**General Information**

TeamViewer is an S/W to access and control a remote PC by Internet connection. Access of your PC includes the possibility to see/change your data files and programs as long as they are not password protected. Data transfer will be possible as well.

Before authorization make sure that you have done Back-ups of all relevant data and that all programs are closed which are not required!

In case of TeamViewer session done by Shimadzu various Service activities such as troubleshooting S/W Installations, Instrument Control, Support for method developments … can be done.

Starting such a session always requires your approval. When the session is started your monitor will be displayed on our PC and we can do remote control of your PC. In case of trouble you can stop any time the session by activating the Close Symbol in the TeamViewer program.

Once the session is stopped, we have no longer access to your PC. Restarting the session requires a new Password created from your TeamViewer Client and forwarded from your side to us.

Following information is taken from the TeamViewer Website: (<https://www.teamviewer.com/en/products/security.aspx>)

Security and Privacy:

TeamViewer includes encryption based on RSA private-/public key exchange and AES (256 bit) session encryption. This technology is based on the same standards as https/SSL and is considered completely safe by today's standards.

The key exchange also guarantees full, client-to-client data protection. This means that even our routing servers will not be able to read the data stream.

Access protection:

In addition to the PartnerID TeamViewer generates a session password that changes with every software start to provide additional security against unauthorized access to a remote system.
Security relevant functions like file transfer require additional, manual confirmation of the remote partner.
Also it is not possible to invisibly control a computer. For data protection reasons the person sitting on the remote computer has to be able to detect when someone is accessing the machine.

Code Signature:

All program files are secured using VeriSign code signing technology. This allows you to verify the origin of the executables you received.

Additional Information:

* The customer is responsible for Data Safety using appropriate Virus Scanner/Firewall and Data backups.
* Shimadzu won´t be liable for any problems independent to the Remote Service Session.
* The TeamViewer Session will be recorded for Safety/Quality purposes.

**Authorization Declaration**

I am aware about the process of Remote Service by TeamViewer described in the same document.

By this authorization I request Shimadzu Europe GmbH (SEG) to start the TeamViewer session for Remote Service. I am aware that during this session SEG will access/control my PC.

I confirm that all relevant data are saved by back-ups, that I won´t leave the system/PC during remote session and that I will stop the remote session in case of trouble.

**Customer Data:**

|  |  |
| --- | --- |
| Company Name:  |  |
| Customer Name: |  |
| Phone No. : |  |
| E-mail:  |  |

Only for users of Testing Machines (except Hardness Testers and Particle Size Analyzers) :

Herewith I confirm that the Testing Machine has been switched off and that the USB cable between Machine and PC has been disconnected:

□ Yes, I confirm. □ No, I do not confirm.

Please send the completed declaration to Shimadzu. When downloading the actual TeamViewer QS (https://download.teamviewer.com/download/TeamViewerQS.exe) and starting the connection the session will start.

Signature Date