Adaptavist Group Security policy

1 Purpose

The Adaptavist Group's (TAG) CEO and its Management Team recognizes that Information Security is of great importance to our business. In light of this, it is the goal of TAG Management to protect our information assets and operations.

The preservation of information in the scope of these principles (CIA):

- **Confidentiality** - Protecting information from unauthorized disclosure
- **Integrity** - Safeguard the accuracy and completeness of information
- **Availability** - Ensuring information is accessible and usable upon demand by authorized users

It is therefore the purpose of this policy to manage risks and implement security controls against threats to our information systems and our customers, whether internal or external, deliberate or accidental. This is accomplished by preventing and minimizing the impact and/or occurrence of information security incidents. Information security requirements will be aligned with TAG policies and goals with focus on core operations and processes. Continuous improvements to TAG business operations and processes will be implemented in the context of security.

TAG CEO has approved this policy and fully supports its operation.

It has been recognized that TAG may acquire subsidiaries that have a stand-alone certification. Those certifications may be considered by the ISMF in a program of integration and harmonisation.

2 Scope

This policy applies to all employees of TAG and its subsidiaries in all operational locations. In addition, 3rd party suppliers and sub contractors will be managed in accordance with this policy.

3 Policy

- All operations will comply with relevant legislation and standards. In particular TAG focuses on compliance with ISO/IEC 27001:2022 and SOC 2 2017 of AICPA Trust Services Criteria (TSC).
- Appropriate access control is implemented for virtual and physical access and is reviewed on a regular basis based on risk.
- An asset inventory is maintained and classified with view to importance of confidentiality, integrity and availability (CIA).
- Risk is managed within acceptable limits with regular risk assessments and controls by operating Information Security Management System (ISMS) pursuant to ISO/IEC 27001:2022.
- Security objectives are defined and implemented to support TAG business objectives.
- Business continuity plans are documented, maintained and tested on regular basis.
- Compliance to all relevant regulations, legislation, procedures, and contractual requirements is met.
- Security awareness training and education is provided to employees.

4 Responsibility

The following responsibilities are defined for this policy:

- TAG CEO approves and supports the policy.
- Compliance and Security Manager in co-operation with executive management team is responsible for establishing, reviewing, and monitoring compliance to the policy.
- All employees are required to read, understand, and comply with this policy and also to report incidents, external or internal, suspected or actual, accidental or deliberate, to Compliance and Security Manager.

Adaptavist Group Ltd | Registered in England #06878779 | VAT GB: 242 0200 75
Adaptavist Approved Template | Created February 2023

- All managers are responsible for ensuring that contractors and 3rd party vendors with access to TAG information systems are introduced and comply to this policy.

5 Nonconformity

Nonconformity to this policy is to be reported to the Compliance and Security Manager, a member of the Security Forum or to Adaptavist Internal Support.

6 Review

The policy will be reviewed annually or more frequently if required to ensure conformity with the organizational goals.

7 Approval

Approver	CEO
Approved date	24 April 2026
Signed	CEO