CRITICAL PRODUCT SECURITY INFORMATION FOR INSTALLERS, COMMISSIONING ENGINEERS AND USERS

OSID-DE

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

Xtralis takes Cyber Security seriously. To ensure your OSID-DE solution is not compromised by an external threat, please follow the instructions and take the following precautions.

Commissioning Requirements

- All wiring and connection ports must be secured against unauthorized access.
- OSID-DE devices must not be accessible from the Internet.
- OSID-DE is not intended for remote access and no such facility should be provided.
- Restrict access to OSID-DE devices to authorized persons.
- Access to PCs on which Xtralis software is installed must be restricted to authorized persons.
- Xtralis PC software such as OSID Diagnostics, must only be installed on PCs with current active Windows support from Microsoft.

System Maintenance Requirements

- OSID-DE Imager diagnostic port must be used only for diagnostic purposes or firmware upgrade and must not be permanently connected to any device.
- Limit use to authorized persons.
- If an OSID-DE device requires firmware upgrade, ensure that the upgrade package is genuine and obtained directly from Xtralis.

Doc. No. 35556_03
Part Number: AD35556-000
November 2020