New Era Technology, Inc. Data Classification & Management Policy

Classification: Public

Data Classification & Management Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to the proper classification and management of information resources according to the risks associated with its storage, processing, transmission, and destruction.

We expect this policy to be upheld by New Era Technology management, personnel and interested parties.

Contents

1. Terms and Definitions 3
2. Scope 3

Relationship to Local/Regional Policies 4

3. Roles and Responsibilities 4
4. Policy 5

Data Classification & Handling Matrix 5

5. Compliance, Monitoring and Enforcement 8
6. Acknowledgement 8

Document Information 9

Document History 9

Control of Hardcopy Versions 9

References 10

1. Terms and Definitions

Term / Acronym	Definition / Meaning
"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 owner"	• The person responsible for, or dependent upon, the business process associated with an information resource. • Is knowledgeable about how the information is acquired, transmitted, stored, deleted and otherwise processed. • Determines the appropriate value and classification of information generated by the owner or department. • Controls access to their information and must be consulted when access is extended or modified.
"Information user"	• The person, organization or entity that interacts with information for the purpose of performing an authorized task. • Has a responsibility to use information in a manner that is consistent with the purpose intended and in compliance with policy.
"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

This Policy applies to those who access, process, or store New Era Technology data, including paper documents and digital data. It applies to all of the organization's employees, as well as to third-party agents authorized to access the data.

This Policy also 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 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 data classification and management 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 data classification and management standards.

If any additional data classification and 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

Information owned, used, created or maintained by New Era Technology will be classified into one of the following three categories:

1. Public
2. Internal
3. Confidential

The Data Classification & Handling Matrix provides definitions for data classification. It specifies data handing, labeling and marking, physical and administrative controls, reproduction, distribution, storage, retention, destruction, and disposal of data, and must be followed at all times.

Data Classification & Handling Matrix

	DATA CLASSIFICATION		
Labelling (Protective Marking) Guidance	• Document authors will need to ensure that classification status markings are applied appropriately to all documents using the appropriate classifications of '**PUBLIC'**, '**INTERNAL'** or '**CONFIDENTIAL'**. • **If a label is not automatically applied and/or correct, the document owner must manually update the document.** • All information must be marked with the appropriate classification clearly. ○ **New Era recommends, as a minimum, labels are applied in the document header or footer prior to storing, sharing and/or printing**. • Any information that is **not specifically marked** as being 'CONFIDENTIAL or 'INTERNAL' will be **deemed to be 'PUBLIC'**. ***Note***: Removable media such as USB data sticks etc. used to store New Era information must always be classified as 'CONFIDENTIAL' and do not require individual labelling or marking.		
	Public	**Internal**	**Confidential**
Definition	Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders.	Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient.	Highly sensitive or valuable information, both proprietary and personal. Information that is protected by statutes, regulations, New Era Technology policies, or contractual language. Unauthorized or unintentional disclosure of this information could cause legal, competitive, or reputational damage.

Example Documents / Records	Marketing materials authorized for public release such as: • advertisements • brochures • published annual accounts • Internet Web pages • catalogues • external vacancy notices	Most corporate information falls into this category: • departmental memos • information on internal bulletin boards • training materials • policies • operating procedures • work instructions • guidelines • phone and email directories • marketing or promotional information (prior to authorized release) • investment options • transaction data • productivity reports • disciplinary reports • contracts (where no more restrictive confidentiality agreement exists) • Service Level Agreements • internal vacancy notices • intranet Web pages	• Passwords / PIN codes/ VPN tokens • Company intellectual property and trade secrets • Customer data shared and/or collected during a consulting engagement. • Financial information including credit card and account numbers. • Social Security/National Insurance, Social Insurance Numbers; etc. • Personnel and/or payroll records. • Any Information identified by government regulation to be treated as confidential or sealed by order of a court of competent jurisdiction. • Any Information belonging to a New Era Technology customer that may contain personally identifiable information. • Patent information.
Handling	Data may be disclosed or passed to persons outside the organization; has no regulatory restrictions (local, state, federal or contractual).	Disclosure to anyone outside of New Era Technology must be approved (in writing) by a Director-level senior manager.	Must not be disclosed outside of the organization without the explicit written/documented permission of a Director-level senior manager.
Physical & Admin Controls	None	**Author/Owner**: responsible for proper markings. **User/Owner**: responsible for proper storage and document control.	**Author/Owner**: responsible for proper markings. **User/Owner**: responsible for proper storage and document control, must ensure that confidential information is distributed on a strict need-to-know basis.
Reproduction	Unlimited	Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement.	Limited copies may be made only by (written) permission of owner or their designates.

Distribution	No Restrictions	**Hardcopy** • **Intercompany**: use an internal mail envelope. • **External**: use a sealed envelope. **Electronic**: use internal email system. Encryption is required for transmission to external email addresses.	**Hardcopy** • **Intercompany**: use a sealed envelope inside an internal mail envelope. Hand-deliver if possible. • **External**: use a plain sealed envelope. Hand-deliver or send by registered mail, courier etc. **Electronic**: use internal email system; approved company drop box. Encrypt data.
Storage	No Restrictions	**Hard copies:** must be stored in a secured location (locked cabinet or desk drawer) when not in use. **Electronic data:** must be stored in access-controlled drives/folders.	**Hard copies:** must be stored in a secured location (locked cabinet or desk drawer) when not in use. **Electronic data:** must be stored in access-controlled drives/folders.
Retention	No Restrictions	• According to specific schedule established by author or owner. • Until no longer needed • Until information has been superseded by an update • Until downgraded to public information.	• According to specific schedule established by author or owner. • Until no longer needed • Until information has been superseded by an update Until downgraded to public information.
Destruction / Disposal	Recycling / Trash	**Paper documents:** shred. **Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.	**Paper documents:** shred using a confidential bin or commercial grade shredder. **Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.

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	Data Classification and Management Policy
Purpose	The purpose of this policy is to provide a system for classifying and managing information resources according to the risks associated with its storage, processing, transmission, and destruction.
Owner	Governance, Risk & Compliance (GRC)
Document Approvers	Chief Technology Officer (CTO) Director of Governance, Risk & Compliance (GRC)
Intended Audience	New Era Technology management, personnel and interested parties.
Review Plan	Annually
Document Classification	Public

Document History

VERSION CONTROL			
Revision	**Date**	**Record of Changes**	**Approved /Released By**
V1.0	May 24, 2022	Approved release	CTO, Dir GRC
V1.1	Aug 9, 2023	Review	Dir GRC
V2.0	Sep 17, 2023	Annual review; classification & approvers update	CTO, Dir GRC
V3.0	Sep 20, 2024	Annual review, updates to sections 2,3,5,6	Dir GRC
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	Asset Management Policy	Policy establishing the rules for the control of hardware, software, applications, and information used by New Era Technology.
ISO 27000:2014	Information security management systems	Overview and vocabulary.
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.