New Era Technology, Inc. Mobile Devices & BYOD (Bring Your Own Device) Policy

Classification: Public

Mobile Devices & BYOD Statement

The purpose of this policy is to describe 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.

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 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, Inc., and its subsidiaries.

2. Scope

In line with the New Era Mobile Device Management (MDM) Policy, the purpose of this Policy is to describe 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.

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.

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

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 BYOD 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 BYOD standards.

If any additional BYOD 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 with mobile (electronic portable) devices 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 security or information security policies.

The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

This Policy should be read in conjunction with, and is not meant to replace, the New Era Technology Mobile Device Management (MDM) Policy located on the New Era Intranet.

Overview

- The use of a personally owned mobile device to connect to the New Era Technology network is a privilege granted to employees only upon formal approval of IT Management.
- New Era Technology confidential information must only be stored on compliant BYOD devices (see section *BYOD Requirements)*.
- Theft or loss of any device that has been used to create, store, or access confidential or internal information must be reported to a member of the IT team immediately.
- All mobile devices must adhere to the BYOD Security requirements in section *BYOD Security*.
- All mobile devices must meet the BYOD requirements in section *BYOD Requirements*.
- All personnel are expected to use mobile devices in an ethical manner.
- New Era Technology IT Management may use MDM security controls for mobile devices without warning to maintain the security and integrity of New Era Technology Information Resources.
- New Era Technology IT support for personally owned mobile devices is limited to assistance in complying with this policy. New Era Technology IT support may not assist in troubleshooting device itself or device usability issues.
- The use of personally owned devices must be in compliance with all other New Era Technology policies.
- New Era Technology reserves the right to revoke personally owned mobile device use privileges in the event that personnel do not abide by the requirements outlined in this policy.

BYOD Use

BYOD covers the use of a personal device for work purposes. This includes accessing the following corporate resources:

- New Era Technology email, calendars, address books/contacts, and
- New Era Technology business applications or cloud services used and approved by IT Management.

New Era Technology IT reserves the right to decline use for a BYOD device deemed a security risk. Approved BYOD devices will have MDM (mobile device management) installed on them – see New Era Technology Mobile Device Management (MDM) Policy.

Messages, documents, and data originating from New Era Technology, transmitted or received on New Era Technology provisioned infrastructure are Company property.

Personnel are not authorized to save or transfer sensitive business data to their personal accounts or on personal devices without MDM.

Personnel must use a professional voice greeting on their voicemail or when answering a call on any device used for New Era Technology business, including any personal mobile device.

The New Era Technology IT department will configure the BYOD device and implement security controls as it deems necessary, at its discretion, to protect the integrity of New Era Technology information resources. This configuration can usually be completed remotely. Such security controls may include, but are not limited to:

- Encryption,
- Password protection,
- Remote wipe capability of those applications with access to New Era Technology information resources,
- Inactivity timer, and
- Data removal after multiple invalid password entries.

As per the corporate Mobile Device Management (MDM) Policy, New Era Technology reserves the right to use MDM in order to maintain security of New Era Technology data; or should the device be lost or stolen; or in the event that the employment relationship is terminated by the employee or by New Era Technology.

- BYOD devices must not be used for any illegal or unlawful purpose, including transmitting violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful material.
- BYOD devices must not be used to harass, intimidate, or otherwise annoy anyone.
- New Era Technology will not be held liable for damages related to inappropriate use of BYOD devices by any New Era Technology personnel or their families.

New Era Technology will not:

- Assume any financial responsibility for BYOD devices or technologies except as agreed with New Era Technology HR / Finance departments.
- Be held liable for damages related to inappropriate use of personal devices by employees, contractors, or their families.
- Be held responsible, in any way, for the contractual terms, physical device, MDM and/or any personal data stored on the device.
- New Era Technology will not reimburse personnel for the following expenses:
    - BYOD initial cost, maintenance, or replacement.
    - Connectivity charges, including Wi-Fi hotspot usage.
    - Insurance.
    - Expenses related to restoring BYOD if lost, corrupted (e.g., malware, incompatible applications, changes to the operating system), or damaged.

The employee must maintain a clear record of all documentation related to contracts, invoices, and monthly statements for the mobile device and services if they choose to use their plan and provider. These documents must be held for seven (7) years for financial audit purposes; otherwise, the employee may risk creating a tax issue if an audit occurs.

BYOD Security

- All devices that access New Era Technology email must have a PIN or other authentication mechanism enabled.
- BYOD devices must not be used for any illegal or unlawful purpose, including transmitting violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful material.
- BYOD devices must not be used to harass, intimidate, or otherwise annoy anyone.
- New Era Technology will not be held liable for damages related to inappropriate use of BYOD devices by any New Era Technology personnel or their families.
- Personnel must not:
    - "Root '' or "jailbreak" a BYOD to free it from pre-defined limitations. This process modifies the system files and can result in an unstable and insecure device.
    - Modify BYOD hardware and/or software beyond the installation of updates provided by the device maker or service provider.
    - Disable BYOD protection systems such as passwords, encryption, firewalls, et cetera without the approval of the New Era Technology IT department.

BYOD Requirements

Any device being used for BYOD must meet the following standards as a minimum:

- Latest updates are installed as soon as available.
- All personally owned laptops and/or workstations that connect to the New Era Technology network must have approved virus and spyware detection/protection software and active personal firewall protection.
- Ability to install and activate the mandatory New Era Technology MDM.

BYOD Changes

Personnel must inform New Era Technology IT if any of the following occurs:

- A new BYOD is acquired and needs access to New Era information resources.
- A BYOD is taken out of service and is no longer used.
- The user's role changes requiring a change in access (e.g., individual changes positions or goes on a leave of absence).

BYOD Support

New Era Technology IT will not support the device outside the approved office productivity applications.

It is the New Era Technology personnel's responsibility to ensure that they are familiar with the device they choose to use and obtain their own training resources in order to successfully use and maintain the device.

New Era Technology personnel must ensure that they can obtain support through their provider and have the relevant contact information available to them should an issue arise.

BYOD – Damaged, Lost or Stolen

Lost or stolen devices must be reported immediately (within 24 business hours) to the employee's manager and to a member of New Era Technology IT team; in addition, law enforcement may also need to be notified.

If the device is damaged, lost, or stolen, it will be the responsibility of New Era Technology personnel to obtain a replacement device. Failure to maintain a device will result in the cancellation of any previously approved reimbursement plan.

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	Mobile Devices and BYOD (Bring Your Own Device) Policy
Purpose	The purpose of this policy is to describe 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.
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	Internal

Document History

VERSION CONTROL			
Revision	**Date**	**Record of Changes**	**Approved /Released By**
V1.0	Aug 16, 2022	Approved release	CTO, Dir GRC
V2.0	Sep 17, 2023	Annual review, approvers update	CTO, Dir GRC
V3.0	Oct 2, 2024	Annual review, updates to sections 2-6	CTO, Dir GRC, SVP Corp A&E
V3.0	Oct 18, 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	Mobile Device Management (MDM) Policy	Policy describing guidelines and procedures for the secure and responsible use of mobile devices within New Era.
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.