CYBERSECURITY™
MADE IN EUROPE

Conformity declaration with ENISA's 'Indispensable baseline security requirements for the procurement of secure ICT products and services'[1]

"CYBERSECURITY MADE IN EUROPE"

Principle	Requirement	Fulfilled (yes/no)	Explanation[2]
Security by Design	The provider shall design and pre-configure the delivered product such that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations.		
Least Privilege	The provider shall design and pre-configure the product according to the least privilege principle, whereby administrative rights are only used when absolutely necessary, sessions are technically separated and all accounts will be manageable.		
Strong Authentication	The product shall provide and support strong authentication mechanisms for all accounts. If authentication is unsuccessful the product shall not allow any user specific activities to be performed.		
Asset Protection	The product shall provide adequate level of protection for critical information assets during storage and transmission.		
Supply Chain Security	The provider shall give means to ensure that the product is genuine, cannot be tainted during operation, and its integrity are warranted throughout the product's lifecycle.		

[1] ENISA, 'Indispensable baseline security requirements for the procurement of secure ICT products and services', 21 January 2017. Accessible: https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services.

[2] Please explain how you fulfil this requirement and, respectively, if you do not fulfil give an explanation why not or why it may not be applicable.

Documentation Transparency	The provider shall offer comprehensive and understandable documentation about the overall design of the product, describing its architecture, functionalities and protocols, their realisation in hardware or software components, the interfaces and interactions of components with each other and with internal and external services, in order to be able to implement and use the product in the most secure way possible.		
Quality Management	The provider shall be able to provide evidence that a managed security by design approach has been adopted, including documented secure software development, quality management and information security management processes.		
Service Continuity	The provider shall guarantee support throughout the agreed lifetime of the product such that the system can work as agreed and is secure.		
EU Jurisdiction	The provider shall accept that all contracts refer to EU Member State law and only EU Member State law and place of jurisdiction in an EU Member State country and only an EU Member State country, including those with subcontractors.		
Data Usage Restriction	The provider shall explicitly declare, justify and document, context and purpose wise, all data collection and processing activities that take or may take place, including relevant legal obligations stipulating them.		