FORD OTOSAN

FORD OTOMOTİV SANAYİ A.Ş.
INFORMATION SECURITY POLICY

FORD OTOSAN

1. PURPOSE

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

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;

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 Ford Otomotiv Sanayi A.Ş. Information Security Management System Committee which is formed with the participation of Ford Otosan CFO, Information Technologies Director, IT Audit, Compliance and Risk Management Manager, IT Infrastructure and Operations Manager, IT Cyber Security Team Leader, Internal Audit Manager, Risk Management Manager, Total Quality Manager and departments managers of the scope of ISMS,

Information Systems Security Officer: Refers to Ford Otosan IT Audit, Compliance and Risk Management Manager appointed by the Senior Management within the scope of the citation,

Information Technologies and Information Security Violation Management Team: Refers to Ford Otosan team, consisting of the IT Audit, Compliance and Risk Management Team, IT Cyber Security Team, IT Service Desk Team Leader and Infrastructure and Operations Manager, that investigates reported and/or detected information security violations,

Information / Information Assets: Refers to all electronic (software, hardware, communication and security infrastructure, archive systems, etc.) and physical (facilities, rooms, cabinets, etc.) environments and all employees and third parties accessing to information,

Information Technologies Director: Refers to Ford Otomotiv Sanayi A.Ş. Information Technologies Director,

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

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

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

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,

Citation: Refers to The Capital Markets Board's Information Systems Citation (VII-128.9) published on 05.01.2018,

Senior Management: Refers to General Manager and Information Technologies Director of Ford Otosan authorized by Board of Directors of Ford Otosan,

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) Provide the confidentiality, integrity and availability of Information and Information Assets,

c) Prevent uncontrolled and unauthorized access to Information and Information Assets,

d) Define the risks on Information and Information Assets, ensuring 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

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) 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. General Manager and Information Technologies Director of Ford Otosan has been assigned as the Senior Management by the Board of Directors 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 the 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 reviewing of informartion security incidents.

iv. Carrying out activities and providing trainings 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 closely monitor the accessibility, performance, quality of the service, security breach incidents within the scope of this service and security controls of the outsourcing organization, financial conditions and compliance with the contract.

5.3. Information Security Forum

Information Security Forum, under the leadership of the 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 "IT Audit, Compliance and Risk Management Manager" was assigned by the Senior Management as Information Systems Security Officer.

5.4.2. Information Systems Security 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 activies to the Senior Management every 2 months,

d) Auditing the processes regarding information security and reporting the violations to the Internal Audit Management and Human Resources Directorate 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 Information Technologies 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 is responsible for protecting all kinds of Information and Information Assets belongs 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 carries out **GPRBT-062 - Ford Otosan ISMS Risk Management Procedure** in line 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. STANDARDS

The **BT-PM - Ford Otosan Information Security Control Standards** document covers information security processes, policies, procedures and standards.

8. 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**.

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.

9. 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 Ford Otosan Human Resources Directorate by the Information Systems Security Officer in order to carry out the relevant disciplinary procedure.

10. UPDATING AND ANNOUNCEMENT OF THE POLICY

The Information Technologies Directorate is responsible for updating this Policy according to the changing needs and legislation. The policy is also reviewed within the periods specified in **GTYBT-006 - Information Security Forum Instruction**. The updated version of the Policy is made available on the Company portal and on the corporate website. It is also announced to the employees.

11. VALIDITY

This Policy, which came into force on 11.09.2013, has been updated and came into force after being approved by the Board of Directors on 22.03.2021.