STOCKTON UNIVERSITY | COMPUTER AND TELECOMMUNICATION SERVICES

COMPUTER AND TELECOMMUNICATION SERVICES
609-652-4335

STOCKTON UNIVERSITY
101 VERA KING FARRIS DRIVE
GALLOWAY, NJ 08205-9441

VPN / VDI Access Request Form

Off-campus access to certain computer systems that contain confidential, sensitive or otherwise privileged information is not permitted without clearly documenting a pressing business need for off-campus access and acquiring supervisory approval.

A virtual private network (VPN) may be used to enable off-campus access to these systems. There are, however, risks inherent in providing VPN access to systems. A home computer or mobile device that is connected to the university via a VPN provides a gateway to the university's internal network and servers. A VPN enabled home computer or mobile device that is lost, stolen, compromised by hackers, or otherwise made available to persons who are not authorized to access the university's internal network and servers could potentially lead to the unauthorized disclosure of confidential, sensitive or otherwise privileged information and the use of university assets for illegal or unethical purposes.

Persons using VPN enabled devices to access the university's internal network and servers must take responsibility for implementing the following safeguards on their VPN enabled devices:

- VPN enabled devices must be configured with a complex password (at least 8 characters in length with mixture of letters and numbers) and
- VPN enabled devices must be configured to automatically lock after a period of inactivity and require a user to reenter the device's password.
- VPN enabled computers must have an anti-virus package that automatically downloads up-to-date virus protection files.
- VPN enabled devices must have up-to-date operating system patches installed, where possible devices should be configured to automatically download and install patches.

Any device configured for VPN use which is lost or stolen must be promptly reported to Stockton University's Office of Computer and Telecommunication Services so appropriate actions can be taken.

Select the services needed access to from off-campus. Please list other services if applicable.

❒ INB Banner	❒ Discoverer
❒ Workflow	❒ Banner Extender / BDMS
❒ Remote Desktop / VDI	Other _____

I acknowledge the risks associated with providing off-campus access to confidential, sensitive or otherwise privileged systems and in light of the pressing business need described above authorize VPN access for the employee listed below for the time period specified.

Budget Unit Manager _____ (Print) _____ (Sign)

Effective From: _____ Effective Until (Required): _____

I understand that it is my responsibility to take reasonable measures to protect the university's information assets and agree to implement the safeguards noted above on the VPN enabled devices I use.

_____ (Print) _____ (Sign) _____ (Date)

Please scan and return signed form to Demetrios Roubos / Office of Information Security
D108e demetrios.roubos@stockton.edu