校內 (提供網路服務的 Public IP 主機適用)

網站服務

*網站使用的網站平台 ☐ IIS ☐ Apache ☐ Nginx ☐ Tomcat　　版本號_____

☐ http　　TCP 80　or TCP_____　除非必要，請使用加密的 https

☐ https　　TCP 443　or TCP_____

☐ 為保護網站安全，此網站僅提供台灣 IP (含校內)存取。

資料庫存取

*請確認"必需"開放由校外直接連線資料庫，並有確認的來源 IP

☐ MS-SQL TCP 1433　資料庫系統版本號_____

☐ MY-SQL TCP 3306　資料庫系統版本號_____

檔案傳輸

☐ FTP　　TCP 21

☐其它

_____

2. **出校傳輸：**由校內到校外
   請說明用途、網路協定與服務埠號

1. 本校配合教育部政策實施伺服器向上集中措施，非必要請勿自行建置網站服務，靜態網站請申請本校網頁空間，動態網站請申請本校虛擬主機。本校機房不提供主機硬體代管服務。
2. 由於資訊安全相關法規要求，各單位(含研究實驗室)須置有一人負責該單位之 IP 審核及管理，本申請僅提供教職員使用，學生請聯絡各自研究實驗室的資通訊安全管理人員。教師研究室，資通訊安全管理人員即為教師本人。
3. 配合資訊安全相關管制要求，開放期間不宜過久，非課程需要或非計畫/合約設備，僅提供短期開放。請在超過有效日期前辦理續用。
4. 主機提供網路服務，應評估所提供服務系統安全等級，檢附「資通系統安全等級評估表」。
5. 本單為提供校內資通訊及物聯網設備網路存取控制策略異動申請，
   (1) 設備「每日下載流量上限」期間內異動。
   (2) 設備對校外提供的網路服務及管制連接服務埠的開啟或阻擋。(使用者由校外連線)
   (3) 設備對校內跨網路區域管制連接服務埠開啟。(如、ntp, icmp, smtp)
   ※校級伺服器與代管虛擬主機，請使用「防火牆管制開放申請單」申請。
6. 設備若為委外管理，請務必確認委外合約內是否加入資通訊安全及個資保護相關協議。計畫或委外維護，請提供在有效期內，具資安個資條款的採購/維護合約副本 (電子檔可)。
7. 管制連接服務埠：
   (1) 配合資通訊安全及 TANet 使用規範辦理，並減少來自網際網路的攻擊風險，管制「挖礦」、「BitTorrent」、「P2P 傳輸」、「惡意中繼站」、「惡意網域」、「寄件攻擊」及來自外部的「遠端連線」攻擊...等，具弱點風險之特殊服務埠。若有申請開放需求，應提供佐證資料，由資訊處協助提交亞洲大學資訊安全暨個人資料保護委員會，審核通過後方協助開放。
   (2) 遠端控制需求類型：RDP、SSH、TELNET...等遠端控制服務，請連線 VPN 後使用，原則上不提供由網際網路的直接連線申請。
8. 依行政院國家資通安全會報函辦理(資安發字第0970100108號)，公務電腦禁止安裝非公務用 P2P 分享軟體，如教師兼任行政職，於單位內亦不得申請，本申請得於研究室及實驗室內使用。

申請單位		資訊發展處		
申請人	權責主管	資訊發展處聯合服務櫃檯	網路維運組業務承辦	網路維運組主管

*教師研究室權責主管為教師本人

校園網路特殊需求開放申請單 The Application of the campus network service

ISPI-D-044，機密等級 Level of confidentiality：2限閱， 版　　本 Version：2.0

紀錄編號. / NO　　填表日期. / Date.

****Unit / research Lab**		**Ext.**	
***Applicant / The region's ICT security administrator**			
***The applicant's Asia Network ID；ANID**		**@asia.edu.tw**	

To maintain information and communications security and protect personal data, Asia University collects personal data such as organization, name, telephone number, and email address in accordance with its national laws and regulations for internal information and communications security management records. You have the right to request access to, supplementation of, or correction of your personal data; the right to request the cessation of collection, processing, and use of your personal data; and the right to request the deletion of your personal data.

***Purpose or Full name of research/project/service**	
***Type of apply**	☐ Your device provides both on-campus and off-campus network services. ☐ Your device provides on-campus network services. ☐ Your device is only for on-campus teaching and research needs and does not provide network services.
On-campus ICT device IP address	
Off-campus ICT device IP address	
***Service termination date** (from activation date)	☐ 7 days ☐ 14 days ☐ 30 days ☐ Due to "course requirements", until the end of the semester ☐ Execute according to the effective date of the project/contract

*** Item to apply for**

Application for adjustment of the "Daily Internet Traffic Limit" for ICT devices.

1. Currently, we only calculate download traffic; the daily limit for the teaching and research area is 20GB.
2. ☐ Request an increase to _____ GB per day during the specified period.
   (Supporting documentation demonstrating the need to increase the "download traffic limit" during the specified period should be provided..)
3. ☐ Request a short-term (within 30 days) increase in download traffic limit for handling teaching and administrative matters (such as the content in the "Purpose" field).

==========

Internet Services and Controlled Ports

1. **inbound traffic: Off-campus access service:** Internet service for connections from off-campus to on-campus
   (applicable to "Public IP Hosts" that provide network service)

Website services

* Which website platform does the website service use?

☐ IIS ☐ Apache ☐ Nginx ☐ Tomcat　　Version _____

☐ To activate the service port　http　　TCP 80　or TCP_____

(Unless it is absolutely necessary to use an HTTP service, please use encrypted HTTPS.)

☐ To activate the service port　https　　TCP 443　or TCP_____

☐ The website only provides access from Taiwan IP addresses (including IP addresses within the campus).

Accessing the database

*Please confirm that the "Required" direct connection to the target database from outside the university is enabled, and that it has a stable source IP address.

☐ MS-SQL TCP 1433　target DB version_____

☐ MY-SQL TCP 3306　target DB version_____

File transfer

☐ FTP　TCP 21

☐ the other

_____

2. **outbound traffic**：From on-campus to off-campus

. Please specify the purpose, network protocol, and service port number

_____

1. In accordance with the Ministry of Education's policy, we implemented measures to centralize servers. Please do not create your own website for external use within the research lab. Static websites can apply for web hosting provided by the university. Dynamic websites can apply for virtual hosting provided by the university. ◦
2. Due to information security regulations, each server should have designated administrators responsible for managing and reporting information and communication security (ICT) related matters.
3. Services must comply with information security regulations. Activated services should be reviewed regularly, and the activation period should not be too long. This service is only available for short-term access if it is not required for the course or is not part of a planned/contracted program. Please renew your access before the expiry date.
4. The security level of the services provided should be assessed, and a "System Security Level Assessment Form" should be attached.
5. This form is for submitting an application to change the network access control policy, and is available for use by on-campus ICT and IoT devices.
   (1) Increase the device's "daily download traffic limit" during the period.
   (2) The device controls or blocks the "network services provided off-campus" and "connection ports".
   (3) The device enables cross-network area control connection services within the campus. (e.g., NTP, ICMP, SMTP)

   ※If your server and virtual host are located in the Asia University Computing Center, please use the " The Application of the Server Room Firewall Policy " to apply for access control.
6. For outsourced servers, please ensure that the outsourcing contract includes agreements related to ICT security and personal data protection. For planned or outsourced maintenance, please provide a copy of the purchase/maintenance contract (electronic version acceptable) with valid cybersecurity and personal information protection terms.
7. Regulated service ports：
   (1) In accordance with ICT security and TANet usage guidelines, and to reduce the risk of attacks from the Internet, we regulate vulnerable ports such as cryptocurrency mining, BitTorrent, P2P transmission, malicious relay stations, malicious domains, email attacks, and external remote connection attacks. If you need to apply for access to a regulated service port, you should provide supporting documentation, which will be submitted to the "Information Security and Personal Data Protection Committee of Asia University" by OICT. Access will be granted only after the application is approved.
   (2) Remote control types: For remote control services such as RDP, SSH, TELNET, etc., please use them after connecting to an SSL-VPN. We do not provide direct connection requests via the Internet.
8. According to the official document (No.0970100108) of Nation Information & Communication Security Taskforce (NICST), any P2P software is not allowed to be installed in public computers. This application is just for the laboratory and research room, and not for any other department.

Unit		Office of Information and Communication Technology		
Applicant	**Unit Director**	**OICT Service Counter**	**Network Administrator**	**Section Chief**

*The Unit Director of the teacher's research office is the teacher himself