FORD OTOSAN
INFORMATION SECURITY POLICY

1. PURPOSE

The purpose of this Ford Otomotiv Sanayi A.Ş. Information Security Policy (hereinafter briefly the "Policy") is, regarding the establishment, operation, management and use of the information systems of Ford Otomotiv Sanayi A.Ş. (hereinafter briefly "**Ford Otosan**"); to define the roles and responsibilities required for the operation of information security processes to ensure the confidentiality, integrity and availability of information, to establish processes for managing risks related to information systems, to establish controls and to ensure governance and oversight.

2. SCOPE

All Ford Otosan employees, Ford Otosan Authorized Services and Dealers, suppliers, contractors, subcontractors and other third parties and their personnel working with Ford Otosan are covered by this Policy.

3. DEFINITIONS

In this document;

Privileged User / Privileged Account: Refers to user accounts that allow activities requiring high privileges, such as changing system and security settings and performing critical operations,

Principle of Least Privilege: Refers to an authorization approach aiming to grant users the lowest access level necessary to perform their duties,

Information Security Management System (ISMS): Refers to a systematic approach adopted to manage Ford Otosan's sensitive and important information,

Information Security Forum: Refers to the Ford Otomotiv Sanayi A.Ş. Information Security Management System Committee formed with the participation of the Digital Products and Services Leader, DPS Security and Risk Leader, Infrastructure and Operations Leader, Internal Audit Leader, Corporate Risk Management Leader, Quality Platform Area Leader, and the leaders of the departments within the scope of the ISMS.

Information Systems Security Officer: Refers to the Information Systems Security Officer appointed by the Senior Management within the scope of the Communiqué,

Information Technologies and Information Security Violation Management Team: Refers to Ford Otosan team, consisting of the DPS Security and Risk Team, Solution Center Product Owner, and Infrastructure and Operations Leader, that records and investigates information security breaches,

Information / Information Assets: Refers to all information belonging to Ford Otosan and all electronic (software, hardware, communication and security infrastructure, archive systems, etc.) and physical (facilities, rooms, cabinets, etc.) environments required for the use of such information, and all employees accessing information,

Digital Products and Services Leader: Refers to Ford Otomotiv Sanayi A.Ş. Digital Products and Services Leader,

Geographical Separation: Refers to positioning primary and secondary systems in different locations so that they are not simultaneously exposed to the same physical risks,

Employee(s): Refers to all personnel working under an employment contract within Ford Otosan,

Early Warning Mechanisms: Refers to monitoring and alerting systems used for rapid detection of unauthorized access, unusual activities, or security threats,

Disaster Recovery Test (DR Test): Refers to planned test activities performed to verify operability of information systems in backup environments in case of disasters,

Ford Otosan: Refers to Ford Otomotiv Sanayi A.Ş.,

Ford Otosan KVK Committee: Refers to the committee formed under the chairmanship of the Digital Products and Services Leader within the scope of the Personal Data Protection Law No.6698 and consisting of Information Technologies, Legal and Compliance Leadership , Internal Audit Management and assigned KVK officers in all departments,

Service Inventory: Refers to the inventory in which the scope, components, ownership and security classification of all services provided within the information systems are recorded,

Third Parties: Refers to Ford Otosan Authorized Services and Dealers, suppliers, contractors, sub-employers, other third parties and their personnel working with Ford Otosan,

Policy: Refers to Ford Otomotiv Sanayi A.Ş. Information Security Policy,

Process Inventory: Refers to the inventory in which business processes within the information systems are defined, documented, classified and kept up to date,

Communiqué: Refers to the Capital Markets Board of Türkiye's relevant communiqués and regulations on Information Systems Management, including Communiqué No. VII-128.9 published on 05.01.2018 and the amendments introduced by Communiqué No. VII-128.10 effective as of 13.03.2025,

Senior Management: Refers to the Ford Otosan Leader and the Digital Products and Services Leader authorized by the Ford Otosan Board of Directors.

Board of Directors: Refers to Ford Otosan Board of Directors,

4. GENERAL PRINCIPLES

This Information Security Policy commit to;

a) Comply with all legal regulations, Ford Motor Company and Koç Group policies, including the obligations imposed on companies publicly traded with a legal notification.

b) Protect and ensure the confidentiality, integrity and availability of Information and Information Assets (see also Article 9),

c) Prevent uncontrolled and unauthorized access to Information and Information Assets (see also Article 8),

d) Identify risks on Information and Information Assets and ensure that risk mitigation activities are carried out regularly and continuously,

e) Establish and maintain services that will support business continuity in information technology infrastructure and applications (see also Article 11),

f) Provide corporate learning by taking measures to prevent information security violations,

g) Provide information security awareness training to employees and third parties to increase awareness

h) Ensure continuous improvement of the Information Security Management System.

5. RESPONSIBILITIES

5.1. Board of Directors

a) Approval of the Information Security Policy,

b) Establishing effective and sufficient controls on information systems within the scope of the policy,

c) Determining the Senior Management who is responsible for the implementation of the information security policy,

d) Approval of the project development reports prepared to follow the progress of the work during the development, change or acquisition of information systems,

are the responsibilities of the Board of Directors.

5.2. Senior Management

5.2.1. The Board of Directors has designated the Ford Otosan Leader and the Digital Products and Services Leader as Senior Management within the scope of this Policy.

5.2.2. Senior Management responsibilities are;

a) Preparing the Information Security Policy to be approved by the Board of Directors,

b) Ensuring the implementation of the policy,

c) Reviewing critical projects for the use of new information systems and approving them, taking into account the manageability of the risks associated with them.

d) Demonstrating the necessary determination to bring information security measures to an acceptable level allocating sufficient resources for activities to be carried out for this purpose.

e) Establishing the necessary mechanisms for the following activities:

i. Annual review and approval of information security policies and responsibilities,

ii. Identifying potential risks and impacts on information systems and processes, within this framework, performing risk management process which includes defining of activities to mitigate identified risks.

iii. Monitoring and annual evaluation of information security incidents.

iv. Carrying out activities and providing training to increase awareness of information security for all employees.

f) Establishing processes and procedures for managing risks related to information systems within Ford Otosan, and performing follow-ups and audits regarding their operability,

g) Assigning an Information Systems Security Officer who is responsible for the fulfillment and follow-up of the processes and procedures related to information systems security, who reports to the senior management about the risks related to information systems security and the management of these risks, and has sufficient technical knowledge and experience.

h) Preparing business continuity plans in order to ensure the continuity of all critical processes according to business priorities and to determine acceptable downtime and maximum acceptable data loss for critical business processes in the plan,

i) To ensure that security risks related with information systems are adequately managed within the scope of information security policy; ensuring the development, operation and up-to-dateness of the controls regarding the measures that will ensure the confidentiality, integrity and accessibility of the information systems and the data,

j) Establishing an monitoring mechanism that will allow the risks of outsourced services to be adequately assessed and managed within the scope of information systems, and to conduct effective relations with organizations that provide outsourced services,

k) Identifying the responsible persons for outsourced services, who have sufficient knowledge and experience to operate the oversight mechanism (see Article 10).

5.3. Information Security Forum

Information Security Forum, under the leadership of Senior Management; is responsible for

a) Reviewing and approving sub-policies and other supportive standards and processes in order to identify the application principles within the scope of this Information Security Policy,

b) To follow the fulfillment of information security requirements,

c) Analyzing identified internal security violations and to ensure that they are controlled with appropriate disciplinary rules,

d) Planning and implementing the necessary activities to keep the risks to information assets at an acceptable level.

5.4. Information Systems Security Officer

5.4.1. Ford Otosan Information Systems Security Officer shall have technical knowledge and at least 5 years of experience in information systems internal control, audit, governance or security, shall not have any operational duties related to fulfilling information systems management requirements, and shall work directly under Senior Management.

5.4.2. *Information Systems Security Officer is responsible for;*

a) Establishing, submitting for approval and publishing procedures and instructions related to information security,

b) Performing, monitoring and auditing the requirements of information systems security processes and procedures,

c) Managing risks related to information systems security by defining and evaluating the risks, determining risk mitigating activities, following the timely completion of these activities and reporting risks and related activities to Senior Management every 2 months,

d) Auditing the processes regarding information security and reporting the violations to the Internal Audit Management and Human Resources and Transformation Leaderhisp when necessary.

5.5. Employees

Employees are responsible for complying with the Information Security Policy, related Ford Otosan procedures and the information security rules specified in the legislation, and notifying the Digital Products and Services and Information Security Violation Management Team via alert@ford.com.tr as soon as possible.

5.6. Third Parties

During the business relations with Ford Otosan, they are responsible for protecting all kinds of Information and Information Assets belong to Ford Otosan in accordance with the criteria determined by Ford Otosan, taking the required measures, and notifying Ford Otosan via alert@ford.com.tr as soon as possible in case of any information security deficiencies and violations they encounter.

6. RISK MANAGEMENT

Ford Otosan applies the **ISMS Risk Management Procedure** in alignment with the Corporate Risk Management Process in order to identify, evaluate and classify information security risks, take necessary risk mitigation measures and monitor these activities.

Information and Information Assets and their criticality are handled within the scope of risk assessment by calculating the effects of threats and probability of occurrence and risk matrices are created.

Risk matrices are regularly reviewed within the framework of the Corporate Risk Management Process and handled in the Corporate Risk Management Committee.

7. INFORMATION ASSET, SERVICE AND PROCESS INVENTORIES

An inventory of all Information and Information Assets within Ford Otosan is created and kept up to date, covering at least the description, owner, user, security classification, backup information and similar minimum elements.

A service inventory for all services provided within the information systems and a process inventory for the information systems processes are prepared; such inventories are reviewed and updated periodically.

Obligations regarding the creation, management and security of these inventories are fulfilled in accordance with relevant procedures.

8. ACCESS AND AUTHORIZATION MANAGEMENT

In access to Ford Otosan information systems, segregation of duties and the principle of least privilege are applied in accordance with Article 11 of the Communiqué. Accordingly, authorization definition, approval and usage processes, as well as development, test and production activities, are carried out by different persons or units to the extent possible, and end-to-end execution of critical operations by a single person is prevented.

User authorizations are regularly reviewed and updated in terms of business requirements. In case of role change or termination, relevant access rights are revoked without delay.

The use of common, default or shared user accounts is prevented except for mandatory cases; where mandatory, responsible persons are clearly identified and audit trails (logs) for all actions performed through such accounts are retained.

Local administrator rights are not granted to users; however, they may be granted temporarily based on business justification and with the approval of the Information Systems Security Officer. Separate user accounts are used for privileged operations, and activities related to such accounts are recorded.

Unusual, unexpected or unauthorized access attempts are monitored through early warning mechanisms and security controls, and necessary preventive measures are taken.

9. DATA CONFIDENTIALITY AND CRYPTOGRAPHY MANAGEMENT

Protecting confidentiality, integrity and availability principles is essential for all data transmitted, processed, stored and accessed within Ford Otosan information systems. In particular, sensitive data and customer information are protected using appropriate cryptographic methods.

Proven and up-to-date encryption algorithms are used in implementing cryptographic controls; usage of encryption keys that are compromised, broken or stolen is immediately ceased.

Processes for generation, storage, distribution, access and destruction of encryption keys are controlled; key management is regularly updated and audited in periods defined according to the criticality level of the data and the related operation.

Responsibilities related to data security are defined within relevant procedures, and compliance is overseen by the Information Systems Security Officer.

10. OUTSOURCED INFORMATION SYSTEMS SERVICES MANAGEMENT

Ford Otosan takes the necessary managerial and technical measures to ensure that final responsibility and decision-making authority in outsourced information systems services remain with Ford Otosan.

Before signing a contract with an external service provider, a technical adequacy report is prepared by evaluating the candidate provider's technical infrastructure, financial capability, information security controls, human resources and sectoral experience, and submitted to Senior Management for approval.

Senior Management assigns responsible persons with sufficient knowledge and experience to monitor performance, reliability, security level and business continuity of critical outsourced services. Such responsible persons prepare an evaluation report at least once a year and report to Senior Management.

Outsourcing contracts include, at minimum, the elements specified in Article 19/3 of the Communiqué.

Depending on the outsourced service, necessary security controls are ensured by considering data privacy, regulatory compliance and business continuity requirements.

11. BUSINESS CONTINUITY AND DISASTER RECOVERY MANAGEMENT

Ford Otosan prepares, maintains and implements business continuity and disaster recovery plans to ensure uninterrupted and secure service delivery of information systems.

Primary and secondary information systems infrastructures are positioned so as not to be simultaneously exposed to the same risks, including natural disasters and environmental incidents, and necessary geographical separation is ensured.

Disaster Recovery Tests are performed at least once a year (and more frequently if necessary) to verify operability of critical information systems through backup infrastructure. The following are recorded and reported to Senior Management:

- Test date and scope
- Participants
- Implementation results

- Identified improvement areas

Business continuity and disaster recovery plans are revised when necessary based on test results and are continuously improved in line with new risks.

12. DATA CENTER AND SYSTEM HOSTING MANAGEMENT

Primary and secondary infrastructures of information systems used within Ford Otosan are positioned by taking business continuity and information security requirements into account; planning and implementation related to continuity of information systems are carried out within the scope of Articles 6 and 27 of the Communiqué.

Under Communiqué No. VII-128.10 on Principles and Procedures Regarding Information Systems Management, publicly traded companies are not required to host information systems within the borders of the Republic of Türkiye. Accordingly, Ford Otosan is authorized to use domestic or international data centers, co-location or cloud services based on operational needs.

In data processing and storage activities, availability, security, compliance, stability, data integrity and personal data protection requirements are essential. Where services are procured abroad, data security, compliance, business continuity and disaster recovery measures are established in accordance with relevant procedures and are regularly overseen.

13. STANDARDS

The Ford Otosan Information and Cyber Security Control Standards document covers information security processes, policies, procedures and standards.

14. PROTECTION OF PERSONAL DATA

It is essential that this Policy and related Ford Otosan procedures are carried out in accordance with the provisions of the **Personal Data Protection Law No.6698, Ford Otosan Personal Data Protection Policy** and **Ford Otosan KVK Committee Working Principles Instruction**. The Senior Management and Information Systems Security Officer works together with the Ford Otosan KVK Committee on technical measures to be taken for the security of personal data.

15. AUDIT

Suspicious events and findings detected as a result of Ford Otosan's audits or notifications regarding information security violations are evaluated together with Ford Otosan Internal Audit Department and Information Systems Security Officer. In case a violation is detected, the case is properly forwarded to the Ford Otosan Human Resources and Transformation Leader by the Information Systems Security Officer in order to carry out the relevant disciplinary procedure.

16. UPDATING AND ANNOUNCEMENT OF THE POLICY

The Digital Products and Services function is responsible for updating this Policy according to changing needs and legislation. The Policy is reviewed at least once a year and updated when necessary. The current version of the Policy is announced to employees and made available on the Company portal and the Company’s corporate website.

17. VALIDITY

This Policy, which first entered into force on 11.09.2013, was revised in line with changing needs and legislation and updated upon approval by the Board of Directors on 22.03.2021.
The Policy was lastly updated by the Board of Directors resolution dated 30.12.2025 and numbered 2025/33, entered into force as of that date, and replaced all previous versions.

Revision	Date	Description
1	22.03.2021	Update
2	30.12.2025	Update