New Era Technology, Inc. Remote Worker Security Policy

Classification: Public

Remote Worker Security Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to promoting acceptable practices regarding the use and protection of New Era Technology Information Resources.

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
"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]
"BYOD"	means Bring Your Own Device; pertains to non-corporate issued devices, i.e., smart phones, tablets, laptops workstations/desktops.
"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.
"MDM"	means Mobile Device Management of corporate and non-corporate devices.
"mobile device"	means a smart phone, tablet, laptop, etc.
"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.
"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.
"we", "our", "New Era", or "New Era Technology"	refers to New Era Technology, Inc., and its subsidiaries.

2. Scope

The New Era Technology Remote Worker Security 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.

This Policy is not intended to restrict communications or actions protected or required by regional/local laws and regulations.

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

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 remote worker security standards.

If any additional remote worker 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) 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 Requirements

1. Personnel must be approved to work remotely per the *Remote Work Policy* in their local/regional Employee Handbook.
2. Personnel are responsible for complying with New Era Technology policies when working using New Era Technology Information Resources and/or on New Era Technology time. If requirements or responsibilities are unclear, please seek assistance from the Director, GRC.
3. All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on New Era Technology time and/or using New Era Technology Information Resources are the property of New Era Technology.
4. The remote worker is responsible to ensure that non-employees do not access New Era Technology data, including in print or electronic form.
5. Personnel will be required to maintain a regular schedule.
    a. All hours of work must be recorded according to regular New Era Technology policies.
    b. Overtime and time off must have advance approval according to the regular policies of New Era Technology.
6. Equipment and information must be protected according to their classification and in alignment with the Data Classification and Management Policy.
    a. Remote workers are responsible for protecting New Era Technology equipment and information from theft, damage, or other loss while in transit or at the remote work location.
    b. At no time should documents or company equipment be left unattended in a public area.

Internet Connection

1. Personnel must endeavor to not connect to an unsecured Wi-Fi network with New Era Technology equipment or to perform New Era Technology business.
2. Wi-Fi connections must be secured with strong encryption (WPA2). The use of WPA or WAP is not allowed.
3. When connecting to a Wi-Fi network, personnel must use only the pre-approved remote access solution(s).
4. Personnel must not connect to another wireless network and the New Era Technology wireless network simultaneously.
5. The use of split-tunnel VPN is prohibited.
6. Wireless networks must be secured with a strong password, consisting of 16 or more characters.

Equipment

1. Only New Era Technology provided computing devices, such as desktops and laptops, personally owned laptops and/or workstations with approved virus and spyware detection/protection software and active personal firewall protection or approved mobile device (company-issued or BYOD approved) may be used for working remotely.
2. Computing devices must be secured with New Era Technology provided or approved:
    a. Active and up-to-date antivirus software
    b. Active local firewall
    c. Full-disk encryption
    d. Automatic screen lock
3. Personnel are responsible for regularly rebooting their device to allow software patches and updates to be installed.
4. Personally owned devices, are not allowed to be connected to New Era Technology equipment, including wireless connections without appropriate corporate approvals.
5. Maintenance of New Era Technology provided equipment must be provided or pre-approved by IT.

Printing

1. The printing of any non-public New Era Technology information to a public printer is prohibited.
2. Personnel approved for remote working must have (or have access to) a shredder.
3. All non-public New Era Technology information must be secured when not in use and shredded when no longer needed in accordance with New Era Technology's Data Classification and Management Policy.
4. The printing of Confidential information at a remote location is not permitted.

Collaboration Tools (mobile devices, video conferencing, unified communications etc.)

1. Remote personnel must use a New Era Technology provided and/or approved collaboration tools/systems (company-issued or BYOD approved) for all New Era Technology related communication.
2. When other people are present in the remote work location, privacy and confidentiality must be maintained and discretion used to safeguard the conversation/communication.

Office Requirements

1. Workspaces must be secured to protect all New Era Technology equipment and maintain the confidentiality of all information related to the organization and/or its customers.
2. Personnel must allow IT to retrieve the equipment provided to them at any time.
3. New Era Technology may retrieve any New Era Technology information maintained at home by personnel.
4. The use of personal video surveillance on home entrances and exits is encouraged to help ensure the protection of Company-provided equipment and information.

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	Remote Worker Security Policy
Purpose	The purpose of this policy is to establish 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.
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 2, 2022	Approved release	CTO, Dir GRC
V2.0	Sep 17, 2023	Annual review; classification & approvers update	CTO, Dir GRC
V3.0	Oct 1, 2024	Annual review, updates to sections 2-6	Dir GRC, SVP 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	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 Access Policy	Policy defining 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 damages 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.
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.