Manantial LTD
17 Mary Shunn Way,
Wantage, Oxfordshire, OX128GN,
United Kingdom

General Information Security Policy

Owner: udara wijeratna

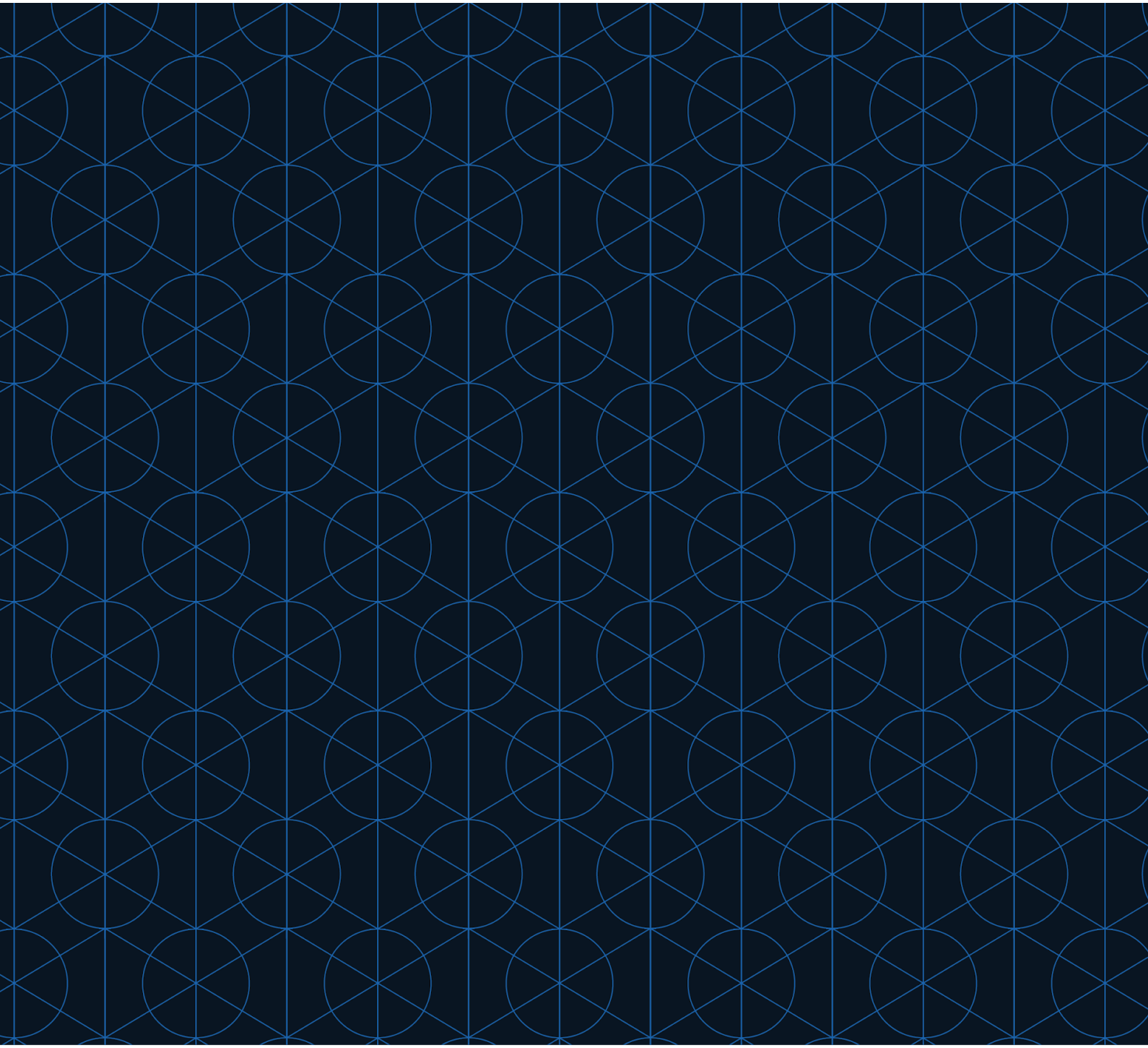
Approver: Dilanka Kalutota

Classification: Company Internal

Document ID: POL-04

Version: 1.0

Effective Date: 18/12/2022



Manantial LTD
17 Mary Shunn Way,
Wantage, Oxfordshire, OX128GN,
United Kingdom

Table of contents

Manantial LTD
17 Mary Shunn Way,
Wantage, Oxfordshire, OX128GN,
United Kingdom

ISO 27001 Coverage

C.5.1; C.5.2; C.7.2; C.7.3; A.5.1.1; A.5.1.2; A.6.2.1; A.6.2.2; A.7.1.2; A.7.2.1; A.7.2.3; A.8.1.3; A.8.2.3; A.9.2.4; A.9.3.1; A.11.2.6; A.11.2.8; A.11.2.9; A.12.5.1; A.12.6.2; A.16.1.3

1 Version History

Version #	Date	Author	Change detail
v1.0	18 Dec 2022	Ruween Iddagoda	

2 Document Goal

This document is for internal use only. Distribution of this document outside of Manantial LTD requires approval from Information Security Management Leader at udara@velaris.io

The purpose of this document is to outline the acceptable and unacceptable use of information and IT assets provided or managed by Manantial LTD. The acceptable use rules are in place to protect Manantial LTD, it's employees, partners and customers from various information security risks like virus attacks, compromise of IT assets & services, unauthorized disclosure or theft of personal and business sensitive information potentially leading to legal & regulatory non-compliance, reputational damage, operational disruption and/or financial loss. These best practices also provide valuable guidance to the users in protecting their personal digital identity online, which remains users' responsibility.

Manantial LTD has designated a senior level information security official as Chief Information Security Officer's (hereafter referred to as Information Security Management Leader) responsible for direction and oversight of the security program. Information Security Management Leader's intentions for publishing an Information Security Policy are not to impose restrictions that are contrary to Manantial LTD's established culture of openness, trust and integrity. Information Security Management Leader is committed to protecting Manantial LTD's employees and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including, but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and Cloud computing, that are provided by Manantial LTD are the property of Manantial LTD. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Manantial LTD employee and affiliates who deal with information and/or IT assets. It is the responsibility of every Employee, consultant, contractor and other third-party who use Manantial LTD information and IT assets to know the requirements stated in this policy, and to conduct their activities accordingly.

Manantial LTD management is committed to continuously invest and improve ISMS controls and efforts with appropriate human, technical and procedural support, as well as ensure that all required elements are met in order to establish, implement, maintain and continually improve the ISMS.

2.1 Scope of the document

This document applies to all Employees, consultants, contractors and other third-parties who use Manantial LTD information and IT assets (hereafter referred to as IT Users).

2.2 Audience and roles

- Managing directors are responsible for approving the Policy.
- Information Security Management Leader is responsible for creating, reviewing, and updating the Policy.
- Implementation responsibilities are defined in each segment respectively.
- All employees are responsible for reading, acknowledging and practicing requirements in this Policy segment.

2.3 System Owners

- System owners are responsible for a specific system used to support Manantial LTD business goals, by ensuring the system is functioning properly and is used for intended business purpose, access to the system is strictly regulated, reviewed and access granted based on least-privilege and need-to-know principles.
- System owner role is assigned by Information Security Management Leader to an individual most familiar with the system they have been assigned for and with relevant experience and training to manage the system in question.
- System Owners are responsible to assist Information Security Management Leader in the quarterly User Access review process.

2.4 Table of definitions, terms and abbreviations

Term	Description
Business Sensitive Information	Manantial LTD information which is classified as "Internal" or "Confidential", per classification matrix in POL-14 Data Management, will be considered as business sensitive information. It includes anything that poses a risk to the company if discovered by a competitor or general public. Such information includes trade secrets, acquisition plans, financial data and supplier and customer information, among other possibilities. For the purpose of this document, Sensitive Personally Identifiable Information (PII) and Protected Health Information (PHI) are also included in this broad definition of Business Sensitive Information.
IT User	The term "IT User" refers to any person authorized to access the IT tools, resources of Manantial LTD (and those of its entities) and to make use of them: Employees(staff), contractors, temporary personnel, service provider personnel, etc.
IT Asset	The term "IT Asset" refers to any information, system or hardware that is used in the course of business activities. It can be a device such as a notebook, smartphone, network equipment, conferencing equipment and an information system such as an information or communication technology used by Manantial LTD or authorized third party to provide a service i.e. AWS cloud hosting platform, third party applications, internally developed systems. This refers to company-owned assets, acquired third party assets and personal assets that are subject to BYOD policy in this document.

3 General Information Security Policy

Protect Manantial LTD's informational and IT assets (including but not limited to all computers, mobile devices, networking equipment, software and sensitive data) against all internal, external, deliberate or accidental threats and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems;

Ensure information will be protected against any unauthorized access. Users shall only have access to resources that they have been specifically authorized to access. The allocation of privileges shall be strictly controlled and reviewed regularly.

Protect CONFIDENTIALITY of information. When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties;

Ensure INTEGRITY of information. Integrity of information refers to protecting information from being modified by unauthorized parties;

Maintain AVAILABILITY of information for business processes. Availability of information refers to ensuring that authorized parties can access the information when needed.

Comply with and, wherever possible, exceed, national legislative and regulatory requirements, standards and best practices;

Develop, **Maintain** and **Test** business continuity plans to ensure we stay on course despite all obstacles that we may come across. It is about "keeping calm and carrying on!";

Raise awareness of information security by making information security training available for all Employees. Security awareness and targeted training shall be conducted consistently, security responsibilities reflected in job descriptions, and compliance with security requirements shall be expected and accepted as a part of our culture;

Ensure that no action will be taken against any employee who discloses an information security concern through reporting or in direct contact with Information Security Management Leader, unless such disclosure indicates, beyond any reasonable doubt, an illegal act, gross negligence, or a repetitive deliberate or willful disregard for regulations or procedures;

Report all actual or suspected information security breaches to "IRT" email group by using the form linked in https://velaris.atlassian.net/servicedesk/customer/portals

3.1 Enforcement, Exceptions and Complaints

Non-conformance to policy and standard statements in this Policy could result in disciplinary action including, but not limited to, informal or formal warnings, up to termination of contract. Any exceptions to what is governed will require written authorization by email from Information Security Management Leader. Exceptions granted will be issued a policy waiver for a defined period of time. All target users of this Policy can submit complaints to its contents to Information Security Management Leader at any point. All complaints will be filed and processed accordingly where Information Security Management Leader will respond within 14 days of initial submission. Requests for exceptions to this policy as well as complaint submissions will be addressed to Information Security Management Leader at udara@velaris.io .