FORGES TARDIEU GROUP

INFORMATION SECURITY POLICY

1. The Board of Directors and management of FORGES TARDIEU GROUP, comprising of FORGES TARDIEU Limited and its subsidiaries, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image.

2. In view of its information and information security requirements, the Management of FORGES TARDIEU GROUP shall devise an Information Security Management System ('ISMS'). The Board of Directors of FORGES TARDIEU GROUP has also approved this Information Security Policy for preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout FORGES TARDIEU GROUP. This Information Security Policy supplements FORGES TARDIEU GROUP's General Data Protection Policy and shall be read in conjunction and subject to the said General Data Protection Policy.

3. FORGES TARDIEU GROUP's information and information security requirements will continue to be aligned with FORGES TARDIEU GROUP's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, for e-commerce and for reducing information-related risks to acceptable levels.

4. FORGES TARDIEU GROUP's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS.

5. The ISMS shall provide, inter alia, for a risk assessment and a risk treatment plan which will identify how information-related risks are controlled. FORGES TARDIEU GROUP's Head of IT Department, in collaboration with FORGES TARDIEU GROUP's Data Protection Officer, is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

6. In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy.

7. FORGES TARDIEU GROUP aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

8. All employees/staff of FORGES TARDIEU GROUP are expected to comply with this policy and with the ISMS which supports this policy. All employees/staff, and certain external parties, if need be, will receive appropriate training in this respect. The consequences of breaching this Information Security Policy and/or the ISMS will give rise to disciplinary measures against FORGES TARDIEU GROUP's employees.

9. Furthermore, FORGES TARDIEU GROUP has entered and shall enter into Non-Disclosure Agreements and/or Privacy Agreements with third parties in order to ensure the latter's compliance with this Information Security Policy and the ISMS.

10. The ISMS will be subject to continuous, systematic review and improvement.

11. This Information Security Policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

12. This Information Security Policy is implemented and the ISMS shall be implemented by FORGES TARDIEU GROUP for **preserving** the **confidentiality**, **integrity** and **availability** of all the **physical assets** and electronic **information assets** throughout FORGES TARDIEU GROUP.

13. The mission statement and commitment of FORGES TARDIEU GROUP as set out in paragraph 12 above is more fully defined as follows:

Preserving

This means that the Management, all full time or part time employees/staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. A security breach is any

incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of FORGES TARDIEU GROUP. All employees/staff will receive information security awareness training and more specialized employees/staff will receive appropriately specialized information security training.

Availability

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and FORGES TARDIEU GROUP must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information.

Confidentiality

This involves ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to FORGES TARDIEU GROUP's information and proprietary knowledge and its systems including its network(s), website, extranet(s), and e-commerce systems.

Integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification, of either physical assets or electronic data. There must be appropriate contingency [including for network(s), e-commerce systems, website, extranet(s)] and data backup plans and security incident reporting. In this respect, FORGES TARDIEU GROUP will scrupulously comply with all relevant data-related legislation in those jurisdictions within which it operates.

Physical assets

The physical assets of FORGES TARDIEU GROUP include, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

Information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, websites, extranets, intranets, PCs, laptops, mobile phones, CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means.

Document Owner and Approval

FORGES TARDIEU GROUP is the owner of this document.

This document may, from time to time, be reviewed in line with any changes in FORGES TARDIEU GROUP's General Data Protection Policy and the law.

This Information Security Policy been duly approved by the Board of Directors of FORGES TARDIEU GROUP on 18 Sept 2019.

By order of the Board of Directors of FORGES TARDIEU GROUP.

Made in good faith on 18 Sept 2019 at 31 Route Nicolay, Port-Louis, Republic of Mauritius.