New Era Technology, Inc. Asset Management Policy

Classification: Public

Asset Management Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to maintaining the rules for the control of hardware, software, applications, and information used by New Era Technology.

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

The New Era Technology Asset Management Policy applies to New Era Technology personnel who are responsible for the use, purchase, implementation, and/or maintenance of New Era Technology's 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 to Local/Regional Policies

This Asset Management 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 asset management standards.

If any additional asset management 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

Hardware, Software, Applications and Data

1. All hardware, software and applications intended for New Era Technology business use and installation to use and/or access the corporate network and business applications must be approved by New Era Technology Corporate IT.
2. Installation of new hardware or software, or modifications made to existing hardware or software must follow approved New Era Technology procedures and change control processes.
3. All (asset) purchases must follow the New Era Technology purchasing processes (please contact IT or managers for guidance).
4. Software used by New Era Technology employees, contractors and/or other approved third parties working on behalf of New Era Technology, must be properly licensed.
5. Software installed on New Era Technology computing equipment, outside of that noted in the New Era Technology Standard Software List, must be approved by New Era Technology's Chief Technology Officer, or delegate and installed by New Era Technology IT personnel.
6. Only New Era Technology Corporate IT- authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
7. The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g., personally identifiable information (PII), protected health information (PHI), corporate financial data, etc.
8. Two-factor authentication is required for managing all New Era Technology infrastructure, applications or core services (i.e., DNS, firewalls, active directory etc.),
9. Two-factor authentication is required for users accessing New Era Technology applications containing any confidential information for which New Era Technology has a custodial responsibility.
10. Contracts with cloud computing applications providers must address data retention, destruction, data ownership and data custodian rights.
11. Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
12. A general inventory of information (data) must be mapped and maintained on an ongoing basis.
13. All New Era Technology assets must be formally classified with ownership assigned.
14. Maintenance and repair of organizational assets must be performed and logged in a timely manner and managed by New Era Technology IT Management.
15. New Era Technology assets exceeding a value of 1,000 USD are not permitted to be removed from New Era Technology's physical premises without management approval.
16. All New Era Technology physical assets exceeding a value of 1,000 USD, must contain asset tags or a means of identifying the equipment as being owned by New Era Technology.

17. If a New Era Technology asset is being taken to a High-Risk location, as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by Corporate IT before being taken offsite and before reconnecting to the New Era Technology network.
18. Confidential information must be transported either by New Era Technology personnel or a courier approved by IT Management.
19. Upon termination of employment, contract, or agreement, all New Era Technology assets must be returned to New Era Technology.

Mobile Devices

1. 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.
2. Mobile devices that access New Era Technology email must have a PIN or other authentication mechanism enabled.
3. New Era Technology confidential information must only be stored on compliant BYOD devices (at 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.

Refer to New Era Technology's Mobile Devices and BYOD (Bring Your Own Device) Policy and Mobile Device Management (MDM) Policy for further policy information.

Media Destruction and Re-use

1. All assets and/or media that may contain confidential or internal information must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
2. Media reuse and destruction practices must be conducted in compliance with New Era Technology's media reuse and destruction standards.
3. All decommissioned media must be stored in a secure area prior to destruction.
4. Media reuse and destruction practices must be tracked and documented.
6. Dispose assets only through approved waste handlers or recyclers, and in a manner that complies with applicable regulations; obtain a certificate of destruction when data has remained on the asset.
7. All assets containing storage media must be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
8. Storage media containing confidential or copyrighted information must be physically destroyed or the information must be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.
9. Damaged equipment must undergo a risk assessment to determine whether the items can be physically destroyed rather than sent for repair or discarded.

10. In addition to secure disk erasure, whole-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed.
11. New Era Technology IT must ensure and request confirmation that a cloud service provider has the policies and procedures for secure disposal or reuse of resources.

Backup

1. Backup (and recovery) activities must be performed in compliance with the New Era Technology Backup and Restore Policy.
2. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
3. The New Era Technology backup and recovery process for each system must be documented and periodically reviewed according to the defined review schedule.
4. Any vendor(s) providing offsite backup storage for New Era Technology must be formally approved by New Era Technology's Chief Technology Officer, or delegate to handle the highest classification level of information stored.
5. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest New Era Technology sensitivity level of information stored.
6. A process must be implemented to verify the success of the New Era Technology electronic information backup.
7. Backups must be periodically tested to ensure that they are recoverable in accordance with New Era's backup standards.
8. Procedures between New Era Technology and an offsite backup storage vendor(s) must be reviewed at least annually.
9. Backups containing confidential information must be encrypted in accordance with New Era's encryption standards.

Removable Media

1. The use of removable media for storage of New Era Technology information must be supported by a reasonable business case.
2. All removable media use must be approved by New Era Technology IT prior to use.
3. Personally owned removable media use is not permitted for storage of New Era Technology information.
4. Personnel are not permitted to connect removable media from an unknown origin without prior approval from New Era Technology IT.
5. Confidential and internal New Era Technology information must not be stored on removable media without the use of encryption.
6. All removable media must be stored in a safe and secure environment.
7. The loss or theft of a removable media device that may have contained any New Era Technology information must be reported to the New Era Technology IT team.

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	Asset Management Policy
Purpose	The purpose of this Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by New Era Technology.
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 8, 2024	Annual review, updates to sections 2-6	Dir GRC, SVP Corp A&E, EVP XoC
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	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	Media Sanitization and Destruction Policy	Policy to outline the proper disposal / sanitization / destruction of media (physical or electronic) at New Era Technology.
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	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.