Remote Access Policy

Classification: Public

Remote Access Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to ensuring secure remote access to Company networks and systems to protect the confidentiality, integrity, and availability of information assets. This includes defining clear rules and requirements for connecting from any authorised device, such as laptops, tablets, and mobile phones, to minimise the risk of unauthorised access and potential harm to the organisation.

This Policy applies to all individuals who access New Era Technology networks remotely, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All personnel are expected to comply with established remote access requirements and act responsibly when connecting to Company resources.

New Era will implement and maintain controls to ensure that:

- Remote access is authorised, secure, and monitored.
- Strong authentication and encryption are enforced for all remote connections.
- Devices used for remote access meet Company security standards and are regularly updated.
- Confidential and sensitive information is protected from unauthorised disclosure.
- Remote access practices comply with all applicable Company policies and regulatory requirements.

Contents

Remote Access Policy Statement 1

1. Terms and Definitions 3

2. Scope 3

Relationship with Local/Regional Policies 4

3. Roles and Responsibilities 4

4. Policy 5

Approved Remote Access Methods 5

Access Approval and Support 5

Security Requirements 5

User Responsibilities 5

Remote Access Compliance 6

5. Compliance, Monitoring and Enforcement 6

6. Acknowledgement 6

Document Information 7

Document History 7

References 8

1. Terms and Definitions

Term / Acronym	Definition / Meaning
"asset", "information asset"	means any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware, software, applications and (confidential) information. Assets must be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization.[1]
"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.
"remote work"	means to work at home or from another remote location by using the internet or a computer linked to one's place of employment, as well as digital communications such as email and phone.
"staff", "users", "personnel"	means those who are employed by New Era Technology on a full-time, 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 Remote Access Policy applies to any individual connecting remotely to New Era Technology Information Resources.

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.

[1] https://en.wikipedia.org/wiki/Asset_(computer_security)

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 remote access security standards.

If any additional remote access 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

Approved Remote Access Methods

1. New Era Technology provides secure remote access through approved methods, including:
    a. Collaboration tools (e.g., Microsoft Teams, Sharepoint,).
    b. Virtual Private Networks (VPNs).
    c. Remote Monitoring and Management tools (e.g., N-Central, Take Control).
    d. Internet-facing services and applications.
    e. Software-as-a-Service (SaaS) platforms.

Access Approval and Support

1. Personnel must contact the IT help desk to:
    a. Connect to an existing remote access service.
    b. Obtain approval before introducing any new remote access method into the New Era environment.
2. Remote access may only be granted following formal approval by the requestor's manager and/or New Era IT.

Security Requirements

1. All remote access connections must:
    a. Use approved remote access methods.
    b. Employ strong encryption and multi-factor authentication.
    c. Be logged and monitored by IT.
2. Remote users must ensure their devices comply with the Mobile Devices and BYOD (Bring Your Own Device) Policy.
3. Non-New Era Technology systems requiring network connectivity must meet all applicable IT standards and cannot connect without prior written authorization from IT Management.
4. Personal equipment used for remote access must meet the same security requirements as Company-owned equipment.

User Responsibilities

1. Authorized users must protect their login credentials and never share them, including with family members.
2. Remote sessions must be terminated after a defined period of inactivity.

3. Remote maintenance of organizational assets must be approved, logged, and performed securely to prevent unauthorized access.

Remote Access Compliance

1. All hosts connected via remote access must comply with applicable policies within the Security Framework.
2. Remote access must be strictly controlled and monitored to prevent unauthorized use.

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	Remote Access Policy
Purpose	The purpose of this policy is to define the rules and requirements for connecting to New Era Technology's networks from any host (cell phones, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damage that may result from unauthorized use of company resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.
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	Aug 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.
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	Mobile Devices and BYOD (Bring Your Own Device) Policy	Policy describing the conditions under which New Era Technology personnel may use corporate owned/provided mobile devices as well as their own personal mobile devices for business purposes. This policy covers mobile phones, tablets, and laptops.
New Era GRC Policy	Remote Worker Security Policy	Policy establishing the rules and conditions under which short and long-term remote working may occur in order to maintain acceptable practices regarding the use and protection of 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.