資安及網路設備異動申請表 (Security and Network Equipment Change Request Form)					
文件編號 (Document No)	ISMS-308-01	機密等級 (Confidentiality Level)	限閱 (Restricted)	版次 (Version)	7.1

紀錄編號(Record Number)：YYY-MM-DD-XXX　　填表日期(Date)：

*申請單位 (Applicant Unit)	○○處○○組	*申請人 (Applicant)	○○○
*Email	○○○○@ccu.edu.tw	聯絡分機 (Extension No.)	11111
*申請用途 (Purpose)	○○設備阻擋校外攻擊		
*管制方式 (Action)	☐ 允許連線(Permit)　■ 阻擋連線(Deny)　☐ WAF 防護(WAF)		
*Source IP/URL	All / 臺灣 / XXX.XXX.XXX.XXX		
*Destination IP/URL	140.123.xxx.xxx		
*Port/Service	TCP： All	UDP： All	其他(Other)：
有效日期 (Validity Period)	From 2026 ／ 08 ／ 01　To 2027 ／ 07 ／ 31 ※預設最長 1 年，若因特殊業務需求申請>1 年者，填寫下一欄。 Standard limit is 1 year. If requesting > 1 year for special business needs, fill in the field below.		
長效申請原因 (Reason for >1 Year)			
注意事項 (Reminders)	1. 每年須至少執行一次弱點掃描，並完成中風險（含）以上漏洞修補。 Annual vulnerability scans and remediation of Medium-or-higher risks are required. 2. 遵守「最小特權原則」，嚴禁全開放（Any to Any）；遠端管理埠（如 SSH、RDP）須限定 IP 範圍，並建議優先採用本校 VPN。 Rules must follow "Least Privilege"—no "Any-to-Any". Remote ports (e.g., SSH, RDP) require IP restriction, with campus VPN strongly recommended. 3. 規則效期最長一年，到期前須申請展延，逾期將自動停用或刪除。 Rules are valid for up to 1 year. Unrenewed rules will be automatically disabled or deleted upon expiration. 4. 若發生資安事件或異常流量，管理員得直接阻斷連線至威脅排除。 In case of security incidents or abnormal traffic, access may be blocked immediately without prior notice.		
*申請人簽章 (Applicant Signature)	承辦人核章	*申請單位主管簽章 (Unit Head Signature)	承辦單位主管核章

表必填寫欄位／ Indicates a required field

資安及網路設備異動申請表 (Security and Network Equipment Change Request Form)					
文件編號 (Document No)	ISMS-308-01	機密等級 (Confidentiality Level)	限閱 (Restricted)	版次 (Version)	7.1

以下由執行單位填寫 Completed by implementing unit.			
審核結果 (Review Result)	☐同意(Approved) ☐不同意(Not Approved)	執行日期 (Execution Date)	
設備名稱 (Device Name)			
處理紀錄 (Processing Record)	☐設定檔備份(Configuration Backup)		
承辦人簽章 (Case Officer Signature)		承辦單位 主管簽章 (Unit Head Signature)	