New Era Technology, Inc. Cloud Computing Policy

Classification: Public

Cloud Computing Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to upholding 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.

We expect this policy to be upheld by all employees, (permanent, temporary, or contracted), including executives, officers, and directors of New Era.

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, Inc., and its subsidiaries.

2. Scope

This Policy applies to all New Era Technology staff, users, and contractors that create, deploy, or support infrastructure, applications, and/or systems software in third-party hosted cloud-based infrastructure. The scope includes all information technology systems, software, databases, applications and network resources that are implemented in cloud-based and/or managed service infrastructures needed by New Era to conduct its business. This Policy is in line with the New Era Vendor Management Supplier Security Policy.

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 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) 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

This Policy addresses all New Era Technology infrastructure, systems, data and networks implemented in private, hybrid and/or public cloud infrastructures, plus all other New Era Technology IT assets implemented in cloud services as identified by IT department management.

1. Cloud computing usage must be approved by IT.
2. The IT department will:
    a. Define cloud security processes and procedures.
    b. Secure and utilize specialized software and systems to reduce the threat of cloud security breaches.
    c. Regularly test the security of New Era's perimeters and the cloud service vendor's perimeters using penetration tests and other forensic methods.
    d. Document all information cloud procedures and controls.
3. The New Era Technology IT department will prepare and document IT information security and cybersecurity plans with a focus on cloud services; it will facilitate the maintenance and review of those plans.
4. The IT department will periodically conduct a risk assessment of the internal and external threats and vulnerabilities of the IT environment, as applicable to all cloud environments.
5. The IT department will establish a policy for data media implemented in cloud services, its creation, storage and destruction.
6. The IT department will establish a policy for accessing New Era Technology systems, networks, applications and files implemented in cloud services, both locally and remotely, including passwords and other cloud security access controls; this policy will also include authentication of New Era Technology and non-New Era Technology users.
7. The IT department will ensure that malware (e.g., viruses, spam, phishing attacks, denial-of-service attacks and other unauthorized access attempts) is prevented through the use of antivirus software and other appropriate prevention and detection resources. It will ensure that cloud service vendors have similar antimalware capabilities and that the use of those services must be approved by New Era Technology.
8. The IT department will establish a network perimeter & cloud environment management layer security policy to ensure that unauthorized attempts to penetrate the New Era Technology cloud security perimeter are prevented. It will also have a similar policy for cloud service vendors.
9. The IT department will establish and document a formal process for identifying a possible breach in cloud-based technologies (e.g., phishing, brute force, infrastructure abuse, web application attack), assessing the breach, determining the nature and possible impact of the breach, notifying New Era Technology management of the breach, minimizing the impact of the breach as quickly as possible,

and documenting the steps taken when dealing with the incident. This process will apply to all cloud environments, whether internal, hybrid and/or public clouds.

10. The IT department will establish and document a formal process for identifying a possible internal cloud security breach (e.g., theft of information, social engineering, unauthorized access to systems), assessing the breach, determining the nature and possible impact of the breach, notifying New Era Technology management of the breach, minimizing the impact of the breach as quickly as possible, and documenting the steps taken when dealing with the incident.
11. New Era will provide cloud security education, training and awareness programs as applicable.
12. The IT department will include business continuity and disaster recovery in its cloud security controls.
13. The IT department will define consequences of violations of cloud security policy.
14. The IT department will define how cloud security incidents are reported and managed.
15. The IT department, in collaboration with the company legal department, must prepare and have executed the appropriate service level agreements (SLAs) with cloud service providers to ensure acceptable third-party cloud vendor performance.
16. Data in use at New Era Technology, whether at rest or in motion, within any approved cloud environment, must be encrypted.
17. All proposed changes to cloud security operations are to be documented in detail.
18. The IT department will develop a schedule of all relevant cloud security activities for the company and will ensure that these activities are completed on time.
19. The IT department will ensure all cloud security policies and associated procedures will comply with appropriate legislative, regulatory and contractual requirements, as well as accepted standards and good practice.

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	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 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 3, 2022	Approved release	CTO, Dir GRC
V2.0	Sep 17, 2023	Annual review; classification & approvers update	CTO, Dir GRC
V3.0	Oct 3, 2024	Annual review, updates to sections 2,3,5,6	Dir GRC, SVP Corp A&E
V3.0	Oct 22, 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	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 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.