ThoughtRiver™
Legal Contract AI

Information Security Policy

Version 2.0

30/10/2024

Document control

Summary

Title	ThoughtRiver Information Security Policy
Version	2.0
Date	30/10/2024

Change history

Version	Date	Issued by	Reason for issue
1.0	21/01/2022	ThoughtRiver	Final
2.0	30/10/2024	Kirsty Alderton	Updated for new controls and branding

Introduction

ThoughtRiver recognises that maintaining the confidentiality, integrity and availability of information and information systems is a critical factor to its continued success. The company is establishing and committed to maintaining, reviewing and continually improving an information security management system (ISMS) that aligns to the requirements of the international standard, ISO/IEC 27001. The standard enables the organisation to achieve our stated objective of effectively managing information security risk across the organisation.

Purpose

The purpose of this policy, and the ISMS it relates to, is to:

- Provide principles for defining and regulating the management of information systems and other information assets;
- Ensure relevant and accurate information is available to staff members and customers;
- Ensure ThoughtRiver remain compliant with relevant legal, statutory, regulatory and contractual obligations;
- Provide the framework that assures a secure and safe working environment for authorised staff members, contractors and interns;
- Protect its assets from all relevant threats, internal or external, deliberate or accidental;
- Ensure that all staff members, contractors, interns and any other third party understand their responsibility in protecting confidentiality, integrity and availability of the organization;
- Ensure appropriate information security objectives are defined and, where practicable, measured;
- Ensure appropriate business continuity arrangements are in place to counteract interruptions to business activities and that these arrangements consider information security;
- Ensure that appropriate information security education, awareness and training is available to staff and relevant others working on behalf of the company;
- Ensure that breaches of information security, actual or suspected, are reported and investigated without delay through appropriate processes;
- Ensure that appropriate access control is maintained, and information is protected against unauthorised access;
- Ensure the ISMS is subject to continual improvement.

Information security principles

All information shall be adequately classified following relevant regulatory and/or contractual obligations.

Information shall be protected from unauthorised access and processing to a degree appropriate to its value and classification.

All authorised users are held responsible for information management and handling.

Actual or suspected information security events and incidents shall be reported and responded to promptly as per ThoughtRiver's policy.

Information security objectives

ThoughtRiver's Information Security Policy objectives are designed to ensure that:

1. ThoughtRiver information is protected from unauthorised access
2. Confidentiality of the information is assured
3. Integrity of the information is maintained
4. Availability of the information is ensured
5. A framework is developed for identifying and mitigating risks to information assets by implementing controls and monitoring effectiveness
6. Regulatory, contractual and legislative requirements are met
7. Business continuity plans are produced, maintained and tested
8. Adequate resources are deployed to implement, maintain and improve an effective information security program
9. Information security training will be available to all employees and relevant third parties
10. All employees, who have access to confidential and/or client information are informed of their responsibilities and obligations with respect to security

Measurement of ISMS Objectives

ISMS objectives are periodically reviewed and measured as listed below and also form part of the agenda in every Information Security Forum meeting. More details are set out in ThoughtRiver's ISMS Objectives and KPI Monitoring document.

KPI Number & Title	ISMS Objective (see list above)
1 - Service uptime	**4 -** Availability of the information is ensured; **6 -** Regulatory, contractual and legislative requirements are met;
2 - Continual Improvement	**9 -** Adequate resources are deployed to implement, maintain and improve an effective information security program;
3 - Awareness Training (new staff)	**8 -** Information security training will be available to all employees and relevant third parties; **10 -** All employees, who have access to confidential and/or clients' information are informed of their responsibilities and obligations with respect to security.
4 - Number of security incidents compared to previous period	**6 -** Regulatory, contractual and legislative requirements are met;
5 - Number of restore tests carried out in target time	**3 -** Integrity of the information is maintained; **4 -** Availability of the information is ensured;
6 - Awareness Training	**8 -** Information security training will be available to all employees and relevant third parties; **10 -** All employees, who have access to confidential and/or clients' information are informed of their responsibilities and obligations with respect to security.
7 - Non-conformances	**1 -** To ensure ThoughtRiver Information is protected from unauthorized access;
8 - Non-conformances	**7 -** Adequate resources are deployed to implement, maintain and improve an effective information security program; and
9 - Annual testing of business continuity to be completed	**4 -** Availability of the information is ensured; **7 -** Business continuity plans are produced, maintained and tested;

KPI Number & Title	ISMS Objective (see list above)
10 - Internal Audit	**1 -** To ensure ThoughtRiver Information is protected from unauthorized access; **2** - Confidentiality of the information is assured; **3** - Integrity of the information is maintained; **4** - Availability of the information is ensured; **5** - A framework is developed for identifying and mitigating risks to information assets by implementing controls and monitoring effectiveness **6** - Regulatory, contractual and legislative requirements are met;
11 - % of risks reviewed within 365 days of last review	**5 -** A framework is developed for identifying and mitigating risks to information assets by implementing controls and monitoring effectiveness;

Compliance, awareness and disciplinary procedure

All staff members, contractors, interns or others working under the control of the company shall:

Be aware of this policy, other information security-related policies and procedures described in the ISMS and shall acknowledge understanding of their responsibilities and contribution to the ISMS.

Comply with its information security policies and procedures and will be made aware that breaches of information security-related policies or procedures may result in disciplinary or other action.

Be provided with information security awareness, education and training relevant and appropriate to their role.

Authorisation

Accepted and authorised

e-signed

Jennifer Hill

CEO

ThoughtRiver Limited

Effective date: 30th October 2024