Mobile Devices & BYOD (Bring Your Own Device) Policy

Classification: Public

Mobile Devices & BYOD Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to ensuring that the use of mobile devices, whether Company-provided or personally owned, is managed securely and responsibly to protect the confidentiality, integrity, and availability of Company information assets. This includes defining clear requirements for mobile phones, tablets, and laptops used for business purposes.

This Policy applies to all individuals who use mobile devices to access New Era Technology Information Resources, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All personnel are expected to comply with established security requirements and act responsibly when using mobile devices for Company business.

New Era will implement and maintain controls to ensure that:

- Mobile devices meet Company security standards, including encryption, antivirus protection, and automatic screen lock.
- Access to Company systems from mobile devices is authorized and monitored.
- Personally owned devices (BYOD) are approved and configured in accordance with Company policies.
- Confidential and sensitive information is protected from unauthorized access or disclosure.
- Mobile device usage complies 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.
"MAM"	means Mobile Application Management and refers to the set of technologies, policies, and processes used to secure, manage, and control access to business applications and their data on mobile devices, regardless of whether the device is company-owned or personally owned (BYOD).
"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 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.

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

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 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), 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 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) and Mobile Application Management (MAM) Policy** located on the New Era Intranet.

Overview

This section outlines the general principles governing BYOD access and responsibilities.

- The use of a personally owned mobile device to connect to the New Era Technology network is a privilege granted 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 used to create, store, or access confidential or general business information must be reported to IT.
- All mobile devices must adhere to the *BYOD Security* and *BYOD Requirements* sections.
- All personnel are expected to use mobile devices ethically and in compliance with Company policies.
- IT Management may apply MDM and/or MAM security controls without prior notice to maintain the security and integrity of Company Information Resources.
- IT support for personally owned mobile devices is limited to assistance in complying with policy compliance; troubleshooting device usability issues is not provided.
- New Era Technology reserves the right to revoke BYOD privileges if requirements are not met.

BYOD Use

BYOD refers to using a personal device for work purposes, including access to:

- Company email, calendars, and contacts.
- Approved business applications or cloud services.

To maintain security and compliance, the following conditions apply when using personal devices for Company business:

Key requirements:

- IT may deny BYOD use if the device poses a security risk.
- Approved BYOD devices must have MDM and/or MAM installed (see MDM and MAM Policy).
- Company data transmitted via corporate infrastructure remains remains Company property.

- Sensitive business data must not be saved or transferred to personal accounts or devices without MDM/MAM.
- Professional voicemail greetings are required on devices used for Company business.

Security Controls (configured by IT)

To protect Company data, IT may apply the following controls:

- Encryption.
- Password protection.
- Remote wipe capability (via MDM/MAM).
- Inactivity timer.
- Data removal after multiple invalid password attempts.

New Era Technology reserves the right to enforce MDM/MAM controls to protect Company data and may apply these measures without notice, including in cases of device loss, theft, or termination of employment.

Prohibited Use

In order to to maintain ethical and legal standards, the following activities that are strictly forbidden:

- Illegal activities or transmission of prohibited content.
- Harassment or intimidation.

Liability and Financial Disclaimer:

New Era Technology will not:

- Cover device costs, maintenance, connectivity, insurance, or restoration expenses.
- Assume responsibility for personal data, contracts, or damages from inappropriate use.

Employee Responsibilities

Maintain clear records of all documentation related to contracts, invoices, and monthly statements for their mobile device and services for seven (7) years for financial audit purposes. Failure to do so may result in tax issues during audits.

BYOD Security

Mandatory security standards for BYOD devices to prevent data breaches:

- All devices that accessing Company email must have a PIN or other authentication mechanism enabled.
- Devices must not be used for any illegal, unlawful, or inappropriate purposes.
- Personnel must not:
    - "Root '' or "jailbreak" devices.
    - Modify hardware/software beyond approved updates.
    - Disable security features (e.g., passwords, encryption, firewalls, MDM/MAM) without IT approval.

BYOD Requirements

To ensure security and compliance, all personal devices used for Company business must meet the following minimum standards before access is granted; devices must:

- Install updates promptly.
- Have approved antivirus and spyware protection with active firewall.
- Support mandatory MDM and/or MAM installation and activation.

BYOD Changes

Personnel must notify IT if:

- A new BYOD device has been acquired.
- A BYOD device is retired.
- Role changes require access adjustments.

BYOD Support

- The scope of IT support for BYOD devices is limited to approved productivity applications.
- Personnel are responsible for device maintenance and obtaining support from their provider.

BYOD – Damaged, Lost or Stolen

- Lost or stolen devices must be reported within 24 business hours to IT and the employee's manager; law enforcement may also need to be notified.
- Replacement of damaged or lost devices is the responsibility of the employee.
- Failure to maintain a device may result in cancellation of any 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 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	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 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, approvers update	CTO, Dir GRC
V3.0	Oct 2024	Annual review, updates to sections 2-6	CTO, 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	Mobile Device Management (MDM) and Mobile Application Management (MAM) Policy	Policy describing guidelines and procedures for the secure and responsible use of mobile devices and business applications within New Era.
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.