INFORMATION SECURITY POLICY OF TEAMLINE

Document Control

Reference: ISMS DOC 5.2

Issue No:

Issue Date:04/03/2025

The Board of Directors and management of Agile Factory Limited, located at Room 604, 6/F, Easey Commercial Building Nos. 253-261 Hennessy Road, Wan Chai, Hong Kong, which operates in the IT sector and provides Teamline software for automation of software development processes, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organization in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Agile Factory Limited goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

Agile Factory Limited'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. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. Artem Borodin a s a Head of Risk 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.

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.

All staff of Agile Factory Limited are expected to comply with this policy and with the ISMS that implements this policy. All staff, and certain external parties, will receive appropriate training(s). The consequences of breaching the information security policy are set out in Agile Factory Limited disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

Agile Factory Limited has established a top level management steering group named as Information Security Committee, chaired by Artem Borodin - Chief Product Officer (CPO) / Oleg Krasavin - Chief Information Security Officer (CISO).

Agile Factory Limited takes ISO27001:2013. as its guideline standard for company ISMS. This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving

This means that management, all full time or part time 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 (in line with the policy and procedures identified in Section 16 of the Manual) and to act in accordance with the requirements of the ISMS. All staff will receive information security awareness training and more specialized staff will receive appropriately specialized information security training.

the availability,

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network must be resilient and Agile Factory Limited 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. There should be appropriate business continuity and incident response plans.

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 Agile Factory Limited information and proprietary knowledge and its systems including its network(s), website(s), extranets), and other systems.

and 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), payment system(s), website(s), extranets)] and data backup plans and security incident reporting. Agile Factory Limited must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of Agile Factory Limited including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, a s well as information stored electronically on servers, website(s), extranets), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the systems) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

Of Agile Factory Limited

Agile Factory Limited and such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

The ISMS is the Information Security Management System, of which this policy and other supporting and related documentation is a part, and which has been designed in

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 Agile Factory Limited

Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed.

A current version of this document is available to all members of staff on the corporate intranet and company Slack. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the Board of Directors on 04/03/2025 and is issued on a version controlled basis under the signature of the Chief Executive Officer

Signature (CEO): Signed by: Vladislav Zhigulin 6CAD161A882344F... Date: 04/03/2025

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Oleg Krasavin	04/03/2025