Remote Worker Security Policy

Classification: Public

Remote Worker Security Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to ensuring that remote working practices uphold the confidentiality, integrity, and availability of Company information assets. This includes implementing measures to protect New Era Technology Information Resources when accessed outside of Company premises.

This Policy applies to all individuals working remotely, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All personnel are expected to follow established security requirements and act responsibly when accessing Company systems and data remotely.

New Era will implement and maintain controls to ensure that:

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

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 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.

[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 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), 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 Requirements

1. Personnel must be approved to work remotely in accordance with the *Remote Work Policy* outlined in their local/regional Employee Handbook.
2. Personnel are responsible for complying with New Era Technology policies when using Company Information Resources or working on Company time. If requirements or responsibilities are unclear, personnel must seek guidance from their line manager or Human Resources.
3. All inventions, intellectual property, and proprietary information developed on Company time and/or using Company Information Resources remain the property of New Era Technology.
4. Remote workers must ensure that non-employees do not access New Era Technology data in any form (print or electronic).
5. Personnel must maintain a regular schedule and comply with timekeeping requirements:
    a. All hours of work must be recorded in accordance with Company policy.
    b. Overtime and time off must be approved in advance.
6. Equipment and information must be protected according to their classification and alignment with the **Data Classification and Management Policy**.
    a. Remote workers are responsible for safeguarding Company equipment and information from theft, damage, or loss while in transit or at the remote location.
    b. Documents and equipment must never be left unattended in public areas.

Internet Connection

1. Personnel must not connect to unsecured Wi-Fi networks when using Company equipment or performing Company business.
2. Wi-Fi connections must use strong encryption (WPA2 or higher). WPA or WAP is prohibited.
3. Only pre-approved remote access solutions may be used when connecting to a Wi-Fi network.
4. Personnel must not connect to another wireless network and the Company network simultaneously.
5. Split-tunnel VPN is prohibited.
6. Wireless networks must be secured with a strong password of at least 16 characters.

Equipment

1. Only Company- provided devices or BYOD-approved with approved security controls may be used for remote work. (see **Mobile Devices & BYOD (Bring Your Own Device) Policy**)
2. Devices must have:
    a. Active and up-to-date antivirus software
    b. Active local firewall
    c. Full-disk encryption
    d. Automatic screen lock

3. Devices must be rebooted regularly to apply patches and updates.
4. Personally owned devices must not connect to Company equipment without prior approval.
5. Maintenance of Company-provided equipment must be performed or approved by IT.

Printing

1. Printing non-public Company information on public printers is prohibited.
2. Remote workers must have access to a shredder for secure disposal of sensitive documents.
3. All non-public information must be secured when not in use and shredded when no longer needed in accordance with the **Data Classification and Management Policy**.
4. Printing Confidential information at remote locations is not permitted.

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

1. Remote personnel must use Company-provided or approved collaboration tools for all work-related communication.
2. When others are present at 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 Company equipment and maintain confidentiality of all information.
2. IT must be allowed to retrieve Company equipment at any time.
3. Company may retrieve any Company information maintained at home by personnel.
4. Use of personal video surveillance on home entrances and exits is encouraged to protect Company 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 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 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 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.
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 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.