Remote Desktop Users Acknowledgement

 A signed copy of this document must be turned in to SSB Computer Support before your office computer can be configured for remote connections.

Licensing:
Some of the software that may be installed on your desktop computer cannot be used remotely. Executing the following programs via a remote connection is a violation of our licensing agreements for the following software and is prohibited by OSU policy.

SAS	GAUSS	SDC Platinum
Adobe Acrobat	nlogit/LIMPDEP	Quickbooks
FARS	Mathematica	ProSim

Security Concerns:

Computers that allow remote desktop connections are more vulnerable to attack and hacking than computers that do not allow remote connections. If your computer is compromised by an intruder masquerading as you the intruder has the ability to read download and delete any file you have access to including files you share with colleagues located on both the local and network drives.

If you believe your password has been compromised you agree to change your password immediately. If you cannot change your password contact SSB Computer Support or the IT Help desk for assistance.

It is very important that you contact SSB Computer Support, OSU IT Security or the IT Help Desk right away if you believe that your computer has been compromised.

 If your system is compromised we must assume that all confidential data that you have access to locally and on the network will have been compromised. State and Federal laws regarding notification, penalties and procedures may apply in cases where certain types of data have been compromised (grades, SSN, financial, medical). You may be held liable if an intruder uses your system to access confidential data.

I have read this document and understand that allowing remote desktop connections to my office PC represents and increased data security risk.

User:
Sign:_____ Date:_____

If you are a staff member or GTA you will need to have your supervisor read and sign this document below.

Supervisor:
Sign:_____ Date:_____