COMPANY WITH
INFORMATION SECURITY
MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/IEC 27001

INFORMATION SECURITY MANAGEMENT SYSTEM
DNV
ISO/IEC 27001

Tata AutoComp Systems Limited –

Information and Cyber Security Policy Overview

1. Purpose

In the journey towards achieving Vision and Mission of the organization through Industry 4.0 and digitalization, Tata AutoComp understands the importance of securing business information and ensuring adherence to IT compliance requirements. Information Security and Cyber Security are essential in attaining the Cyber Excellence at Tata AutoComp.

Tata AutoComp has established a comprehensive Information Security Management System (ISMS) framework for managing and protecting organisation's information assets by ensuring the confidentiality, integrity, and availability of business information, while supporting business continuity, regulatory compliance, and stakeholder trust.

The purpose of spearheading Information & Cyber Security Policy under this framework, is to enable, facilitate & support the business of Tata AutoComp by reducing the risks related to unavailability, unauthorized modification, inappropriate use, or disclosure of business information which is entrusted by its customers, partners, suppliers, employees and other stakeholders.

2. Scope

Tata AutoComp Information & Cyber Security Policy applies to:

a) Group Office, all Business Units, Subsidiaries, Joint Ventures in India

b) All employees, contractors, and third-party service providers of Tata AutoComp

c) Assets purchased, leased, rented, or obtained as a service by Tata AutoComp

d) Business Information created, accessed, or processed using Information Technology or Operations Technology

e) Entities or personnel who can create, access, or process the information by having access to any of the IT/OT systems from anywhere

3. Policy and Commitment

We at Tata AutoComp Systems Ltd. are committed to protect the data and information available with us. We would continue to work towards keeping all the data and information safe and secure.

We would ensure the highest standard of integrity while processing or dealing with data and information using our Information Technology (IT) and Operational Technology (OT) systems.

Tata AutoComp shall strive to ensure Confidentiality, Integrity, Availability, and Privacy of information by:

- Maintaining an effective Information Security Management System (ISMS).
- Creating security awareness and security conscious culture.
- Ensuring adherence to ISMS Policies & Processes.
- Deploying appropriate technological and operational level controls.
- Complying with applicable contractual, legal & regulatory requirements related to Information Security.
- Continually monitoring and improving the effectiveness of ISMS.
- Ensuring & maintaining readiness of IT/OT systems during Business disruption
- Reporting, investigating & acting upon actual or suspected incidents, breaches related to information & cyber security.

Tata AutoComp has adopted industry-leading practices to build a robust, risk-based cybersecurity framework that proactively detects and responds to threats, ensuring the protection of critical assets.

Led by our Chief Information Officer (CIO) and supported by the Chief Information Security Officer (CISO), we conduct regular training sessions to enhance employee awareness of data privacy and security. All employees have access to our Policy, which outlines key guidelines for data handling and a clear escalation process for employees to report incidents, vulnerabilities, or suspicious activities.

Tata AutoComp committed to protecting the data and information available with us. We will continue to work towards keeping all the data and information safe and secure. We will ensure the highest standard of integrity while processing or dealing with data and information using our Information Technology (IT) and Operational Technology (OT) systems. Tata AutoComp is ISO 27001:2022 certified.

Board-level responsibility for overseeing information security matters is held by the Audit Committee, where Information and Cybersecurity issues are regularly reviewed and discussed.

Key Commitments

Tata AutoComp is committed to maintaining a robust, risk-based cybersecurity framework that proactively detects and responds to threats. Our key commitments include:

1. **Data Integrity & Protection**: Ensuring the confidentiality, integrity, and availability of all data
2. **Defined Responsibilities**: Assigning clear roles and responsibilities for information security across the organization
3. **Threat Monitoring & Response**: Proactively identifying and mitigating security threats
4. **Third-Party Security**: Enforcing security requirements for suppliers and partners through our ISMS Handbook
5. **Business Continuity**: Maintaining and testing business continuity and incident response plans

6. **Vulnerability Management**: Conducting regular vulnerability assessments and penetration testing
7. **Internal Audits**: Performing periodic internal audits of IT infrastructure and ISMS
8. **External Audits**: Undergoing independent audits annually to ensure compliance with ISO 27001:2022
9. **Incident Reporting**: Providing an escalation process for employees to report incidents, vulnerabilities, or suspicious activities and disclosing the total number of security breaches year-on-year
10. **Security Awareness**: Conducting regular training sessions to promote information security awareness

4. Data Privacy Practices

Tata AutoComp emphasizes ethical data handling through:

a) **Privacy by Design**: Embedding privacy into systems and processes from the outset

b) **Data Minimization**: Collecting only the data necessary for business operations

c) **Security Controls**: Using encryption, access controls, and secure storage to protect personal data

5. Supporting (Internal) Policies and Processes

a) ISMS Policies & Processes

b) ISMS Handbook for Suppliers (covers Information Security, Cybersecurity, Privacy Protection, anti-malware, cloud security, and cryptography)

c) Data Privacy Policy

d) ICT Readiness Framework for Business Continuity

e) Risk Management Processes

f) Information Transfer Policy

g) Backup and Restore Policy

h) Systems Acquisition and Secure Development Policy

i) Internal Audit Procedure

6. Review & Maintenance

Tata AutoComp ISMS Policies are reviewed annually or upon significant changes to the business or regulatory environment. The Chief Information Officer (CIO) is responsible for ensuring the Policy remains current and effective.

Date: 6th January, 2025

Ranjeet Kadam

Chief Information Officer,
Tata AutoComp Systems Limited