Security Policy

Classification: Public

Security Policy Statement

New Era Technology and its subsidiaries (collectively the “Company” or “New Era”) are committed to safeguarding Company and customer data, systems, and infrastructure by implementing robust security measures and adhering to established protocols that govern cybersecurity and responsible use.

This Policy applies to all individuals who access or manage Company information resources, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All users are expected to act responsibly and follow approved procedures to protect the confidentiality, integrity, and availability of information assets.

New Era will implement and maintain controls to ensure that:

- Security requirements are embedded in systems and processes.
- Access to information and resources is authorised and monitored.
- Data is protected against unauthorized access, alteration, or loss.
- Cybersecurity practices comply with applicable laws and Company standards.
- Periodic reviews and audits validate security effectiveness.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“availability”	property of being accessible and usable on demand by an authorized entity.
“confidentiality”	property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
“information security”	preservation of confidentiality, integrity and availability of information.
“integrity”	property of accuracy and completeness.
“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

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 Security Policy is New Era’s corporate policy. New Era Technology business units and/or subsidiaries may complement this with a local/regional information 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 security standards.

If any additional security or information 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 security or information security policies.

The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

Information security is the preservation of confidentiality, integrity and availability of information.

New Era Technology is committed to preserving the confidentiality, integrity and availability of all physical and electronic information assets throughout the organization:

- Confidentiality – information is accessible only by authorized users.
- Integrity – the accuracy and completeness of information is maintained.
- Availability – information is accessible to authorized users and processes when required.

Information security requirements are aligned with the organization's goals, and our internal integrated management system (IMS) is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

The organization's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of our Security Framework and in accordance with ISO/IEC 27001:2022 requirements. ISO27001 is the primary reference for designing and implementing information security within New Era Technology. The use of the ISO/IEC 27001:2022 Standard enables New Era to design and implement security controls consistently across the organization and to define its requirements for security in third-party contracts and partnerships. The Standard also provides a means of benchmarking against other organizations and a method of checking that security polices and standards are being implemented effectively.

In addition, New Era's Information security controls are further aligned to additional information security-related requirements and frameworks (i.e., SOC 2, NIST Cyber Security Framework (NIST CSF), PCI DSS and GDPR). Application of these controls is supported by documented policies and procedures that are subject to continuous, systematic review and improvement.

Security measures are put in place throughout the Security Framework to ensure New Era Technology data (information) and technology remain secure and protected. The Security Framework incorporates, but is not limited to, the following objectives:

- Only authorized users can securely access technology necessary to perform their roles.
- Only authorized users can securely access and share data necessary to perform their roles.
- Our contractual and legal obligations relating to information security and data protection are met.
- Users accessing our data and technology are aware of their security roles and responsibilities.
- Incidents affecting our data and/or technology are resolved and assessed to improve our controls.

The Security Framework is subject to annual review.

Security Framework

The following policies are included as part of, but not limited to, the Security Framework:

- Acceptable Use Policy
- Asset Management Policy
- Backup and Restore Policy
- Business Continuity and Disaster Recovery Policy
- Change Management - Change Control Policy
- Clear Desk and Clear Screen Policy
- Cloud Computing Policy
- Data Classification and Management Policy
- Data Protection Policy
- Encryption Policy
- Identity and Access Management (IAM) Policy
- Incident Response Policy
- Media Sanitization and Destruction Policy
- Mobile Devices and BYOD (Bring Your Own Device) Policy
- Network Management Policy
- Remote Access Policy
- Remote Worker Security Policy
- Risk Management Policy
- Security Awareness and Training Policy
- Vendor Management / Supplier Security Policy

Security Framework Change Control

Any changes to the security framework must be jointly approved by the CIO, CTO and Director of Governance, Risk and Compliance and communicated accordingly.

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 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	Security Policy
Purpose	The purpose of this policy is 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. Provide the framework for review and management of security policies at New Era Technology.
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 management, personnel and interested parties.
Review Plan	Annually
Document Classification	Public

Document History

VERSION CONTROL			
Revision	**Date**	**Record of Changes**	**Approved /Released By**
V1.0	May 2022	Approved release	CTO, Dir GRC
V1.1	Oct 2022	Revised scope language	CTO, Dir GRC
V2.0	Sep 2023	Annual review, 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
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.