Security Awareness & Training Policy

Classification: Public

Security Awareness & Training Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to ensuring that all individuals with access to New Era Technology Information Resources receive appropriate security awareness and training to perform their roles responsibly and protect the confidentiality, integrity, and availability of Company information assets.

This Policy applies to all individuals with access to New Era Technology Information Resources, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All personnel are expected to complete required training and adhere to established security practices.

New Era will implement and maintain controls to ensure that:

- Security awareness training is provided to all personnel upon onboarding and refreshed at regular intervals.
- Role-specific training is delivered to individuals with elevated or specialised responsibilities.
- Training content reflects current threats, regulatory requirements, and Company policies.
- Completion of mandatory training is tracked and monitored for compliance.
- Additional guidance and resources are available to support ongoing security awareness.

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.
"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 Security Awareness and Training Policy applies to all individuals responsible for hiring, onboarding, offboarding, and training of personnel given access to New Era Technology Information Resources.

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 security awareness and training standards.

If any additional security awareness and training 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

General

1. The hiring process must ensure candidates have the necessary competence and can be trusted perform their role, particularly where responsibilities involve the use, management or protection of information security.
2. Information security responsibilities must be communicated to employees during onboarding.
3. New Era will regularly assess and measure the effectiveness of its security posture and employee awareness through activities such as phishing simulations, penetration testing, and other security exercises.
4. Upon termination of employment, personnel must be reminded of confidentiality and non-disclosure obligations.

Training and Awareness

1. All new personnel must complete approved security awareness training prior to, or within 30 days of being granted access to New Era Technology Information Resources.
2. All personnel, including third parties and contractors, must be provided with, or have access to, relevant information security policies to enable them to protect New Era Technology Information Resources effectively.
3. All personnel, including third parties and contractors, must acknowledge receipt of and agree to adhere to the New Era Technology Security Policies before access is granted.
4. All personnel must be provided with and acknowledge in writing that they have received and agree to adhere to the Security Policy, Acceptable Use Policy, and any other applicable policies.
5. All personnel must complete security awareness training at least annually, with additional training provided as needed to address emerging threats or changes in policy.

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	Security Awareness and Training Policy
Purpose	The purpose of this policy is to ensure that all personnel with access to New Era Technology Information Resources are adequately vetted, qualified, and trained according to their role.
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	Oct 2024	Annual review, updates to sections 2-6	Dir GRC, SVP Corp A&E
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 27002:2022	Information security, cybersecurity and privacy protection — Information security controls	Guidance document for determining and implementing commonly accepted information security controls.
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.