Risk Management Policy

Classification: Public

Risk Management Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to identifying, assessing, and managing information security risks to protect the confidentiality, integrity, and availability of Company information assets. This includes implementing processes that support proactive risk treatment and continuous improvement across all business operations.

This Policy applies to all individuals involved in activities that impact information security, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All personnel are expected to act responsibly and follow established procedures to ensure risks are managed in line with organisational requirements.

New Era will implement and maintain controls to ensure that:

- Information security risks are identified, assessed, and documented using a structured methodology.
- Risk treatment plans are developed and implemented to reduce risks to acceptable levels.
- Risk assessments are reviewed regularly and updated to reflect changes in business, technology, and regulatory requirements.
- Roles and responsibilities for risk management are clearly defined and communicated.
- Risk management activities are monitored and reported to support compliance and decision-making.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“data”	are items of information.
“information”	Information is processed, organized, and structured data. It provides context for data and enables decision-making processes. Information can be collected, used, stored, reported, or presented in any format, on any medium.
“information resource”	means information and related resources, such as personnel, equipment, funds, and information technology.
“risk”	per ISO 27005 risk is defined as “potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization”.
“staff”, “users”, “personnel"	means those who are employed by New Era Technology on a fulltime, part-time, or temporary basis; those who access and / or utilize New Era Technology’s information resources, including, but not limited to employees, contractors, interns, third and external parties.
“we”, “our”, “New Era”, or “New Era Technology”	refers to New Era Technology and its subsidiaries.

2. Scope

The New Era Technology Risk Management Policy applies to all New Era Technology individuals that are responsible for management, implementation, or treatment of risk activity.

This Policy also applies to all New Era Technology's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to New Era’s electronic systems, information, software, and/or hardware.

The terms set out in this Policy work in conjunction with, and do not replace, amend, or supplement any terms or conditions of employment stated in any collective bargaining agreements and/or employment contracts.

This Policy is not intended to restrict communications or actions protected or required by regional/local laws and regulations.

Relationship with Local/Regional Policies

This Policy is New Era’s corporate policy. New Era Technology business units and/or subsidiaries may complement this with a local/regional policy however, this Policy shall always be the minimum standard; a local/regional policy may augment, or increase the standards, but shall not detract from the New Era Technology risk management standards.

If any additional risk management policies are developed, Director of Governance, Risk and Compliance (GRC) must review and approve prior to release and publication.

3. Roles and Responsibilities

The Director of Governance, Risk and Compliance (GRC), Chief Information Officer (CIO) and the Chief Technology Officer (CTO) are responsible for the New Era Technology Security framework and its associated policies.

This Policy is reviewed annually by members of GRC. Any changes to this Policy will be approved by New Era Technology's CIO, CTO and Director of Governance, Risk, and Compliance prior to its release.

Suggestions for change to this Policy should be reported to GRC@neweratech.com.

All employees, contractors and third parties who access New Era Technology's information must abide by this and associated policies.

Technology owners are responsible for technical standards applicable to their operating environments and domains.

Line managers have day–to–day responsibility for this policy, and employees should refer any questions about this policy to them in the first instance.

In line with their applicable solutions groups, New Era's business units shall develop, disseminate, and maintain formal, documented processes and/or procedures to facilitate the implementation of this Policy and, where applicable, any local/regional access management policies. The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

1. Formal Risk Assessments
    a. Comprehensive risk assessments will be performed when new assets or technologies are introduced into New Era's environment.
    b. Re-assessments of existing assets will be conducted when significant changes occur in the operating environment, technology landscape, or regulatory requirements.
    c. An annual review of the overall risk management process and critical risks will be carried out to ensure continued effectiveness and alignment with business objectives.
2. Risk Registers
    a. Risk Registers must be maintained to ensure comprehensive risk management by regularly assessing and updating registers for all critical business risks, including but not limited to operational, compliance, financial, health & safety, information security, sustainability, and project-related risks.
3. Structured Risk Management Process
    a. Information security risk management procedures must be documented and include, at a minimum:
        i. Risk Assessment- Identify and analyse risks to information assets.
        ii. Risk Treatment - Define and implement measures to reduce risks to acceptable levels.
        iii. Risk Communication - Ensure relevant stakeholders are informed of risks and treatment plans.
        iv. Risk Monitoring and Review - Continuously monitor and update risk status and controls.
4. Risk Evaluation Criteria
    a. Criteria for evaluating information security risks must consider:
    b. Strategic value of the business processes and information.
    c. Criticality of information assets.
    d. Legal, regulatory and contractual obligations.
    e. Operational importance of confidentiality, integrity and availability.
5. Classification, Ownership and Independent Evaluation
    a. All identified risks must be classified and prioritized based on their significance to the organization and potential impact.
    b. Each risk must have an assigned risk owner responsible for monitoring and treatment.
    c. Periodically, New Era Technology may engage a third-party to conduct risk assessments or validate the effectiveness of the risk management process.
6. Reporting and Continuous Improvement
    a. Risk register updates and assessment results must be documented and reported to senior management for oversight.
    b. Risk management processes will be reviewed and updated regularly to reflect changes in threats, technology, and business priorities.

5. Compliance, Monitoring and Enforcement

This Policy is intended for all New Era businesses, in all countries.

New Era Technology seeks to proactively prevent and mitigate instances of non–compliance with this Policy.

Compliance is measured through various methods, including but not limited to risk assessments, business tool reports, internal and external audits, etc.

Any breaches or concerns, including ethical concerns or potential breaches in our commitment to information and data protection standards, should be reported as soon as possible through our Whistleblowing Policy.

Any need for improvements will be applied as soon as possible. Employees are encouraged to offer their feedback on this Policy if they have any suggestions for how it may be improved. Feedback of this nature should be addressed to GRC@neweratech.com.

Any exception to this Policy must be approved by the Any exception to this Policy must be approved by the CTO, CIO, and / or Director of Governance, Risk, and Compliance in advance.

Personnel found to have intentionally violated this Policy may be subject to disciplinary action, up to and including termination of employment and other penalties as set forth herein. New Era Technology reserves the right to pursue any, and all, legal and civil action in connection with any such violation.

Any vendor, consultant, or contractor found to have violated this Policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

6. Acknowledgement

Those in receipt of this Policy acknowledge its receipt and understanding of its contents; and that New Era Technology expressly reserves the right to change, modify, or delete its provisions without notice.

Document Information

Reference	Security Framework
Title	Risk Management Policy
Purpose	The purpose of the New Era Technology Risk Management Policy is to establish the requirements for the assessment and treatment of information security-related risks facing the business.
Owner	Governance, Risk & Compliance (GRC)
Document Approvers	Chief Information Officer (CIO) Chief Technology Officer (CTO) Director of Governance, Risk & Compliance (GRC)
Intended Audience	New Era Technology permanent, temporary, and contracted staff.
Review Plan	Annually
Document Classification	Public

Document History

VERSION CONTROL			
Revision	**Date**	**Record of Changes**	**Approved /Released By**
V1.0	Nov 2022	Approved release	CTO, Dir GRC
V2.0	Sep 2023	Annual review; classification & approvers update	CTO, Dir GRC
V3.0	Sep 2024	Annual review, updates to sections 2-6	Dir GRC
V3.0	Oct 2024	Approved release	CTO, Dir GRC
V4.0	Jan 2026	Annual review, updates, approval	CTO, CIO, Dir GRC

References

Standard / Framework / Other	Title	Description
New Era GRC Policy	Security Policy	Policy to (a) protect New Era Technology and its customers' data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.
New Era GRC Policy	Acceptable Use Policy	Policy to establish acceptable practices regarding the use of New Era Technology Information Resources to protect the confidentiality, integrity, and availability of information created, collected, and maintained. Inappropriate use exposes New Era to risks, including virus attacks, loss of confidential data, compromise of network systems and services, and legal issues.
ISO/IEC 27005:2018	Information technology — Security techniques — Information security risk management	Guidelines for information security risk management.
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements	Requirements for establishing, implementing, maintaining, and continually improving an ISMS.
ISO/IEC 27002:2022	Code of Practice for Information Security Controls	Guidance on implementing information security controls.
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations	Catalog of security and privacy controls for information systems and organizations.