# NETWORK SECURITY NOTICE

It was brought to the attention of The Vision Council that a number of our members may face security concerns during the sharing of lens data. As information is shared between your LMS and the LDS/ Calculation Server, there are numerous companies with outdated network security settings that may expose them to corruption or breaches in data security.

In order to conform to industry standard security recommendations we recommend upgrading from TLS 1/1.1 to TLS 1.2:

- Transaction Later Security (TLS) encrypts the communication between a client LMS and a LDS/ Calculation Server.
- TLS 1.1 and 1.0 are now vulnerable to a range of attacks which could be used to gain plain text data from encrypted communication.
- TLS 1.2 is necessary to ensure that customer data is secure whilst in transit and is required for PCI compliance (Payment Card Industry -> All credit card transactions in the US).
- TLS 1.2 has been available for nearly 10 years so this is not new technology.
- Most major websites have implemented (or are currently implementing) the upgrade; e.g. Microsoft has made TLS 1.2 mandatory for Office 365 services.
- As customer data and health records may be transmitted in some LMS configurations it is essential that an encryption method which is not vulnerable be used.

If you have any questions regarding the above information, please contact your LMS vendor or your network administrator. For more guidance from The Vision Council on the issue, please reach out to Michael Vitale at **mvitale@thevisioncouncil.org**.

*The Vision Council would like to thank Carl Zeiss Vision and Adrian Blackburn for bringing this issue to the attention of the industry.*