# Business Continuity & Disaster Recovery Policy

Classification: Public

## Business Continuity & Disaster Recovery Policy Statement

New Era Technology ("New Era" or "the Company") is committed to implementing the necessary requirements to ensure that business continuity and disaster recovery processes protect Company information, maintain operational resilience, and comply with applicable Company policies and procedures.

This Policy applies to all individuals responsible for supporting, managing, or executing business continuity and disaster recovery activities 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 ensure the secure and effective recovery of Company information assets and critical operations.

New Era will implement and maintain controls to ensure that:

- Approved methods and processes are used for business continuity and disaster recovery planning and execution.
- Critical systems and data are protected and recoverable in a manner that minimises disruption and prevents unauthorised access.
- Continuity and recovery activities comply with legal, regulatory, and Company requirements, including testing and validation of plans on a regular basis.

## 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.<br>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.<br>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.<br>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 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 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 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), 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 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.

**Requirements**

1. New Era Technology must create and maintain Business Continuity Plans (BCPs) for critical business processes.
2. BCPs must be tested at least annually, with results reported to executive management.
3. BCPs must be reviewed and updated:
    a. After significant organisational or operational changes.
    b. Following plan tests.
    c. At least annually.
4. BCPs must be communicated and distributed to relevant personnel and executive management.

Business Continuity Planning Must Ensure That:

1. Safety and security of personnel is the priority.
2. 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.
3. Documented plans, response, and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event.

**BCP Components**

BCPs must include, at a minimum:

1. Business Impact Assessment (BIA); a risk assessment for critical processes.
2. Inventory of critical systems records and dependencies.
3. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
4. Information security requirements during continuity operations.
5. Identification of supply chain dependencies and critical infrastructure support.
6. Personnel safety procedures.
7. Internal and external communication strategies.
8. Mitigation strategies to reduce impact.
9. Plans to address reputational risk.

10. Contingency plans for various disruption scenarios.
11. Secure storage and availability of plan documentation.
12. Procedures for testing, review, and updates.

**Governance and Preparedness Requirements**

Business Continuity planning must ensure:

1. Clear roles and responsibilities are assigned for continuity management and decision-making.
2. Integration with organisational risk management processes to align continuity planning with enterprise risk strategy.
3. Regular training and awareness programmes for staff involved in continuity and recovery activities.
4. Scenario-based exercises and tabletop drills to validate readiness and identify gaps.
5. Defined KPIs and performance metrics for recovery objectives to support continuous improvement.

## Disaster Recovery

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

**Requirements**

1. New Era Technology must create and implement Disaster Recovery Plans ("DRP") aligned with business objectives.
2. DRPs must be tested annually, with results reported to executive management.
3. DRPs must be reviewed and updated:
    a. After significant IT infrastructure changes.
    b. Following plan tests.
    c. At least annually.

**DRP Components**

DRPs must include, at a minimum:

1. Roles and responsibilities for implementing a disaster recovery plan.
2. List of potential risks to critical systems and sensitive information.
3. Procedures for:
    a. Reporting and escalating disaster events.
    b. Recovery of critical operations.
    c. Resumption of normal operations.

4. Information security requirements during recovery.
5. Inventory of backups and offsite storage locations.
6. Contingency plans for various disruption scenarios.
7. Secure storage and availability of plan documentation.
8. Procedures for testing, review, and updates.

**Governance and Preparedness Requirements**

Disaster Recovery planning must ensure:

1. RTO and RPO targets are validated during each test to confirm recovery objectives.
2. Cyber-attack and ransomware scenarios are included in DR exercises to strengthen resilience.
3. Backup integrity checks are performed and offline copies maintained for critical data.
4. Documented and tested procedures for activating alternate processing sites or cloud failover are in place.
5. Escalation paths and contact lists are maintained and reviewed regularly for rapid response.
6. Predefined communication templates are available for internal and external notifications during recovery events.

**Continuous Improvement**

1. Lessons learned from tests and real events must be documented and incorporated into updated plans.
2. Plans must be revised to reflect changes in business processes, technology, or 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** | 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 Information Officer (CIO)<br>Chief Technology Officer (CTO)<br>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** | Sep 2024 | Annual review, updates to sections 2,3,5,6 | Dir GRC |
| **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** | 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 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. |