Network Management Policy

Classification: Public

Network Management Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to implementing the necessary requirements to maintain a secure, reliable, and well-managed network infrastructure that supports business operations and protects Company information assets. Our network is designed, operated, and monitored in accordance with recognised international standards and best practices for information security and privacy.

This Policy applies to all individuals who access or manage New Era Technology network resources, including permanent, temporary, and contracted employees, as well as executives, officers, directors, and authorised third parties. All users are expected to act responsibly and in accordance with established procedures to maintain the confidentiality, integrity, and availability of network services.

New Era will implement and maintain controls to ensure that:

- Network confidentiality, integrity, and availability are safeguarded through robust security measures.
- Access controls and authentication mechanisms are applied to prevent unauthorised use.
- Network performance and resilience are monitored and maintained to support business continuity.
- Compliance with legal, regulatory, and industry standards is upheld across all network operations.

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 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 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 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), 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. Ownership and Accountability
    a. New Era Technology IT owns and is responsible for the network infrastructure and and its ongoing development, maintenance, and security.
    b. All changes and enhancements must follow documented change management procedures.
2. Cabling Standards
    a. To maintain a consistent and secure network infrastructure, all cabling must be installed by New Era Technology IT or an approved contractor, following recognized industry standards.
3. Security Requirements for New Systems
    a. Information security requirements must be incorporated into any new system or enhancement, including authentication, encryption, and monitoring controls.
4. Technical Controls
    a. Appropriate technical solutions (e.g., next-generation firewalls, IDS/IPS, DLP) must be implemented to protect confidential information from unauthorized transfer, modification, or disclosure.
5. Network Documentation
    a. A current network and data flow diagram, including external connections, must be maintained.
    b. Updated after any network changes.
    c. Reviewed regularly for accuracy.
6. Authentication and Authorization
    a. All systems on the network must be authenticated and all connections authorized by IT.
    b. Multi-factor authentication should be applied where feasible.
7. Hardware Management
    a. All hardware connected to the network is subject to IT management and monitoring standards.
8. Baseline Configurations
    a. Documented baseline configurations must be maintained for all network-created resources and stored securely (i.e., encrypted).
    b. Devices must be configured to these specifications.
9. Operating Procedures
    a. Documented procedures for network operations must be available to authorized personnel.
10. Performance Monitoring
    a. Resource usage must be monitored to ensure system performance and detect anomalies.

11. Redundancy and Availability
    a. Network facilities must include redundancy measures to meet availability requirements.
12. Change Management
    a. All configuration changes to network devices must follow the **Change Management/Control Policy**.
13. Approved Protocols
    a. Only sanctioned networking protocols may be used.
    b. Any exceptions require IT Management approval.
14. External Connections
    a. All connections to third-party networks must be managed and approved by New Era Technology IT.
15. Network Segmentation
    a. Information services, users and systems must be segregated based on security requirements.
    b. Perimeters must be clearly defined.
16. Device Installation Standards
    a. Network devices must be installed and configured according to New Era Technology standards.
17. Departmental Devices
    a. Use of departmental network devices requires written authorization from IT Management
18. Hardware Access Restrictions
    a. Personnel must not access or alter network hardware without authorization.
19. Dual Network Connections
    a. Users must not connect to another network and the New Era Technology network simultaneously.

Wireless Networking

1. Wireless access points must be approved by IT Management and placed in secure locations.
2. Wireless networks must be segmented and protected by appropriate technical controls.
3. Authentication settings (passwords, encryption keys) must be changed and after suspected compromise.
4. All wireless traffic must be encrypted in accordance with the New Era Technology Encryption Policy.
5. Wireless networks must not be used for:
    a. Intercepting transmissions.
    b. Running utilities or services that degrade performance or deny access.
6. Users must not tamper with wireless access points or security settings.
7. IT will scan for authorized and unauthorized wireless access points at least quarterly.

Network Cabling

1. Core and distribution racks must be secured and accessible only to authorized personnel.
2. Cabling must be organized, labeled and protected from interception.
3. Network closets must be secured with auditable controls.
4. Demarcation points must be segregated or isolated appropriately.
5. Switch ports must be reconciled and inventoried regularly; compensating controls must documented where full reconciliation is not possible.

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	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 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, SCP 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.
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 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.