Data Classification & Management Policy

Classification: Public

Data Classification & Management Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to implementing the necessary requirements to ensure the proper classification and management of information resources based on the risks associated with their storage, processing, transmission, and destruction.

This Policy applies to all individuals who create, access, store, transmit, or manage Company 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 safeguard the confidentiality, integrity, and availability of Company information.

New Era will implement and maintain controls to ensure that:

- Information assets are classified according to sensitivity and risk, following this Data Classification and Management Policy.
- Handling, storage, and transmission of information complies with legal, regulatory, and contractual requirements.
- Retention and disposal of information assets follow approved methods to prevent unauthorised access or recovery.

.

Contents

1. Terms and Definitions

CLASSIFICATION LABELS	Definition / Meaning
Public	Approved for unrestricted disclosure; no business or regulatory risk.
General Business / Internal	Low-sensitivity business information for internal use; may be shared externally with trusted parties under agreement.
Confidential	Sensitive or regulated data requiring strict access controls (e.g., financial reports, customer data, PII).
Highly Confidential	Critical, highly sensitive data that would cause significant harm if disclosed (e.g., strategic plans, intellectual property, key financial records).

Term / Acronym	Definition / Meaning
"data"	are items of information.
"DLP"	means Data Loss Prevention. Refers to the set of security technologies, processes, and controls used to detect, prevent, and monitor the unauthorized disclosure, transmission, or extraction of sensitive information from the organization.
"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.
"MFA"	means Multi-Factor Authentication. A security control that requires users to verify their identity using two or more independent authentication factors before gaining access to company systems, data, or applications.
"PII"	means Personally Identifiable Information. Any information that can uniquely identify people as individuals, separate from all others, is PII.
"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

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 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 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), Chief Information Officer (CIO) 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 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 create, access, store, transmit, or dispose of New Era Technology 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

This Policy establishes a framework for classifying, labeling, and managing information resources using New Era Technology's data protection and labeling system. It ensures data is protected according to its sensitivity and risk throughout its lifecycle.

Classification Levels

Label	Definition
Public	Information approved for unrestricted disclosure, including corporate policies published on the New Era website. No business or regulatory risk.
General Business (also referred to as Internal)	Business information with minimal sensitivity. Intended primarily for internal use but may be shared externally with trusted parties under agreements. Includes internal policies not intended for public release.
Confidential	Sensitive business or regulated data requiring strict access controls. Examples include financial reports, customer data, Sensitive Personal Information (SPI), Personally Identifiable Information (PII).
Highly Confidential	Very sensitive business data that would cause damage to the business if it was shared with unauthorized people. Examples include strategic plans, intellectual property, or financial records which must be safeguarded to maintain the charity's competitive advantage, operational integrity, and business continuity.

Labelling Guidance

Automated Labeling: Where supported by New Era's data protection systems, sensitivity labels will be applied automatically based on predefined rules (e.g., detection of sensitive information such as financial data or personal identifiers).

Employee Responsibility: Employees will not be required to apply labels using technical tools. If automated labelling has been implemented, they must correctly identify the classification category (Public, General Business, Confidential, Highly Confidential) and follow the handling requirements for that category. If automated labelling has not been implemented, employees must either clearly mark the classification in the document header/footer (e.g., 'Confidential') per the section below or apply the appropriate label to the document using the labelling option in the file properties or ribbon (e.g., in Microsoft Word or Outlook).

Manual Labeling for Non-Automated Content: For documents that do not have automated labelling implemented employees must:

1. Clearly mark the classification in the document header/footer (e.g., 'Confidential').
2. Apply the appropriate label to the document using the labelling option in the file properties or ribbon (e.g., in Microsoft Word or Outlook).
3. Apply any required visual indicators (watermarks, stamps) as per the Data Classification & Handling Matrix.
4. Ensure proper handling controls (secure storage, restricted access).

If unsure about classification or labeling, employees should consult their line manager or IT.

Example Documents by Classification

Classification	Example Documents / Records
Public	• Press releases • Published product specifications • Public website content • Corporate policies published on the New Era website
General (or Internal)	• Departmental memos • Internal bulletin board information • Training materials • Internal policies (not published externally) • Operating procedures • Work instructions • Guidelines • Phone and email directories

General (or Internal) **(cont'd)**	• Marketing or promotional information (prior to authorized release) • Investment options • Transaction data • Productivity reports • Internal vacancy notices • Intranet web pages
Confidential	• 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 • Personnel and/or payroll records • Any information identified by government regulation to be treated as confidential or sealed by court order • Any information belonging to a New Era Technology customer that may contain personally identifiable information (PII) • Patent information • Disciplinary reports • Contracts (where no more restrictive confidentiality agreement exists) • Service Level Agreements • Customer data • Financial statements • Employee records • Regulated data (GDPR, HIPAA).
Highly Confidential	• Encryption keys, private certificates, and cryptographic materials • Source code for proprietary software or security systems • Detailed vulnerability assessments, penetration test results, and security architecture diagrams • Merger and acquisition plans or strategic business initiatives • Personally Identifiable Information (PII) combined with sensitive financial or health data (e.g., full medical records, tax returns) • Authentication databases (e.g., password hashes, MFA seeds) • Regulatory compliance submissions before public disclosure (e.g., SEC filings, GDPR breach reports) • Legal documents under attorney-client privilege or litigation strategy • Executive compensation details and board meeting minutes • Any data classified as "restricted" by law or contractual obligation (e.g., classified government data, export-controlled information)

Data Classification & Handling Matrix

Retention periods for all classifications are governed by New Era Technology's official retention schedule.

Category	Physical & Admin Controls	Reproduction & Distribution	Storage & Retention	Destruction/Disposal
Public	No special controls	Unrestricted	Standard retention	Normal disposal
General	Access limited to employees and trusted external parties under agreements	Internal systems or secure external channels	Secure internal systems; optional encryption	Shred physical copies; delete securely
Confidential	Restricted access, encryption	Approved recipients only; no external sharing without legal approval	Encrypted storage, MFA, DLP monitoring	Secure shredding, certified wipe
Highly Confidential	Strict access control (least privilege), encryption, MFA, logging	No reproduction without executive approval; distribution only via secure, encrypted channels	Encrypted storage with key management; retention per legal/regulatory requirements	Physical destruction (cross-cut shred), certified digital wipe, cryptographic erasure

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	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 Information Officer (CIO) 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 2022	Approved release	CTO, Dir GRC
V1.1	Aug 2023	Review	Dir GRC
V2.0	Sep 2023	Annual review; classification & approvers update	CTO, Dir GRC
V3.0	Sep 2024	Annual review, updates to sections 2,3,5,6	Dir GRC
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	Asset Management Policy	Policy establishing 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 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.