Digital Operational Resilience Act (DORA) Compliance Policy

Classification: Public

Digital Operational Resilience Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to maintaining the highest standards of digital operational resilience in accordance with the EU Digital Operational Resilience Act (DORA). As a technology company, we recognize that robust ICT (Information and Communication Technology) systems and risk management practices are essential to safeguard our operations, protect client data, and ensure continuity of critical services. This statement reflects our dedication to resilience, transparency, and accountability across all business units and third-party relationships.

We expect this Policy to be upheld by New Era Technology management, personnel, and all interested parties.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“availability”	property of being accessible and usable on demand by an authorized entity.
“BIA”	Business Impact Analysis – process to identify critical systems and recovery priorities.
“information security”	preservation of confidentiality, integrity and availability of information.
“integrity”	property of accuracy and completeness.
“BCP”	Business Continuity Plan – operational document defining steps for response and recovery after a disruption.
“confidentiality”	property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
“CTPPs”	Critical ICT third-party providers. **18 November 2025** - The European Supervisory Authorities designate critical ICT third-party providers. The European Supervisory Authorities (EBA, EIOPA, and ESMA – the ESAs) published the list of designated critical ICT third-party providers (CTPPs) under the Digital Operational Resilience Act (DORA). This designation marks a crucial step in the implementation of the DORA oversight framework.
“DORA”	Digital Operational Resilience Act – EU regulation establishing requirements for digital operational resilience in the financial sector.
“DRP”	Disaster Recovery Plan – structured approach for resuming work after an unplanned incident.
“GDPR”	General Data Protection Regulation – EU regulation on data protection and privacy.
“ICT”	Information and Communication Technology – systems and technologies used for information processing, storage, and communication.
“information security”	preservation of confidentiality, integrity and availability of information.
“integrity”	property of accuracy and completeness.
“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

The purpose of this Policy is to define the principles, governance, and operational requirements necessary to comply with DORA and ensure digital resilience across all ICT systems and services.

This Policy applies to all New Era business units, subsidiaries, and employees engaged in the development, delivery, and support of technology products and services. It covers all ICT systems, platforms, and processes that underpin our operations, including cloud infrastructure, software development environments, data centers, and customer-facing applications.

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 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 security standards.

If any additional security or information security 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.

Relevant functions and service owners within New Era shall develop, disseminate, and maintain formal, documented processes and/or procedures to support the implementation of this Policy and, where applicable, any local or regional security or compliance policies. The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

New Era Technology recognises the critical importance of digital operational resilience in safeguarding our organisation, customers, and stakeholders against ICT-related risks and disruptions. In alignment with the EU Digital Operational Resilience Act (DORA), this Policy establishes the foundational principles, responsibilities, and controls that underpin our approach to digital resilience.

The Digital Operational Resilience Principles set out in this Policy define the mandatory requirements and standards for information security, ICT risk management, business continuity, incident response, data protection, and third-party risk management. These principles are designed to ensure the confidentiality, integrity, and availability of our information systems and data, and to support the continuity of our operations in the face of evolving threats.

All employees, contractors, suppliers, and third parties are required to adhere to these principles and the supporting procedures, contributing to a culture of compliance, security, and continuous improvement across New Era Technology.

Digital Operational Resilience Principles

Information Security

In accordance with New Era's corporate Security Policy, information security is maintained by:

- Preserving confidentiality, integrity, and availability of all information assets.
- Aligning security controls with ISO/IEC 27001:2022, NIST SP 800-53, and other relevant frameworks.
- Ensuring only authorised users can access and share data required for their roles.
- Meeting contractual, legal and regulatory obligations for information security and data protection.

New Era Technology will maintain an up-to-date inventory of ICT assets and map these assets to critical and important business functions. This mapping will support risk assessments, resilience planning, and compliance with DORA requirements.

Information Communication Technology (ICT) Risk Management

As required by New Era's corporate Risk Management Policy, ICT risks must be identified, recorded, assessed, and managed across all New Era systems and data.

New Era's risk management framework supports continuous improvement and will ensure compliance with DORA. Business impact analyses (BIA) are conducted to identify critical systems and dependencies; assessments of identified risks are captured in the appropriate risk register(s) and reviewed regularly and upon significant business changes.

Business Continuity and Disaster Recovery

In accordance with New Era's Business Continuity & Disaster Recovery Policy, Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) must be developed, implemented, and tested annually. Plans shall define recovery time objectives (RTO), recovery point objectives (RPO), and detailed procedures for restoring operations after disruptions.

Plans must be communicated to relevant personnel and executive management and reviewed and updated following major organisational changes or in response to nonconformities, observations, or findings identified during testing.

New Era Technology conducts regular resilience testing of ICT systems, including penetration testing and vulnerability assessments. All test results must be documented, reviewed by senior management, and followed by timely corrective actions to address identified gaps or weaknesses.

Incident Response and Reporting

As per New Era's Incident Response Policy, New Era is committed to ensuring that all security incidents are identified, reported, and addressed promptly and in accordance with applicable legal, regulatory, and contractual obligations.

Documented processes are established for classifying, reporting, escalating, and responding to ICT-related incidents. Incidents are resolved, assessed, and used to improve controls.

All major ICT-related incidents must be reported to the relevant competent authorities within the timelines mandated by DORA.

Data Protection and Privacy

Compliant with GDPR, other applicable data protection laws and New Era's Data Protection and Privacy policies, personal data is processed lawfully, fairly, and transparently.

Data minimisation, accuracy, storage limitation, and security measures are implemented.

We are committed to upholding data subjects' rights including, but not limited to data subjects' rights to access, rectification, erasure, restriction, portability, and objection.

Appropriate safeguards are implemented for special category data and cross-border data transfers.

Third-Party Risk Management

Conforming to New Era's Security framework and information security certifications, risks associated with ICT third-party key vendors and/or suppliers must be assessed and managed. New Era's third-party risk management framework supports continuous improvement and will ensure compliance with DORA.

A register of ICT third-party key vendors/suppliers shall be maintained, detailing services provided, risk assessments, and compliance status. Exit and transition strategies for critical ICT third-party relationships will be documented to ensure continuity and resilience in case of termination or disruption.

5. Compliance, Monitoring and Enforcement

This Policy is intended for all New Era businesses.

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 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	DORA Compliance Policy
Purpose	The purpose of this policy is to define the principles, governance, and operational requirements necessary to comply with DORA and ensure digital resilience across all ICT systems and services.
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 management, personnel and interested parties.
Review Plan	Annually
Document Classification	Public

Document History

VERSION CONTROL

Revision	Date	Record of Changes	Approved /Released By
V1.0	Feb 2026	Approved release	CTO, CIO, Dir GRC

References

Standard / Framework / Other	Title	Description
Digital Operational Resilience Act (DORA)	REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	Regulatory requirements for DORA compliance
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.