New Era Technology, Inc. Business Continuity & Disaster Recovery Policy

Classification: Public

Business Continuity & Disaster Recovery Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to upholding the direction and general rules for the creation, implementation, and management of the New Era Technology Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

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
"BCP"	means Business Continuity Plan; an operational document to define steps for immediate response, resumption and recovering of business operations after a disaster.
"BIA"	means Business Impact Analysis; BIA identifies what our critical systems, processes and functions are and how quickly they need to be recovered or restored in the event of an outage or disruption.
"data"	are items of information.
"DRP"	means Disaster Recovery Plan; a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident.
"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.
"RPO"	means Recovery Point Objective; it is the maximum length of time permitted that data can be restored from, which may or may not mean data loss. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs. RPO is the time from the last data backup until an incident occurred.
"RTO"	means Recovery Time Objective; it is the targeted duration of time between the event of failure and the point where operations resume. RTO is the time that you set to recover the lost data; downed systems/network; etc.
"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

In line with the New Era Technology Backup and Restore Policy, this Business Continuity and Disaster Recovery Policy applies to individuals accountable for ensuring business continuity and disaster recovery 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 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 business continuity or disaster recovery 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 business continuity and disaster recovery standards.

If any additional business continuity and/or disaster recovery 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.

The Information Technology (IT) departments and / or asset owners are responsible for managing business continuity and disaster 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 business continuity and disaster 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

Business Continuity

Business Continuity focuses on sustaining the organization's critical business processes during and after a disruption.

1. New Era Technology must create and implement Business Continuity Plans ("BCP").
2. BCPs must be tested at least annually, and the results must be shared with executive management.
3. BCPs must be reviewed and updated upon any relevant changes to the organization, at the conclusion of plan testing, or least annually.
4. BCPs must be communicated and distributed to all relevant internal personnel and executive management.
5. Business continuity planning must ensure that:
    a. Safety and security of personnel is the priority.
    b. An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence.
    c. Documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event.
6. BCPs should include, at a minimum:
    a. A Business Impact Assessment (BIA); a risk assessment for critical business processes and operations
    b. An inventory of critical systems and records, and their dependencies.
    c. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for critical business systems and processes.
    d. Requirements for ensuring information security throughout the process.
    e. Identification of supply chain relationships and the organization's role to support critical infrastructure.
    f. Processes to ensure the safety of personnel.
    g. Communication strategies for communications both inside and outside the organization.
    h. Mitigation strategies and safeguards to reduce impact.
    i. Strategies to address and limit the reputational impact from an event.
    j. Contingency plans for different types of disruption events.
    k. Protection and availability of plan documentation.
    l. Procedures for plan tests, review, and updates.

Disaster Recovery

Disaster Recovery focuses on restoring the technology systems that support both critical and day-to-day business operations.

1. New Era Technology must create and implement Disaster Recovery Plans (“DRP”) to support business objectives.
2. DRPs must be tested annually, at a minimum.
3. DRPs must be reviewed and updated upon any relevant change to IT Infrastructure, at the conclusion of plan testing, or least annually.
4. DRPs must be communicated and distributed to all relevant internal personnel and executive management.
5. DRPs should include at a minimum:

a. Roles and responsibilities for implementing a disaster recovery plan.
b. List of potential risks to critical systems and sensitive information.
c. Procedures for reporting disaster events, event escalation, recovery of critical operations, and resumption of normal operations.
d. Requirements for ensuring information security throughout the process.
e. An inventory of backups and offsite storage locations.
f. Contingency plans for different types of disruption events.
g. Protection and availability of plan documentation.
h. Procedures for plan tests, review, and updates.

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	Business Continuity and Disaster Recovery Policy
Purpose	Policy is to provide direction and general rules for the creation, implementation, and management of the New Era Technology Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
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	Sep 19, 2024	Annual review, updates to sections 2,3,5,6	Dir GRC
V3.0	Oct 18, 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	Backup and Restore Policy	Policy 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.
New Era GRC Policy	Data Classification and Management Policy	Policy providing a system for classifying and managing information resources according to the risks associated with its storage, processing, transmission, and destruction.
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.