Backup & Restore Policy

Classification: Public

Backup & Restore Policy Statement

New Era Technology and its subsidiaries (collectively the “Company” or “New Era”) are committed to upholding the requirements necessary to ensure that data backup and restoration processes support business continuity, information security, and compliance with applicable Company policies and procedures.

This Policy applies to all individuals responsible for managing or interacting with New Era Technology information systems and data, 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 ensure the resilience and availability of Company information assets.

New Era will implement and maintain controls to ensure that:

- Backup and restoration processes are documented and regularly reviewed.
- Backups are performed at defined intervals and stored securely.
- Restoration procedures are tested periodically for reliability.
- Backup data is retained and disposed of in line with requirements.

Contents

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 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

In line with the New Era Technology Business Continuity and Disaster Recovery Policy, this Backup and Restore Policy applies to individuals accountable for ensuring backup and restore processes are developed, supported, tested, and maintained. The scope includes information technology systems, software, databases, applications and network resources needed by New Era Technology to conduct its business.

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 Policy is New Era's corporate policy. New Era Technology business units and/or subsidiaries may complement this with a local/regional backup and restore 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 backup and restore standards.

If any additional backup and restore 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 are responsible for managing data backup and recovery activities for New Era Technology.

The IT departments are also responsible for executing technology disaster recovery (DR) plans to ensure that data are backed up and securely stored, with the ability to quickly access and restore the data as quickly and securely as possible. IT departments are responsible for developing, executing and periodically testing procedures for data backup and recovery.

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

1. Data backup and recovery activities must be performed as part of New Era business continuity (BC) plans and technology disaster recovery (DR) plans, which govern the overall technology data backup program, including:
    a. Planning and design and documentation of data backup and recovery processes.
    b. Assignment of roles and responsibilities, with training and readiness for incident response.
    c. Planning, design and documentation of data backup and recovery plans.
    d. Regular reviews of business impact analyses and risk assessments.
    e. Scheduled exercises and continuous improvement activities.
    f. Awareness and training for employees and backup teams.
2. Formal risk and impact assessments must be conducted and reviewed at least annually to ensure alignment with business and technology requirements.
3. Backup strategies must address critical systems, networks, databases, and data supporting key business activities.
4. Backup data must be encrypted, securely stored, and protected against unauthorised access and environmental risks.
5. Backup and recovery plans must be tested at least annually in a controlled environment to validate effectiveness and ensure personnel understand their roles.
6. All backup and restore activities must be logged, monitored, and retained for compliance and audit purposes.
7. Plans and related documentation must be kept current and reflect changes in business, technology, and regulatory requirements.

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	Backup and Restore Policy
Purpose	The purpose of this policy is to define the activities associated with the provision of data backup and recovery plans and programs that protect New Era Technology 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	Business Continuity and Disaster Recovery Policy	Policy providing direction and general rules for the creation, implementation, and management of the New Era Technology Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
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.