Vendor Management Supplier Security Policy

Classification: Public

Vendor Management Supplier Security Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to ensuring that all vendor and supplier relationships are managed in a manner that protects the Company, its business partners, and stakeholders from undue risk. This includes implementing appropriate controls to safeguard information security, compliance, and operational integrity throughout the supplier lifecycle.

This Policy applies to all individuals involved in vendor or supplier engagement, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All users are expected to act responsibly and in accordance with established procedures to ensure that supplier relationships meet the Company's security and risk management requirements.

New Era will implement and maintain controls to ensure that:

- Vendors and suppliers are assessed for security and compliance risks prior to engagement.
- Contracts include clear security, confidentiality, and compliance obligations.
- Supplier performance and risk posture are monitored and reviewed regularly.
- Access provided to vendors is limited, authorised, and promptly revoked when no longer required.
- Issues or incidents involving suppliers are reported and managed in line with Company procedures.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“critical vendor”	A critical vendor provides goods or services that cannot be easily and efficiently replaced; a vendor with a specialized skillset, mandatory compliance certification or proprietary product whose discontinuation of service would have a significant negative impact on a New Era Technology’s operation.
“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.
“vendor”, “supplier”	used interchangeably. A vendor, or a supplier, is a supply chain management term that means a company who provides goods or services of experience to another entity. Vendors may sell B2B (business-to-business, i.e., to other companies), B2C (business to consumers), or B2G (business to government). Some vendors manufacture inventoriable items and then sell those items to customers, while other vendors offer services or experiences. The term generally applies only to the immediate seller, or the organization that is paid for the goods, rather than to the original manufacturer or the organization performing the service if it is different from the immediate supplier[1].
“we”, “our”, “New Era”, or “New Era Technology”	refers to New Era Technology and its subsidiaries.

2. Scope

In line with the New Era Cloud Computing Policy, the New Era Technology Vendor Management / Supplier Security Policy applies to any individuals that interact, set up or manage any New Era Technology vendors and/or suppliers, from now on referred to as “vendors”.

This Policy 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 vendor management or supplier security 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 vendor management or supplier security standards.

If any additional vendor management or supplier security 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

Assessments

1. Vendors granted access to New Era Technology Information Resources must sign the New Era Technology Vendor Non-Disclosure Agreement/Business Associate Agreement.
2. Vendors must be evaluated prior to the start of any service and thereafter on an annual basis.
3. High risk findings must be remediated and verified.
4. Vendor risk assessment must be performed for vendors with physical or logical access to general business and/or confidential information or that is considered critical.
5. Risk assessments must be performed on all requested cloud providers before approval.
6. Vendors with PCI DSS compliance requirements must have their status reviewed annually.
7. Vendors must acknowledge compliance with the New Era Supplier Code of Conduct as part of onboarding and ongoing reviews.

Management

1. Vendor agreements and contracts must specify:
   a. The information the vendor may access.,
   b. How information is to be protected and transferred.
   c. Methods for return or secure disposal of information at the end of the contract.
   d. Minimum security requirements and Incident response obligations.
   e. Right for New Era Technology to audit vendor compliance.
2. Vendors must ensure appropriate security practices throughout their supply chain and notify New Era Technology of any subcontracting.
3. Vendors may only use New Era Technology Information Resources only for agreed business purposes.
4. Vendor performance must be reviewed annually against contractual and SLA requirements.
5. Vendors must report all security incidents promptly and comply with escalation procedures.
6. Vendors must return or securely destroy sensitive information upon employee departure or contract termination.
7. Upon termination of contract or at the request of New Era Technology, the vendor must surrender all New Era Technology badges, access cards, equipment and supplies immediately.
   a. Equipment and/or supplies to be retained by the vendor must be documented by authorized New Era Technology IT management.
8. Vendors must comply with the **Supplier Code of Conduct** (See Appendix A)

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.

Appendix A: Suppliers & Subcontractors Code of Conduct

New Era Technology and its subsidiaries ("New Era" or "the Company") are committed to conducting business with integrity, ethical behavior, and compliance with all applicable laws and regulations. We expect the same high standards from our suppliers and subcontractors.

This Supplier Code of Conduct outlines the minimum requirements that all suppliers and subcontractors must adhere to, in alignment with New Era's compliance principles and the United Nations Global Compact Initiative[1].

Human Rights

Suppliers and subcontractors must:

- Support and respect internationally recognized human rights.
- Ensure they are not complicit in any form of human rights abuse.

Labor Standards

Suppliers and subcontractors must:

- Uphold freedom of association and the right to collective bargaining.
- Prohibit all forms of forced, compulsory, and child labor.
- Eliminate discrimination in employment and occupation.
- Provide a safe and healthy working environment.
- Treat employees with respect, fairness, and non-discrimination.
- Employ and remunerate workers based on fair and legally compliant contracts.
- Maintain international minimum labor standards.

Environmental Responsibility

Suppliers and subcontractors must:

- Comply with all applicable environmental laws and regulations.
- Minimize environmental impact and pollution.
- Promote sustainable practices and initiatives that enhance environmental responsibility.

Anti-Corruption & Anti-Bribery

Suppliers and subcontractors must:

- Actively work against corruption in all forms, including extortion and bribery.

Compliance with New Era Policies

Suppliers and subcontractors are expected to familiarize themselves with and comply with New Era's policies, available at: www.neweratech.com.

Reporting Concerns

Any concerns or suspected violations of this Code should be reported to: privacy@neweratech.com.

Consequences of Non-Compliance

If New Era determines that a supplier or subcontractor has violated this Code of Conduct, we reserve the right to terminate the business relationship immediately and pursue legal remedies, including claims for damages.

Suppliers and subcontractors may be required to complete an annual questionnaire to provide details on their policies, certifications, and compliance practices.

Conflict Resolution

In case of any conflict between this Code of Conduct, contractual terms, and applicable laws, the following priority applies:

1. Applicable legal and regulatory requirements (highest priority)
2. Contractual agreement with New Era
3. This Supplier Code of Conduct

Updates

New Era may update this Code of Conduct periodically. The latest version will be published at: www.neweratech.com.

Acknowledgment

By engaging in business with New Era Technology, suppliers and subcontractors confirm that they have received, understood, and agree to comply with this Supplier Code of Conduct, in addition to all contractual obligations.

Document Information

Reference	Security Framework
Title	Vendor Management /Supplier Security Policy
Purpose	The purpose of the New Era Technology Vendor Management / Supplier Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to New Era Technology, its business partners, and its stakeholders from any of its vendors and or suppliers.
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 2,3,5,6	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.
New Era GRC Policy	Cloud Computing Policy	Policy to define the activities associated with the provision of security for cloud-supported activities that protect New Era Technology's cloud-based information systems, networks, data, databases and other information assets.
New Era GRC Policy	Risk Management Policy	Policy establishing the requirements for the assessment and treatment of information security-related risks facing the business.
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.