Encryption Policy

Classification: Public

Encryption Policy Statement

New Era Technology and its subsidiaries (collectively the “Company” or “New Era”) are committed to implementing the necessary requirements to ensure the secure and appropriate use of encryption technologies to protect the confidentiality, integrity, and availability of Company information resources.

This Policy applies to all individuals who create, access, 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 apply encryption wherever required.

New Era will implement and maintain controls to ensure that:

- Encryption is applied to data at rest, in transit, and during processing in accordance with recognised industry standards and organisational security requirements.
- Approved encryption methods and key management practices are used to safeguard sensitive and confidential information.
- Encryption activities comply with applicable legal, regulatory, and contractual obligations.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“data”	are items of information.
“cryptography”	means the process of encrypting and decrypting data.
“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.
“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:

- All systems, networks, applications, cloud environments, and devices handling New Era Technology data.
- All employees, contractors, and third parties who access or manage encrypted data.
- All data classified as Confidential or higher under New Era’s Data Classification and Management Policy.

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 Encryption 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 encryption standards.

If any additional acceptable use 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.

The Information Technology (IT) departments and / or asset owners are responsible for managing encryption activities for New Era Technology.

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 acceptable use policies.

The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

Overview

This policy establishes requirements for the secure use of encryption technologies to protect the confidentiality, integrity, and availability of New Era Technology's information resources. It ensures compliance with legal, regulatory, and contractual obligations and supports the organisation's Integrated Management System (IMS).

Policy Governance and Responsibilities

1. Approval of Encryption Technologies
    a. All encryption technologies and techniques must be approved by the Chief Information Officer (CIO).
    b. Cryptographic solutions must provide:
        i. Authentication
        ii. Message authentication (e.g., code signature, message signature)
        iii. Encryption (in transit, at rest, and in use)
        iv. Key management and certificate management
2. Key Management Responsibility
    a. New Era Technology IT Management is responsible for distributing, managing, and securing all encryption keys using a commercially approved key management system.
3. Access to Encrypted Data
    a. Encryption must be implemented in a manner that allows authorised personnel to access data promptly for investigation, compliance, and business continuity.
4. Approved Technologies
    a. Only encryption technologies approved, managed, and distributed by New Era Technology IT may be used with New Era Technology information resources.
5. Encryption Standards
    a. IT Management will maintain Encryption Standards specifying:
        i. Approved algorithms and key lengths (e.g., AES-256 for data at rest, TLS 1.2+ for data in transit).
        ii. Key lifecycle management: generation, storage, rotation, archiving, retrieval, distribution, retirement, and destruction.
6. Mandatory Encryption for Confidential Data
    a. All information classified as Confidential must be encrypted when:
        i. Transferred electronically over public networks.
        ii. Stored on mobile storage devices.

iii. Stored on laptops or other mobile computing devices.
iv. At rest in any approved system or cloud environment.

7. Prohibited Practices
    a. Proprietary or non-standard encryption algorithms are prohibited unless explicitly approved by the CIO.
    b. Data transfer without encryption requires prior CIO approval.
8. External Storage and Transfer
    a. Any data (encrypted or not) stored or transferred outside New Era-approved systems must be approved by the CIO.

Cryptographic Controls

1. Cryptographic controls must be applied to sensitive information, including:
    a. Personally Identifiable Information (PII)
    b. Protected Health Information (PHI)
    c. Payment card data
    d. Passwords and authentication credentials
    e. Intellectual property
    f. Legal and financial documents
    g. Research and development information
2. All encryption mechanisms must:
    a. Be authorised by the CIO.
    b. Meet relevant regulatory and legal requirements, including import/export restrictions and international cryptography laws.
    c. Prohibit deprecated algorithms.

Key Management

1. All encryption keys must be managed using a secure key management system.
2. Access to keys must be restricted to authorised personnel with role-based access controls.
3. Master keys and privileged access must require dual control (at least two administrators).
4. Keys must be:
    a. Randomly generated and resistant to brute-force attacks.
    b. Rotated periodically based on risk and compliance requirements.
    c. Securely destroyed when retired.
5. When transmitting keys to third parties, use a separate secure channel from the encrypted data.
6. All key recovery operations must be authorised and logged.
7. IT Management must review key management logs at least annually.

Network Encryption

1. All sensitive information classified as Confidential must be encrypted when transmitted outside New Era networks.
2. Approved protocols include TLS 1.2 or higher, IPsec, and SSL/TLS VPNs.
3. Remote management sessions must always use strong session encryption

Storage (Data-at-Rest) Encryption

1. All sensitive information classified as Confidential must be encrypted at rest.
2. Hardware-based encryption is preferred over software-based encryption where feasible.
3. All laptops and desktops must use full disk encryption (e.g., BitLocker or equivalent).

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	Encryption Policy
Purpose	The purpose of the New Era Technology Encryption Policy is to establish the rules for acceptable use of encryption technologies relating to New Era Technology Information Resources.
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 responsible for setting up or maintaining New Era Technology encryption technology.
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
V1.1	Aug 2023	Review	Dir GRC
V2.0	Sep 2023	Annual review, classification & approvers update	CTO, Dir GRC
V3.0	Oct 4 2024	Annual review, updates to sections 2-6	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	Identity and Access Management (IAM) Policy	Policy to establish the requirements necessary to ensure that access to and use of New Era Technology Information Resources is managed in accordance with business requirements, information security requirements, and other New Era Technology policies and procedures.
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.