New Era Technology, Inc. Network Management Policy

Classification: Public

Network Management Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to upholding the rules for the maintenance, expansion, and use of the network infrastructure.

We expect this policy to be upheld by all employees, (permanent, temporary, or contracted), including executives, officers, and directors of New Era.

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, Inc., and its subsidiaries.

2. Scope

The New Era Technology Network Management Policy applies to individuals who are involved in the configuration, maintenance, or expansion of the New Era Technology network infrastructure.

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 to 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 network management standards.

If any additional network 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) and the Chief Technology Officer 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 Chief Technology Officer 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. New Era Technology IT owns and is responsible for the New Era Technology network infrastructure and will continue to manage further developments and enhancements to the infrastructure.
2. To provide a consistent network infrastructure capable of leveraging new networking developments, all cabling must be installed by New Era Technology IT or an approved contractor.
3. Information security requirements must be included in any new information system or enhancements to the existing system.
4. Appropriate technical controls and solutions must be implemented to protect Confidential information from unauthorized transfer, modification, or disclosure (i.e., next-gen firewalls, IDS/IPS, DLP).
5. A map or diagram of the network and data flow, including external connections, must be maintained.
   a. This map or diagram must be updated after any changes to the network occur.
   b. This diagram must be reviewed every 6 months to ensure it continues to represent the network architecture.
6. All systems on the network must be authenticated. Connections to the network must be authorized by IT.
7. All hardware connected to the New Era Technology network is subject to New Era Technology IT management and monitoring standards.
8. Documented baseline configurations must be maintained for all Information Resources that create, collect, store, and/or process confidential or internal information and all network connected resources must be configured to these specifications. The baseline configurations must be stored securely (i.e., encrypted).
9. Operating procedures for activities associated with information processing must be documented and made available to personnel who need access to them.
10. Resource usage must be monitored to ensure the required system performance.
11. Information processing facilities must address redundancy sufficient to meet availability requirements.
12. Changes to the configuration of active network management devices must be made according to the Change Management/Control Policy.
13. The New Era Technology network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by New Era Technology IT Management.
14. All connections of the network infrastructure to external third-party networks are the responsibility of New Era Technology.
15. Groups of information services, users and information systems must be segregated on the network. The perimeter of each domain must be well defined and based on the relevant security requirements.

16. Network devices must be installed and configured following New Era Technology implementation standards.
17. The use of departmental network devices is not permitted without the written authorization from New Era Technology IT Management.
18. Personnel are not permitted to access or alter existing network hardware in any way.
19. Users must not connect to another network and the New Era Technology network simultaneously.

Wireless Networking

1. All wireless access points or devices that provide access to the New Era Technology wireless network must be approved by management.
2. Wireless access points must be placed in secure locations.
3. Wireless networks must be segmented using appropriate technical controls.
4. Authentication settings (passwords, encryption keys, etc.) must be changed on a periodic basis as well as anytime it is suspected that such information has been compromised or if anyone with knowledge of the information leaves the organization.
5. All wireless network traffic must be encrypted in accordance with the New Era Technology Encryption Policy and supporting standards, regardless of information sensitivity.
6. The New Era Technology Wireless Network must not be used inappropriately; in particular, persons must not use the network to:
   a. Intercept or attempt to intercept other wireless transmissions for the purposes of eavesdropping.
   b. Access or run utilities or services which might negatively impact on the overall performance of the network or deny access to the network, e.g., RF jamming, Denial of Service (DoS).
7. New Era Technology wireless network users must not tamper with network access points or security settings.
8. New Era Technology will conduct scans of wireless access points and identify all authorized and unauthorized wireless access points at least quarterly.

Network Cabling

1. Core and distribution racks must be secured and restricted to authorized personnel.
2. All networking cabling must be protected from unauthorized interception, organized, tied down and labeled.
3. All network closets must be secured with auditable controls.
4. Demarcation points need to be secured with adequate segregation or isolation.
5. All ports on switches must be reconciled and inventoried regularly. Where this is not possible, compensating controls must be used and documented.

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 New Era Technology's Chief Technology Officer, or delegate 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	Network Management Policy
Purpose	The purpose of the New Era Technology Network Management Policy is to establish the rules for the maintenance, expansion, and use of the network infrastructure.
Owner	Governance, Risk & Compliance (GRC)
Document Approvers	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 3, 2022	Approved release	CTO, Dir GRC
V2.0	Sep 17, 2023	Annual review; classification & approvers update	CTO, Dir GRC
V3.0	Oct 8, 2024	Annual review, updates to sections 2-6	Dir GRC, SCP Corp A&E
V3.0	Oct 22, 2024	Approved release	CTO, Dir GRC

Control of Hardcopy Versions

The digital version of this document is the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. The printed version of this document is uncontrolled, and cannot be relied upon, except when formally issued by the Director of Governance, Risk and Compliance and /or the Chief Technology Officer and provided with a document reference number and revision in the fields below:

Document Ref.		**Rev.**		**Uncontrolled Copy**	**X**	**Controlled Copy**	

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	Change Management/Control Policy	Policy establishing the rules for the creation, evaluation, implementation, and tracking of changes made to New Era Technology Information Resources.
New Era GRC Policy	Data Classification and Management Policy	Policy providing a system for classifying and managing information resources according to the risks associated with its storage, processing, transmission, and destruction.
New Era GRC Policy	Encryption Policy	Policy establishing the rules for acceptable use of encryption technologies relating to New Era Technology Information Resources.
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements	Requirements to meet the Standard.
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations	Catalog of security and privacy controls for information systems and organizations.