Eicher Motors Limited

Information Security Policy

Eicher Motors Limited (“EML” or “the Company”) has recognized that its business information is a critical asset and its ability to manage, control, and protect this asset will have a significant impact on its reputation. The Information Security Policy (“Policy”) provides an integrated set of protection measures that must be uniformly applied across EML to ensure a secure environment for its business operations. The Policy defines the controls that are required to ensure protection of EML’s information assets, and to allow access, use and disclosure of information in accordance with appropriate standards, laws and regulations.

The Policy applies equally to any individual, entity, or process that interacts with EML Information Resource.

It is expected that all concerned would:

- Serve to protect the confidentiality, integrity, and availability of the information resources maintained within the Company using administrative, physical and technical controls;
- Design and implement appropriate security controls to prevent unauthorized physical access, damage and modification to EML’s information processing facilities and to protect information assets of EML;
- Ensure data protection and privacy controls as per the applicable law, including GDPR requirements, including but not limited to data collection, usage, storage, protection and management of cookies;
- Ensure that all information systems and services of EML undergo security risk analysis using a formalized process, to ensure that appropriate security controls are identified and incorporated in them;
- Implement suitable network controls across application, services and infrastructure layers of user, control and management planes of the network;
- Implement controls required for timely detection, reporting and resolution of security incidents and weaknesses;
- Ensure appropriate security controls (such as technical controls, contractual or agreement requirements) during exchange of business information with stakeholders as well as with employees during human resources processes;
- Implement changes that could impact confidentiality, integrity or availability of information processed by or stored in the information systems and processing facilities as per approved change management process;
- Impart regular information security training to all relevant individuals, including guidelines on breach of the information security policy and procedures as well as subsequent disciplinary action that would be taken.

Additionally, all concerned are expected to abide by the *Acceptable Usage Policy* and the *Information Technology Disaster Recovery Plan Document* in conjunction with the Information Security Policy.