NETWORK SECURITY PROTECTION

Smart City requires all devices directly or indirectly accessing Smart City's network to have the following: the latest virus scan software, Windows® security updates and operating system patches. Smart City requires these necessary precautions to maintain a healthy, viable network and protect all customer provided devices from viruses, malicious programs, and other disruptive applications. Misuse of network services may result in service interruption to yourself and other customers leading to the disconnection of your equipment from the network. All service/installation charges will apply and no refunds will be given.

Any device adversely impacting Smart City's network will be disconnected with or without prior notice at Smart City's discretion. The device(s) in question will remain disconnected until all ensuing issues are resolved. Additional charges may apply for trouble diagnosis and/or problem resolution.

Your business is important to us. We are confident that we can provide network services that perform as expected for all clients with advanced and timely notification of your needs. Your internet connection will not be activated until we receive this signed affidavit ensuring your compliance with our network protection requirements.

SHOW NAME_____ BOOTH NUMBER_____

COMPANY NAME_____

ARE YOU RENTING COMPUTERS?   Yes   No

NAME OF COMPUTER RENTAL COMPANY_____

DEVICE'S OPERATING SYSTEM_____

TYPE OF ANTI-VIRUS SOFTWARE INSTALLED:
   _____   Norton
   _____   McAfee
   _____   Other _____

DATE VIRUS-SCAN WAS LAST UPDATED: _____

DATE SECURITY UPDATES WAS LAST PERFORMED:_____

By my signature below, I attest that my equipment to be connected to Smart City's network at the Las Vegas Convention Center during the _____ event, dates from _____ through _____, has been properly protected with up-to-date anti-virus software and the latest security updates and patches have been installed. I also accept responsibility for my equipment's performance and understand that additional charges may be applied should my equipment be found to disrupt the network performance.

_____   _____
Signature   Date

_____   _____
Printed Name   Title