LECS REFERENCE, COMPLIANCE AND CERTIFICATION SUPPORT TABLE
Q1/2022

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 2013 and its full title is now ISO/IEC 27001:2013. 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.12.2.1 Controls against malware	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	LECS LECS + LECS 4.0 LECS SaaS LECS Tool	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.12.3.1 Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy	LECS SOC Service	The LECS SOC service allows you to keep up with all the backup and monitoring policies of the same. Specifically, LECS & Backup Service service strives to constantly and periodically check the redundancy of important company and PA data.
A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	LECS LECS + LECS 4.0 LECS SaaS LECS Tool	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-lasting LOGs allow you to trace any APTs.
A.12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	LECS Tool LECS SOC Service	LECS tool and LECS SOC, allows you to keep track of installed software, also verifying possible IOCs (indicator of compromise).
A.13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.	LECS LECS + LECS 4.0 LECS SaaS LECS Tool LECS SOC Service	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.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	LECS LECS + LECS 4.0 LECS SaaS LECS Tool LECS SOC Service	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.
A.16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	The SOC 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.