

**Company Announcement**  
**No.019/2024**  
**Policy TISAX**

Aeroklas places great importance on protecting data throughout all operations involving critical information, including transfer, storage, usage, and destruction. This ensures that throughout the data lifecycle, information related to the automotive industry and personal data is adequately protected and managed. To build confidence among stakeholders, the following policy has been established:

1. Purpose : The purpose of this policy is to establish the framework for managing information security within the organization in accordance with TISAX requirements. This ensures the protection of sensitive information and the trust of our stakeholders.
2. Scope : This policy applies to all employees, contractors, and third-party service providers who access, store, or manage information on behalf of the organization. It covers all forms of information, maintains including digital, physical and verbal.
3. Information security objectives : The organization aims to:
  - 3.1 Protect the confidentiality, integrity and availability of information.
  - 3.2 Ensure compliance with applicable laws and regulations.
  - 3.3 Establish clear roles and responsibilities for information security.
  - 3.4 Promote a culture of security awareness among employees.
4. Risk management : The organization will conduct regular risk assessments to identify and evaluate information security risks. Appropriate controls will be implemented to mitigate identified risk and the risk assessment process will be reviewed periodically.
5. Access control : Access to sensitive information will be restricted to authorized personnel only. Access control measures including user authentication will be implemented to protect against unauthorized access.
6. Incident management : All information security incidents must be reported immediately. The organization will maintain and incident management process to respond to and investigate incidents and corrective action will be taken to prevent future occurrences.
7. Training and Awareness: Employees will receive regular training on information security policies and best practices. Awareness programs will be conducted to ensure that employees understand their responsibilities regarding information security.
8. Compliance and review: The organization commits to complying with TISAX requirements and will evaluate the effectiveness of the information security management system. This policy will be reviewed annually and updated.
9. Responsibilities: The management team is responsible for the implementation of this policy, while all employees must comply with.
10. Communication: This policy will be communicated to all employees and relevant stakeholders.

Announcement As of October 15, 2024



( Mr.Ekawat Vitoorapakorn )  
Managing Director

Aeroklas Co., Ltd. 東方國際有限公司