MECHEM

ISMS POLICY	Document No:	POL-100
	Revision:	00
	Approval Date	10.03.2022

As **Mechem SA.** we are aware that we are responsible for protecting the data obtained, used or emerging during the realization of our business processes in accordance with the applicable national or international laws and regulations and the principles of accepted information security standards and to take all necessary measures in this regard. Within this understanding, it has implemented the necessary information security management systems within the institution by taking legal and administrative measures;

We are committed to continuing

- Continuous improvement and awareness of information security,
- The participation of all our employees and business partners,
- With the aim of protecting all physical and electronic data processed and obtained.

Based on the principles of Confidentiality, Integrity and Accessibility of data security, on the basis of the KVK Law, Personally identifiable information (PII) data classifications;

- Necessary authorization and task definitions will be made within the scope of information security.
- An Information Systems Management Strategy will be established.
- Compliance with Information Security Standards and relevant legal regulations will be ensured.
- Threats, vulnerabilities and risks against these assets will be identified and managed through the Asset and Data Inventories created.
- Continuous review and improvement of the Information Security Management System and KVKK compliance will be ensured.
- Trainings will be provided to ensure technical and behavioral integrity in order to increase Information Security awareness.
- Sub-policies will be determined to support our basic information security policy.
- The Plan, Do, Check and Act lifecycle will be implemented.
- All responsibility units will act with information security awareness. Information security plans will be created and implemented for the areas of responsibility.
- Compliance with IT security frameworks from our partners and customers will also be ensured.

Within the scope of Personal Data Security;

- PII data inventory will be prepared
- PII data will be determined
- PII data will be reduced as much as possible

• PII data will be stored in appropriate secure areas and process security will be ensured.

All these commitments will be ensured by our;

- Flexible,
- Expandable,
- Traceable,
- Transparent,
- Proactive,
- Continuously updated

information technology strategy and our policy of employing expert technical personnel supported by up-to-date trainings.