Information Security Policy

Disclaimer:

This document is solely for the information of CEAT and shall not be used, circulated, quoted, or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.

1 Introduction

CEAT is involved in the design and development of automotive tyres and tubes which are used by the leading automobile manufacturers and individual users of the nation. The complexity of technology and digitalization in the design and manufacturing process of manufacture of tyres and tubes of all kinds make it imperative to focus on the information security across all the departments and manufacturing facilities so that the systems at CEAT are resilient and able to withstand the cyber intrusions and attacks by inimical elements.

2 Scope & Applicability

This policy applies to all employees, contractors, third-party service providers, and any other personnel with access to CEAT information systems. It covers all information assets, including data, software, hardware, and network infrastructure.

3 Aim

The aim of this policy is to set the guiding principles for establishing information security in the organisation and define the baseline security guidance that is appropriate for securing the IT infrastructure, underlying applications, processes, employee, vendor, customer and other stakeholders' data/information of Company in line with industry good practices.

4 Information Security Objectives

Following are the basic information security objectives which must be achieved by CEAT through implementation of this policy:

- Confidentiality – Information assets are accessible only to those authorized to have access (i.e., protected from unauthorized disclosure /modification/deletion or (un)intended leakage of personal data and sensitive data).
- Integrity – Information assets are accurate, complete and processed correctly (i.e., protected from unauthorized modification, which may include authenticity and non-repudiation).
- Availability – Information assets are resilient and accessible when required (i.e., protected from unauthorized disruption).
- Compliance – Information processing, including PII, to be carried out, by all stakeholders, in compliance with applicable and relevant legal, regulatory, statutory, and contractual obligations, at all times.

Following are the additional information security objectives which must be achieved at the company level:

- Prevent occurrence and recurrence of information security incidents by implementing security proactive/protective measures.
- Protection of information and reduce the risks of loss to the Company. Company stresses on securing the confidentiality, integrity and availability for critical information

- Create mechanisms for security threat early warning, vulnerability management and response to security threats
- Create processes, structures and mechanisms to generate necessary situational scenarios of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions.
- Enable effective prevention, investigation and prosecution of cybercrime, breach of data and enhancement of law enforcement capabilities through appropriate legislative intervention

5 Terms and Definitions

- Asset – Anything that has a value to the organization. In the context of this policy, an asset can be but not limited to hardware, software, people, site, information, intellectual property and so on.
- Availability – The property of an asset or resource being accessible and usable upon demand by an authorized entity.
- Computer Media – Includes all devices that can electronically store information. This includes but is not limited to diskettes, CD's, tapes, and portable hard disks.
- Confidentiality – property which ensures that information is accessible only to those authorized to have access.
- Continual Improvement – Continual Improvement refers to stage improvement programs that facilitate rapid improvement phases with intermediate stabilized phases.
- Control – A mechanism or procedure implemented to satisfy a control objective.
- Disaster Recovery (DR) - A plan for the early recovery of Business operations in the event of an incident that prevents normal operations.
- Information Security – Preservation of Confidentiality, Integrity and Availability of information.
- Information Security Incident – A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- Information Security Management System (ISMS) – That part of overall management system based on business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
- Integrity – Safeguarding the accuracy and completeness of information and processing methods.
- Risk – The combination of the probability of an event and its consequence.
- Residual Risk – The risk remaining after risk treatment.
- Risk Acceptance – Decision to accept risk.
- Risk Analysis – Systematic use of information to identify sources and to estimate the risk.
- Risk Assessment – Overall process of risk analysis and risk evaluation.
- Risk Evaluation – Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
- Risk Management – Coordinated activities to direct and control an organization regarding risk.

- Risk Treatment – Process of selection and implementation of measures to modify risk.
- Statement of Applicability (SoA) – The document which lists out the controls along with justification of inclusion/ exclusion. It may be noted that the SoA is not restricted to ISO 27001:2022 controls.

6 Policy

This policy has been created as a supplement to the RPG Group Information and Cyber Security Policy Ver 1.0 and incorporates the steps which are to be followed by CEAT to meet the requirements laid down by the automotive industry guidelines mentioned in TISAX Ver 6.03.

6.1.1. CEAT Information Security Policy Statement

CEAT is committed to providing a secure, reliable, and resilient environment to safeguard critical infrastructure, &- information of employees, businesses, partners, and customers through a well-defined cyber security framework aligning to international standards. It resolves to implement, maintain, and continually Improve cyber security best practices and controls to protect information assets by ensuring Confidentiality, Integrity, and Availability (CIA) in alignment and satisfaction of the applicable requirements.

7 Governance Framework

7.1 Information Security Management System (ISMS)

The ISMS established at CEAT is developed in accordance with ISO/IEC 27001:2022 standards. It provides a systematic approach to managing sensitive company information, ensuring its protection through risk management processes.

7.2 TISAX Compliance

CEAT is committed to compliance of the Trusted Information Security Assessment Exchange (TISAX) Ver 6.03 requirements, which are essential for secure information exchange within the automotive industry. This conformity ensures that the processes followed at CEAT, meet international standards for information security.

8 Policy Framework

CISO and the Information Security Team shall formulate policies for the information and cyber security of the organization. Roles and responsibilities of all the stakeholders will be defined and allocated according to the organization needs. Segregation of duties will be implemented in the conflicting areas of responsibility. Additionally, Standard Operating Procedures (SOPs) will be formulated for cyber security operations and communicated to the respective stakeholders.

8.1 Protection of Information Assets

All information assets in CEAT (including but not limited to hardware, software, applications and information in electronic and other forms) will be classified and protected to ensure their Confidentiality, Integrity, and Availability (CIA). Inventory of all information assets will be

maintained, with ownership, and updated in case of changes. All Intellectual Property (IP) assets of CEAT will also be protected using IP Protection mechanisms like copyright and patents. Application security will be ensured throughout the life cycle of the application i.e. from design to decommissioning. Periodic vulnerability assessments will be carried out and appropriate actions will be taken to ensure that the vulnerabilities are closed in a reasonable time frame.

8.2 Protection of Personal Data

Personal Identifiable Information (PII) & Sensitive Personal Identifiable Information (SPII) will be collected and processed in accordance with the applicable laws and regulations. CEAT will collect personal data and use it in accordance with the applicable regulations. Users will have complete rights over their personal data subject to legal rules and regulations. Details of protection of personal data will be covered in the topic specific policy.

8.3 Regulatory Compliance

All information and technology assets being used for business operations will follow the relevant laws of the land and the guidelines issued by the regulatory agencies. The cyber security team will maintain contact with relevant authorities to remain apprised of the changes in the legal/regulatory requirements and to ensure the compliance level. While using third-party/supplier products and services, protection of third-party Intellectual Property Rights (IPR) will be ensured in accordance with the prevalent laws and the supplier agreements.

8.4 Threat Intelligence

The cyber security team will maintain contact with relevant authorities and special interest groups/forums to acquire threat intelligence and receive information regarding changes in the external cyber security landscape. The threat intelligence acquired by CEAT, will be used to proactively strengthen the cyber security profile of the organisation.

8.5 Acceptable Usage

All information and technology assets will be used in accordance with the acceptable usage policy defined by the organization. Users of CEAT information systems will respect the rights of other users, protect the confidentiality and integrity of the information & associated physical resources, and adhere to prevalent laws and regulations.

8.6 Cyber Security in Project Management

Cyber security requirements will be incorporated in all new IT projects and applications. All such project plans will be reviewed to ensure that necessary cyber security controls are incorporated in the projects and made part of all contracts and supplier relationships including the right to audit the suppliers' information security setup to verify that the requisite cyber security controls are put in place by the supplier.

8.7 Business Continuity and Disaster Recovery

Business continuity planning will be done for all critical information and technology assets and the plan implemented to ensure continuity of operations in case of any adverse event. Provisions of information security will be built into the business continuity plans. Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) will be developed for CEAT and will be used to ensure that the business continues to operate during cyber security incidents.

8.8 Identity and Access Management (IAM)

The complete lifecycle of the identities created in the information systems will be managed to ensure cyber security of these identities. Access to information and technology assets will be controlled based on the business and cyber security requirements, based on the principal of least privilege. The access rights provisioned for the identities will be managed during the entire identity lifecycle.

8.9 Authentication, Authorization and Accounting (AAA)

Only authorized personnel will be allowed to access organizational information and technology assets. Authentication will be implemented for all kinds of access to these assets. Information security accountability will be ensured for all critical information and technology assets. All access actions performed on critical information and technology assets will be monitored and reviewed periodically.

8.10 Cyber Risk Management and Governance

Regular risk assessments will be conducted to identify potential threats to the information assets. Risk Registers will be prepared by the department / plant heads and the CISO and CEAT cyber team will adopt the appropriate risk mitigation strategy to bring the risk down to acceptable levels.

8.11 Information Security in Supply Chain and Supplier Relationships

Cyber security requirements will be incorporated into the supplier agreements based on the type of supplier relationship. Cyber security risks associated with the supply chain will also be addressed in the technical requirements and supplier agreements. The supplier services will be monitored and reviewed to manage the cyber security practices and service delivery of the supplier.

In addition, physical security of the goods and material will be ensured as part of supply chain security by the entire company.

8.12 Cloud Services Security

While using the cloud services, it will be ensured that the cyber security requirements of the company are incorporated in the Service Level Agreements (SLAs). However, overall responsibility of security of information and assets in the cloud, will remain the responsibility of

CEAT. Data stored in the cloud will be protected through encryption, access controls, and regular backups. Compliance with relevant data protection regulations will be strictly enforced

8.13 Cyber Security Incident Management

Cyber security events/incidents will be managed according to a formalized process to minimize risk to the organizations' assets, processes, and reputation. It will be the responsibility of all employees and partners to report any incident or event that has the potential to negatively impact the cybersecurity posture of CEAT, as per the reporting process defined by the organization. The evidence related to incidents will be collected and preserved as per the prevalent laws and regulations. Knowledge gained from cyber security incidents will be used to strengthen and improve the cyber security controls.

8.14 Cyber Security Audit

Cyber security audits will be carried out as per the central audit calendar. Plants may request additional IT/cyber/vigilance audits if required. The outcome of the audit report will be shared and reviewed by the management and the directions given by the management (ISSC) will be implemented for closure of audit observations.

8.15 Information Asset Management

All information assets viz. data, software, hardware, network components, and services, will be identified and inventoried. Assets will be classified based on their sensitivity and criticality. Procedures for handling information assets will be established, ensuring their secure use, storage, and disposal.

- All the information assets of the organization will be protected from physical and environmental threats. Secure areas will be monitored for unauthorized physical access.
- Non-Official devices especially personal devices (including but not limited to smartphones) will not be permitted inside restricted areas
- All official IT Assets will be tagged with a unique identification number issued by the Central IT team. Any exception would require approval from CEO.
- Usage of USB devices (e.g., pen drives) is strictly prohibited for all employees except management. Exceptions for other employees require approval from the CISO and must be reported in management review meetings. Only approved devices will be used inside the company premises.
- Employees and partners will return the organization's information assets in their possession upon change or completion of their employment or service agreement.
- The disposal of information and technology assets will be done in a secure manner at the end of their life cycle.
- All information residing on the company assets will be considered as the property of CEAT. A separate policy will be prepared to lay down the guidelines for information classification, labelling and secure storage/ transfer.

8.16 Cyber Security in HR Hiring Process

All new employees will be subject to background screening and verification before they are hired. The requirement of non-disclosure of organizations information will be incorporated in employment agreements. These requirements will include the responsibilities which will continue to remain valid after termination or change of employment.

8.17 Cyber Security Training and Awareness

CEAT is committed to continually improving its ISMS and will communicate this policy to all employees and ensure that they are given appropriate training to raise awareness on information security.

8.18 Prototype Security

Prototype security is an important facet of information security for a company like CEAT. Unauthorized access to properties where components or parts classified as requiring protection are manufactured, processed, or stored will be prevented. If subcontractors are involved in prototype design, they will meet the minimum requirements for prototype protection. Security requirements for presentations and events involving components or parts which require protection will be defined and ensured. Similar precautions will also be taken in case of filming or shooting the components or parts which require protection.

8.19 User Monitoring and Privacy

All actions occurring on or over CEAT information assets may be monitored without notice for their security and other business requirements.

8.20 Protection of IPR

To effectively protect IPR, CEAT will implement structured procedures across multiple domains, including legal, technical, operational, and employee training measures. IP protection framework tailored to the automotive Industry and digital information assets will be designed as per the requirements of ISO 27001:2022 and TISAX.

8.21 Disciplinary Process

Violation of the cyber security policies or procedures may lead to disciplinary action as per the HR policies of the CEAT group up to and including, but not limited, termination of employment.

8.22 Information Security and TISAX Controls

Appropriate information security and TISAX controls will be deployed to reduce the impact and/or likelihood of risks as per the risk assessment and treatment plan. The cyber security team will design, implement, and operate these controls in consultations with the interested parties to secure the information and technology assets of the organization.

8.23 Roles and responsibilities

Information security is not only the responsibility of IT and Information security functions. At CEAT, we must understand that it is a collective responsibility of each and every employee and external stakeholders like contractors, suppliers, consultants etc. to ensure confidentiality, integrity and availability of organizational information and information assets. Roles and responsibilities of different functionaries are given at Annexure. These will be performed with due diligence to ensure that the information security objectives are achieved at CEAT.

8.24 Continuous Improvement

Our information security practices are continuously monitored and reviewed. Feedback mechanisms will be put in place to identify areas for improvement. The policy will be regularly reviewed and updated at least once a year or earlier to address emerging threats, technological advancements, and changes in operational processes.

9 Exceptions and Limitations

Exceptions may be granted in cases where security risks are mitigated by compensating controls, and in cases where security risks are at a low, acceptable level and in compliance with minimum security requirements, not interfering with legitimate business needs.

10 Conclusion

By adhering to the guidelines of TISAX Ver 6.03 and ISO 27001:2022, and effectively utilizing cloud deployments, CEAT will ensure a strong and resilient information security posture. Besides enabling CEAT to protect its information assets, this policy will also help in building and reinforcing the trust of stakeholders in CEAT's commitment to information security.

---------- END OF DOCUMENT ----------