Keysight Technologies, Inc.
1400 Fountaingrove Parkway
Santa Rosa, California 95403

www.keysight.com

29 June 2021

Keysight Technologies Computer Virus Control Program

Keysight Technologies, Inc. recognizes the potential risk of computer virus infection that may be posed by instruments which are capable of connecting to computers or networks. We take this threat seriously and have acted to minimize the threat. The following Frequently Asked Questions (FAQ) address key areas of concern.

1. What steps do you take to protect your instruments from infection by computer viruses?

a. Keysight has enacted a number of measures to take all reasonable precautions to prevent the spread of viruses from instruments to our customers' computers and networks. In addition to implementation of centrally managed firewall and anti-virus (AV) programs for all business computers, all computers used in operations that touch instruments destined for customers maintain the latest virus definitions and are scanned regularly.

b. Strict virus control protocols have been enacted in manufacturing, service, support, sales, distribution and demonstration environments. These include the use of isolated LANs, control of removable memory devices, scanning of instruments and removable memory devices and/or reimaging hard drives, as appropriate depending upon instrument configuration.

c. Keysight-wide training of all personnel who come in contact with customer instruments to reinforce anti-virus security protocols. These employees include manufacturing, service, support, sales, distribution and demonstration equipment management personnel.

2. How does Keysight respond to reports of viruses on their instruments?

a. All reports of potential instrument infections are escalated to the Director Corporate Quality. In the event a customer reports an infection after receipt of a Keysight product OR Keysight reports that an instrument is infected upon receipt at Keysight (for service, or from demonstration), the following steps occur:

i. Immediate Mitigation/Vector Control – Keysight works with the customer to mitigate the threat, by either taking the unit back and replacing it with a clean instrument, or working with the customer to scan and eliminate the viral threat.

ii. Trace source and extent of the infection to understand where and when the virus was introduced, the nature of the virus and potential for damage. Where appropriate, a thorough report of findings is presented with recommendations for corrective actions to prevent the future spread of viruses.

iii. Once the threat is thoroughly understood and the infection vectors are determined, internal preventative actions are updated to adjust to the new threat(s). If it is determined that the virus originated outside of Keysight, Keysight will recommend actions to protect our customers' instruments.

If you have questions, please contact Keysight.