INFORMATION SECURITY POLICY SUMMARY

Purpose and Scope:

This document is a summary of Litens' Information Security Policy which, forms the foundation for establishing an Information Security Management System (ISMS), supports the Litens Automotive Group strategy and addresses the evolving requirements for information handling and processing for its employees, vendors, contractors, regulators, and other stakeholders. This policy includes organizational structure, processes, rules, regulations, roles, responsibilities, and expectations necessary to ensure the effective planning, implementation, and review of information security measures.

The Information Security Policy formulates the goals and principles of information security and specifies the purposes for which information security is to be ensured and how it is to be achieved. This policy and all regulations on information security must be considered in contractual relationships with third parties.

Significance of Information Security:

Modern work increasingly requires the use of up-to-date information technologies to perform tasks efficiently and effectively. Information security is therefore an indispensable foundation. Tasks, processes, and the organizational structure are subject to constant change and continuous adaptation to technical possibilities. An appropriate level of information security is created by weighing up the values to be protected, the legal requirements and the associated risks. When dealing with information of all kinds, care must be taken to ensure that the respective need for protection is considered accordingly. Information security has the fundamental objective of protecting information of all types and origins. Ensuring an appropriate level of information security is not only an obligation to meet legal or regulatory requirements, but also a mark of quality for the customer-oriented maintenance of the services offered. Information security is therefore a significant corporate priority.

Relation of information security to the goals and functions:

It is necessary to take an integrated view of the interaction of information, IT (Information Technology) processes, tasks, and products, as well as the information technology infrastructure and communication channels. Information security encompasses the summary of all organizational, personnel, physical and technical measures to achieve these goals. Senior management on a global and regional basis is responsible for implementation and maintenance of the ISMS and Information Security policies. All information collected, processed, and retained by Litens Automotive or by our contractors will be managed to meet required confidentiality, privacy, integrity, and availability expectations, in accordance with the law and our obligation to comply to agreed-upon standards.

Information Security Policy Statement and Objectives:

Litens Automotive will ensure security, confidentiality, integrity, and availability of information in accordance with our scope of operations and certification as specifically stated below:

1. **To Preserve Confidentiality** - We shall exercise due diligence to ensure that information is protected against unauthorized disclosure and is made accessible only to authorized persons in a permissible manner therefore preventing both deliberate and inadvertent unauthorized access to Litens information assets and systems.
2. **To Maintain Integrity** - We shall exercise due diligence to protect information assets from deliberate or accidental, partial, or complete, destruction or unauthorized access, use, modification and to ensure the accuracy, authenticity, and completeness of the information is preserved.
3. **To Ensure Availability** - We shall exercise due diligence to ensure that information and associated assets are accessible to authorized users when required, and therefore secured and protected from risks that threaten the continued availability of reliable assets, systems, and information.

In specific terms, our information security objectives and goals are derived from these core principles within our specific context:

1. Provide efficient and effective IT support for the performance of tasks.
2. Ensure the uninterrupted operation of IT systems.
3. Maintain the availability of IT systems to ensure the uninterrupted functioning of core processes.
4. Minimization of potential damage of Information assets resulting from a failure or disruption of processes
5. Safeguarding investments in technology, information, workflows, and knowledge
6. Securing IT systems against manipulation, unauthorized access, and loss
7. Reducing the impact of an information security incident when it occurs and prevent future occurrences.

To accomplish these goals, all necessary measures are implemented and continuously reviewed for completeness, consistency, appropriateness, and effectiveness.

Implementation of the Information Security Policy:

Personnel and financial resources are provided to the extent that are required to ensure an appropriate level of information security in the processing of data that is to be protected. The security measures to be applied must be economically reasonable in respect to the damage that can be caused by security incidents. This also includes damage which is difficult to quantify in monetary terms, such as damage to reputation or personal injury. If several alternative measures are available to achieve a security objective, the one which is the most economical in terms of investment and operating costs should be selected.

Commitment to Continuous Improvement:

Information security is not a static concept, it is dependent on many internal and external conditions and influences, for example new threats, new laws, or the development of new technical solutions. It is necessary to ensure that approaches to information security management are aligned with these changes. As a response to this, it is important to ensure that the security strategy is continually updated. Accordingly, the aim is to continuously improve the processes relating to information security.

Commitment of senior management:

Litens senior management explicitly acknowledges the listed aspects of information security and approves them as part of the fundamental strategy and assures their implementation. Management carries the responsibility for information security and ensures that the implementation and continuous improvement of the ISMS is supported by appropriate human and financial resources to fulfil all objectives mentioned in this policy.

Paul Robinson
President and Chief Executive Officer

Date: Oct 12th, 2023

Tyson Bytzek
Executive Vice President, Chief Operating Officer

Date: Oct 12th, 2023