LECS REFERENCE, COMPLIANCE AND CERTIFICATION SUPPORT TABLE

Q1/2024

ISO 27001

ISO 27001 is an international standard published by the International Standardization Organization (ISO). It describes how to manage information security in a company. It was written by the world's top experts in the field of information security and provides methodology for the implementation of information security management in an organization. The focus of ISO 27001 is to protect the confidentiality, integrity, and availability of a company's information. The latest revision of this standard was published in 2022 and its full title is now ISO/IEC 27001:2022. The standard can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large.

CATEGORY	SUBCATEGORY	LECS TECHNOLOGY or LECS SOC Service	HOW IT HELP
A.8.7 Protection against malware	Protection against malwareshall be implemented and supported by appropriate user awareness.	All LECS family application/ appliance	The LECS device has an engine that constantly monitors the traffic it encounters, and works to detect network malware and infections that are proliferating.
A.8.15 Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	All LECS family application/ appliance	LECS performs a double logging operation, both physical and in the cloud. These logs constantly allow you to monitor what happens not only in the security field but also for telemetry for network debug operations. In addition, the long-lastingLOGs allow you to trace anyAPTs.
A.8.20 Networks Security	Networks and network shall be managed and controlledto protect information in systems and applications.	All LECS family application/ appliance	The LECS device has an engine that constantly monitors the traffic it encounters, and works to detect network malware and infections that are proliferating.

A.6.8 Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	All LECS family application/ appliance	The LECS device has an engine that constantly monitors the traffic it encounters and works to detect network malware and infections that are proliferating. It also performs a myriad of data stream analyzes, exploits, shellcodes, and more. The device report immediately salient security events to the user with different channels.
A.5.26 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	All LECS family application/ appliance	The LECS Service directly supports the safety directives adopted by the company, directly supporting it in its implementation. The device already isolated, with an automatic air-ga the threat intervening and automatically. With the LOGs, actors and compromising factors can then be analyzed to implement the best cleaning and post-infection strategy.