Asset Management Policy

Classification: Public

Asset Management Policy Statement

New Era Technology and its subsidiaries (collectively the “Company” or “New Era”) are committed to to ensuring all information assets - hardware, software, applications, and data -are identified, classified, protected, and managed throughout their lifecycle to support business operations, security, and compliance.

This Policy applies to all individuals responsible for managing or interacting with New Era Technology information assets, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All users are expected to act responsibly and in accordance with established procedures to ensure the security and integrity of Company assets.

New Era will implement and maintain controls to ensure that:

- Asset inventories are accurate and regularly updated.
- Assets are classified and handled based on sensitivity.
- Ownership and accountability are clearly defined.
- Secure disposal is enforced at end-of-life.

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

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.

[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 with 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), 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

Hardware, Software, Applications and Data

1. All hardware, software and applications intended for business use or for accessing the corporate network must be approved by Corporate IT.
2. Installation or modification of hardware or software must follow documented procedures and change control processes.
3. All asset purchases must follow the Company's purchasing processes.
4. Software used by employees, contractors or other approved third parties must be properly licensed.
5. Any software outside the standard approved list must be authorised by Corporate IT and installed by IT personnel.
6. Only authorised cloud applications may be used for storing, sharing, or transferring Company information.
7. Use of cloud services must comply with applicable laws and regulations for sensitive data (e.g., PII, PHI, financial data).
8. Multi-factor authentication is required for managing infrastructure, applications, and core services.
9. Multi-factor authentication is required for accessing applications containing confidential information.
10. Contracts with cloud providers must address data retention, destruction, data ownership and data custodial rights.
11. Hardware, software, and application inventories must be maintained reconciled at least annually.
12. A general inventory of information assets must be maintained and updated regularly.
13. All assets must be formally classified with ownership assigned.
14. Maintenance and repair of assets must be logged and managed by IT.
15. Physical assets exceeding a defined value threshold must not be removed without management approval.
16. High-value physical assets must have asset tags or identification.
17. Assets taken to high-risk locations must be inspected and approved before removal and reconnection.
18. Confidential information must be transported by authorized personnel or approved couriers.
19. All assets must be returned upon termination of employment or contract.

Mobile Devices

1. Use of personal devices to connect to the corporate network requires formal IT approval.
2. Mobile devices accessing Company email must have a PIN or other authentication mechanism enabled.
3. BYOD devices must meet minimum security requirements (latest updates, antivirus, firewall, and mandatory MDM/MAM enrolment).

Refer to New Era Technology's **Mobile Devices and BYOD (Bring Your Own Device) Policy** and **Mobile Device Management (MDM) and Mobile Application Management (MAM) Policy** for detailed requirements.

Media Destruction and Re-Use

1. Media containing confidential or general business (internal) information must be securely erased, destroyed, or rendered unusable before disposal or reuse.
2. Media destruction and reuse must follow Company standards and be documented.
3. Decommissioned media must be stored securely prior to destruction.
4. Disposal must be through approved vendors with certificates of destruction obtained.
5. Storage media must be verified to ensure sensitive data and licensed software are removed or securely overwritten.
6. Physical destruction or secure erasure techniques must be used to make data non-retrievable.
7. Damaged equipment must undergo risk assessment before repair or disposal.
8. Whole-disk encryption should be used to reduce risk during disposal or redeployment.
9. IT must confirm cloud providers have secure disposal and reuse procedures.

Refer to New Era Technology's **Media Sanitization and Destruction Policy** for detailed requirements.

Backup

1. Backup and recovery must comply with the New Era Technology's Backup and Restore Policy.
2. Backup frequency and scope must reflect data importance and risk.
3. Backup processes must be documented and reviewed periodically.
4. Offsite backup vendors must be formally approved to handle the highest classification level of data.
5. Physical access controls at offsite locations must meet or exceed source systems' controls.
6. Backup success must be verified regularly.
7. Backups must be tested periodically for recoverability.
8. Vendor procedures must be reviewed annually.
9. Backups containing confidential data must be encrypted.

Removable Media

1. Use of removable media must be justified by business need and approved by IT.
2. Personally owned removable media is prohibited for Company data.
3. Unknown-origin media must not be connected without IT approval.
4. Confidential data on removable media must be encrypted.
5. Removable media must be stored securely.
6. Loss or theft of removable media must be reported immediately.

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	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 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, EVP XoC
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	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) 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.