CRITICAL PRODUCT SECURITY INFORMATION FOR INSTALLERS, COMMISSIONING ENGINEERS AND USERS

VESDA VLP, VLS, VLC (VN), VRT, VHH AND VHX-02X0

WARNING: Failure to comply with the requirements below exposes the system to malicious interference which could disable alarm reporting

Commissioning Requirements

- All VESDAnet wiring and connection ports must be secured against unauthorized access.
- VESDA devices including HLIs must not be accessible from the Internet. Any provision of remote access to VESDA devices must be subjected to a full cyber security risk assessment and regular review.
- Restrict access to HLI devices to authorized personnel only.
- Default PIN codes must be changed as part of the initial configuration.
- Display devices with buttons should be secured against unauthorized access or have button lockout feature enabled.
- The security of the interface intended for connection to 3rd party equipment on Open HLI products, must be enforced by the commissioning authority.

System Maintenance Requirements

- If Xtralis product requires firmware upgrade, ensure that the upgrade package is genuine and obtained directly from Xtralis.

Doc. No. 33254_02
Part No. AD33254-001
June 2021