Profile Baseline: baseline eligibility criteria matched



This is the entering acceptance level to enable offer visibility and sharing through the DOME ecosystem. To match this level the provider must provide visibility (through **self-attestations**[2]) of the implementation of the following **mandatory compliance criteria under the following categories:**

1- DATA PROTECTION AND MANAGEMENT

Criterion DP-1: The Provider shall offer the ability to establish a written contract under Union or EU/EEA/Member State law and specifically addressing GDPR requirements.

Criterion DP-2 : The Provider shall define in writing the roles and responsibilities attributed to each party in the offerings.

Criterion DP-3: For each offering, the Provider shall clearly define the technical and organizational measures in accordance with the roles and responsibilities of the parties, including an adequate level of detail.

Criterion DP-4: The Provider shall not access Customer Data unless authorized by the Customer or when the access is in accordance with applicable laws to the contract.

Criterion DP-5: The Provider offering is compliant with all the requirements of applicable laws and regulations concerning the protection of personal data, and specifically the General Data Protection Regulation (Regulation (EU) 2016/679).

2- CYBERSECURITY

Criterion CS-1: Organization of information security: Plan, implement, maintain and continuously improve the information security framework within the organisation.

Criterion CS-2: Information Security Policies: Implement adequate and updated information security policies and procedures aligned with the security requirements needed to support the Offering operational requirements.

Criterion CS-3: Risk Management: Ensure that risks related to information security are properly identified, assessed, and treated, and that the residual risk is acceptable to the Provider.

Criterion CS-4: Human Resources: Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation’s assets are protected in the event of changes in responsibilities or termination of employment contract.

Criterion CS-5: Asset Management: Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.

Criterion CS-6: Physical Security: Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.

Criterion CS-7: Operational Security: Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.

Criterion CS-8: Identity, Authentication and access control management: Limit access to information and information processing facilities.

Criterion CS-9: Cryptography and Key management: Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

Criterion CS-10: Communication Security: Ensure the protection of information in networks and the corresponding information processing systems.

Criterion CS-11: Portability and Interoperability: The provider shall provide a means by which a customer can obtain their stored customer data, and provide documentation on how (where appropriate, through documented API's) the customer can obtain the stored data at the end of the contractual relationship and shall document how the data will be securely deleted from the provider's system in what timeframe.

Criterion CS-12: Change and Configuration Management: Ensure that changes and configuration actions to information systems maintain an adequate security of the delivered cloud service.

Criterion CS-13: Development of Information systems: Ensure information security in the development cycle of information the concerned cloud offering.

Criterion CS-14: Procurement Management: Ensure the protection of information that suppliers of the provider can access and monitor the agreed services and security requirements.

Criterion CS-15: Incident Management: Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.

Criterion CS-16: Business Continuity: Plan, implement, maintain and test procedures and measures for business continuity and emergency management.

Criterion CS-17: Compliance: Take positive and affirmative steps to ensure compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.

Criterion CS-18: Dealing with information requests from government agencies: Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of Customer Data.

Criterion CS-19: Offering's security: Provide appropriate mechanisms for cloud customers to enable Offering security. Ensure that the by-default configuration of the offerings is secure.

[2] **Compliance Self-attestation form_CSP_DOME March 2025.docx**

Revision #18
Created 4 June 2024 13:31:13
Updated 3 December 2025 10:35:25 by Juncal Alonso