

CSUF Information Security Office

Request for Internet Host Access to On-Campus Resources

CSU Information Security Requirements mandate restricted access for off-campus Internet host to on-campus resources. Internet access to on-campus servers will be blocked for all network protocols with the exception of HTTP (80) and HTTPS (443). All other network protocols require prior approval through this authorization process.

(1) Requester's Name (Must be an MPP)

(2) Responsible Department

(3) Technical Contact Name

(4) Server IP

(5) Primary Server Purpose

(6) Protected Data Present ? See the CSU Information Security Data Classification Standards:
http://www.fullerton.edu/it/resources/pdfs/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf

a. Is any "Level 1" protected data stored or transferred by/on this server?	Yes	No
b. Is any "Level 2" protected data stored or transferred by/on this server?	Yes	No

(7) Specific Additional Internet Access to On-Campus Server Request:

a. Specify which network Ports/services are needed open. Include whether TCP/UDP protocol, port number, and application that uses the port(s):

b. Rationale for needing this port open AND Impact of Not Doing:

(8) In order to meet campus security compliance, I understand IT has my authority to do periodic vulnerability scans to my server, and I will remediate any vulnerabilities within 30 days or this access will be blocked. I Understand

(9) Required Approvals:

a. Requester (MPP):

Date:

b. Division Vice President:

Date:

Please send the completed form to the Information Security Office (iso@fullerton.edu) for final approval

Information Security Officer:

Date: