Cloud Computing Policy

Classification: Public

Cloud Computing Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to implementing the necessary requirements to ensure the security of all cloud-supported activities. This includes safeguarding New Era's cloud-based information systems, networks, applications, data, databases, and other information assets against unauthorised access, disclosure, alteration, and destruction.

This Policy applies to all individuals who access, manage, or interact with cloud-based resources within New Era Technology, 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 maintain the confidentiality, integrity, and availability of Company information assets in cloud environments.

New Era will implement and maintain controls to ensure that:

- Approved security measures are applied to all cloud environments in line with industry best practices and vendor recommendations.
- Cloud-based systems and data are protected against unauthorised access, modification, or destruction.
- Cloud security activities comply with legal, regulatory, and contractual requirements, as well as Company policies and standards.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
"cloud computing"	means delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. Examples of common cloud service providers: • Infrastructure providers like Amazon Web Services and Microsoft Azure. • Platform and architectural delivery services like Salesforce and Google Apps. Electronic mail systems like Outlook 365 and Gmail.
"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.
"PII"	means Personally Identifiable Information. Any information that can uniquely identify people as individuals, separate from all others, is PII. It may include the following: name, address, email, telephone number, date of birth, passport number, fingerprint, driver's license number, credit or debit card number, Social Security number
"staff", "users", "personnel"	means those who are employed by New Era Technology on a fulltime, 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 New Era Technology infrastructure, systems, data, and networks deployed in private, hybrid, and public cloud environments.
- All other IT assets implemented in cloud services as identified by IT department management.
- All employees, contractors, and third parties who access or manage cloud resources.

This Policy is in line with the New Era Technology **Vendor Management/ Supplier Security Policy**.

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 cloud computing 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 cloud computing standards.

If any additional cloud computing 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

This Policy establishes the security requirements for all cloud-based infrastructure, systems, applications, and data used by New Era. It ensures that cloud services are implemented, managed, and monitored in a manner that protects confidentiality, integrity, and availability, and complies with legal, regulatory, and contractual obligations.

Cloud Usage Approval

All cloud computing usage must be approved by the IT department in collaboration with Security Operations and Governance, Risk And Compliance (GRC) teams.

Governance and Security Responsibilities

The IT department, working closely with Security Operations, will:

- Define and maintain cloud security processes and procedures.
- Implement specialised security tools and controls to mitigate cloud-related threats.
- Ensure continuous monitoring and automated alerting for suspicious activities across all cloud environments.

Cloud Security Operations

The following activities will be carried out by the Enterprise IT department (under the CIO), in collaboration with Security Operations and supported by the CTO Office for helpdesk and triage functions. These responsibilities ensure that cloud environments remain secure, compliant, and resilient.

Security Testing and Assurance

- Conduct continuous vulnerability scanning and periodic penetration testing of internal and vendor-managed cloud environments.
- Validate that cloud service providers maintain equivalent security measures and provide evidence of compliance.

Risk Management

- Perform regular risk assessments of internal and external threats and vulnerabilities affecting cloud environments.
- Update risk assessments following significant changes or incidents.

Data Management

- Establish policies for data creation, storage, retention, and destruction in cloud environments.
- Ensure data at rest and in transit is encrypted using industry-standard algorithms (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

Access Control

- Define and enforce policies for accessing cloud-based systems, networks, and applications:
  - Implement least privilege access, multi-factor authentication (MFA), and Zero Trust principles.
  - Apply strong password controls and prohibit password reuse or cycling.
  - Authenticate both internal and external users securely.

Malware and Threat Protection

- Deploy anti-malware solutions and intrusion detection/prevention systems for all cloud environments.
- Verify that cloud service providers maintain equivalent anti-malware capabilities.

Network and Perimeter Security

- Implement layered security controls to prevent unauthorised access to cloud environments.
- Ensure cloud service providers maintain similar perimeter security measures.

Incident Response

- Establish and document a formal process for:
  - Detecting, assessing, and responding to cloud-related security incidents (e.g., phishing, brute force, infrastructure abuse).
  - Coordinating with the Incident Response Plan for containment, eradication, recovery, and post-incident review.
  - Notifying management, regulators, and affected parties as required.
- Maintain detailed records of all incidents and remediation actions.

Internal Threat Management

- Define procedures for identifying and responding to internal cloud security breaches (e.g., theft of information, social engineering, unauthorised access).

Training and Awareness

- Provide cloud security education and awareness programmes for all employees and contractors.

Business Continuity and Disaster Recovery

- Integrate cloud services into business continuity and disaster recovery plans, ensuring resilience and rapid recovery.

Compliance and Legal Requirements

- Ensure all cloud security policies and procedures comply with:
  - ISO/IEC 27001:2022 Annex A.5.23 (Cloud Services) and related controls.
  - Applicable legislative, regulatory, and contractual requirements (e.g., GDPR).

Vendor Management

- Execute Service Level Agreements (SLAs) with cloud service providers that define:
  - Security obligations.
  - Performance expectations.
  - Breach notification requirements.
- Conduct periodic compliance reviews of cloud vendors.

Change Management

- Document all proposed changes to cloud security operations in detail.
- Review and approve changes through the formal change management process.

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	Cloud Computing Policy
Purpose	The purpose of this policy is to define the activities associated with the provision of security for cloud-supported activities that protect New Era Technology's cloud-based information systems, networks, data, databases and other information assets.
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 2,3,5,6	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	Risk Management Policy	Policy establishing the requirements for the assessment and treatment of information security-related risks facing the business.
New Era GRC Policy	Vendor Management Supplier Security Policy	Policy to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to New Era Technology, its business partners, and its stakeholders from any of its vendors and or suppliers.
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.