STOCKTON UNIVERSITY | INFORMATION TECHNOLOGY

REMOTE ACCESS ENTITLEMENT REQUEST FORM

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

SECTION 1

For the Applicant's Information

Remote Access Acceptable Usage Information

By using remote access technology with personal equipment, users must understand that their machines are a defacto extension of the Stockton network, and as such are subject to the same rules and regulations that apply to Stockton owned equipment, i.e., their machines must be configured to comply with all Stockton security policies.

All computers connected to Stockton campus networks remotely must use up-to-date virus-scanning software and virus definitions. Additionally, all relevant security patches must be installed; this includes personal computers. It is the responsibility of the employee or company with VDI privileges to ensure that unauthorized users are not allowed access to Stockton campus networks.

Remote access is controlled using two-factor authentication composed of an ID and a one-time-use passcode. For Stockton employees, the user ID is in the form of their Stockton Webmail Username and Password. The passcode is provided to the user via either a physical (hard) or application-based (soft) encrypted token.

Individuals using VDI enabled devices to access the University's internal network and servers must take responsibility for implementing the following safeguards on their devices (www.stockton.edu/acceptable-use):

Each user must have a unique profile. Shared profiles are not permitted.

Desktop and mobile devices that contain or provide access to institutional data must be password protected against unauthorized access. These computers and devices should be shut down when not in use for extended timeframes.

Remote access enabled devices must be configured to automatically lock after a period of inactivity and require a user to re-enter the device's password.

Any device configured for VDI use which is lost or stolen must be promptly reported to Stockton University's Office of Information Security, so appropriate actions can be taken.

Remote access services are to be used solely for Stockton business and/or to support academic initiatives.
All remote access gateways on the campus network will be set up and managed by Stockton Telecommunications group.
User created remote access gateways will not be permitted on the Stockton network.

Remote access users may be automatically disconnected from the Stockton network after sixty minutes of inactivity. Artificial network processes are not to be used to keep the connection open.

SECTION 2

To be completed by the Applicant

Personal Identification and Information

Last Name		Z-Number	Z
First Name	Username		

Applicant Signature_____ **Date**_____

SECTION 3

To be completed by the Budget Unit Manager

Budget Unit Manager Authorization

Budget Unit Manager	
Effective From Date	Effective Until Date *(renewed annually)*

Budget Unit Manager Signature_____ **Date**_____

SECTION 4

To be completed by the Office of Information Security

Information Security Entitlements

- ☐ INB Banner
- ☐ Workflow
- ☐ Remote Desktop
- ☐ Recruiter
- ☐ AMPROD
- ☐ Titanium
- ☐ Enforsys
- ☐ Other_____

FINAL APPROVAL

Provision Date	Initial	**De-Provision** Date	Initial