

# NETWORK SECURITY DECLARATION



Smart City has a Network Security Policy that requires adherence to several necessary precautions in order to maintain a healthy, viable network. This signed declaration of compliance with our network security requirements and acknowledgement of our filtering policies must be completed, signed and mailed or faxed to Smart City prior to your network services being activated.

Smart City requires that all devices directly or indirectly accessing Smart City's network have the latest virus scan software, Windows® security updates, system patches, and any other technological precautions necessary to protect yourself and others from viruses, malicious programs, and other disruptive applications. Any device which adversely impacts Smart City's network may cause service interruptions to yourself and others which can lead to disconnection of your equipment from the network, with or without prior notice at Smart City's discretion. The device(s) in question will remain disconnected until all issues are adequately resolved. All charges will apply and no refunds will be given. Additional charges may apply for trouble diagnosis and/or problem resolution.

In addition to the above policy and in the interest of enhanced network security, Smart City has implemented filtering policies on all Internet routers. These filters block all ICMP (Ping, Traceroute, etc.) either destined to or sourced from any Smart City network. Further, to avoid infection by common Internet worms (Nachi, MSBlaster, LoveSAN, etc.), we have implemented similar filters on the following TCP and UDP port numbers: UDP – 69, 137, 138, 402, 1434 and TCP – 135, 139, 402, 445, 4444.

Understanding that Ping and Traceroute are valuable troubleshooting tools, Smart City's policy allows Internet Control Message Protocol (ICMP) packets to the following two hosts: ns1.smarcity.com and ns2.smarcity.com.

If you require inbound or outbound access to any of the filtered ports, please contact your Smart City customer service representative in advance of your event with details of your requirements so that Smart City may consider the potential of a customized alternative.

Your business is important to us and with advanced and timely notification of your needs we are confident that we can provide network services that perform as expected for all clients.

**\*\*\* Please inform all show site personnel about the importance of Smart City's Network Security compliance issues \*\*\***

**\*\*\* Services are activated after Smart City is in receipt of this signed declaration of compliance with our network security requirements \*\*\***

CONVENTION CENTER: \_\_\_\_\_ CUSTOMER REF NO: \_\_\_\_\_

SHOW NAME: \_\_\_\_\_ BOOTH NUMBER: \_\_\_\_\_

COMPANY NAME: \_\_\_\_\_ Are You Renting Computers?  Yes  No

Rental Company Name: \_\_\_\_\_ Contact Number: \_\_\_\_\_

Device(s) Operating System: \_\_\_\_\_ Total # of Devices: \_\_\_\_\_

Type of Anti-Virus Software Installed:  Norton  McAfee  Other: \_\_\_\_\_

Virus Scan Last Updated: \_\_\_\_\_ Date Security Updates Last Performed: \_\_\_\_\_ Date

By my signature below, I attest that my equipment, which will be connected to Smart City's network at the above mentioned Convention Center and Show/Event, from beginning date of: \_\_\_\_\_ through ending date of: \_\_\_\_\_ has been properly protected, contains anti-virus software, and the latest patches and security updates have been installed. I also accept responsibility for my equipment's performance and understand the conditions placed on service delivery by this document as well as the potential that additional charges may be incurred should my equipment be found to adversely impact the network's performance.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Title