Incident Response Policy

Classification: Public

Incident Response Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are to implementing the necessary requirements to ensure robust processes for identifying, reporting, and responding to information security incidents in a timely and effective manner. These measures are designed to protect the confidentiality, integrity, and availability of Company information assets and maintain operational resilience.

This Policy applies to all individuals who access or manage New Era Technology information resources, 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 support the Company's efforts to prevent, detect, and respond to security threats.

New Era will implement and maintain controls to ensure that:

- Incidents are identified and reported promptly through approved channels.
- Incident response procedures are followed to contain, mitigate, and recover from security events effectively.
- Compliance with legal, regulatory, and contractual obligations is maintained during incident handling and reporting.
- Lessons learned from incidents are documented and used to improve security measures and reduce future risk.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“incident”	in the context of information security, a security event that, as assessed by the staff, violates the policies of New Era Technology as related to Information Security, Physical Security, or Acceptable Use, or other New Era Technology policy, standard, or code of conduct; or threatens the confidentiality, integrity, or availability of information systems.
“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 Incident Response Policy applies to executive management and other individuals responsible for protecting New Era Technology Information Resources.

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 with Local/Regional Policies

This Incident Response 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 information security incident management standards.

If any additional security incident response or information security incident management 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.

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 acceptable use policies.

The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

Introduction

The purpose of this Policy in safeguarding the confidentiality, integrity, and availability of New Era Technology's information assets is to establish a clear and consistent framework for managing information security incidents. Effective incident management is critical to minimizing operational disruption, safeguarding sensitive data, and reducing financial, legal, and reputational risks.

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. This Policy outlines the responsibilities, processes, and communication protocols required to respond effectively to incidents and maintain trust with customers, partners, and stakeholders.

An information security incident is any event that results in a compromise of the confidentiality, integrity, or availability of an information asset. Examples include:

- Intentional or accidental disclosure of any New Era data, in particular confidential information to anyone not authorized to view it.
- Loss or theft of paper records, data or equipment such as files, tablets, laptops, or smartphones on which data is stored.
- The execution of a malicious program designed to infiltrate and damage computers without the user's consent (e.g. malware or viruses from clicking on links or attachments in e-mails or from visiting compromised websites).
- Denial of service attacks (e.g. deliberate attempts to interrupt or suspend services of a host connected to the Internet).
- Security attacks on IT equipment systems or networks (e.g. hacking, malware and ransomware).
- Breaches of physical security that pose the threat of unauthorized access to New Era confidential information.

Note: Incidents involving the receipt of spam or 'phishing' emails are also recognized as posing a threat to information security.

A data breach is an incident that results in the confirmed disclosure, not just potential exposure, of data to an unauthorized party.

Note: A personal *data breach* can be broadly defined as a security *incident* that has affected the confidentiality, integrity or availability of personal data.

In the event of an actual or suspected information security incident or breach, New Era must take swift and decisive action to mitigate risks, protect individuals, and minimize operational, financial, legal, and reputational impact. Delayed or unreported incidents can lead to serious consequences, including:

- Significant damage or disruption to corporate systems and services.
- Harm or distress to affected individuals.
- Regulatory penalties, including substantial fines for data protection breaches.
- Reputational damage and loss of stakeholder trust.
- Loss of business assets and intellectual property.
- Increased exposure to fraud or identity theft.

Enterprise IT and Security Operations (in collaboration with CTO Office)

Roles and Responsibilities

The Enterprise IT team, under the CIO function, is accountable for all information security incident response activities. Security Operations, as a branch of Enterprise IT, leads technical investigation, containment, and recovery efforts.

A designated Incident Response Lead within Enterprise IT will:

- Coordinate incident response activities across Enterprise IT, Security Operations, and the CTO Office.
- Ensure compliance with ISO 27001 Annex A.5.25 and A.5.26 and NIST CSF Respond/Recover functions.
- Report incidents to executive leadership, cyber insurance providers (if applicable), and regulatory authorities as required.

The CTO Office provides:

- Helpdesk and triage support for initial incident intake and escalation.
- Assistance in communication and operational continuity during incidents.

Incident Response Plan (IRP)

The IRP must:

- Define the full lifecycle: detection, analysis, containment, eradication, recovery, and post-incident review.
- Include escalation criteria, severity classification, and authority for decision-making.
- Be tested annually with participation from Enterprise IT, Security Operations, and CTO Office.

Incident Reporting and Escalation

Reporting mechanisms must:

- Be accessible to all personnel and allow immediate escalation.
- Include automated monitoring and alerting for suspicious activities.

All incidents must:

- Be logged in a centralised incident repository.
- Be assessed for severity and impact by Enterprise IT and Security Operations.
- Trigger appropriate response procedures promptly.

Notification and Communication

Communication protocols must:

- Follow pre-approved templates for internal and external notifications.
- Ensure compliance with regulatory timelines (e.g., GDPR breach reporting).
- Assign a designated spokesperson for media and public statements.

Interaction with law enforcement and regulators:

- Must be coordinated by the Incident Response Lead and Legal.
- Maintain confidentiality and integrity of evidence.

Post-Incident Review

After resolution:

- Conduct a root cause analysis and review with the applicable parties.
- Update risk assessments and controls based on findings.
- Enter improvements into the Enterprise IT project pipeline for continual improvement.

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 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	Incident Response Policy
Purpose	The purpose of the New Era Technology Incident Response Policy is to describe the requirements for dealing with information security incidents.
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 2-6	Dir GRC, SVP Corp A&E
V3.0	Oct 2024	Approved release	CTO, Dir GRC
V4.0	Jan 2026	Annual review, 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	Acceptable Use Policy	Policy to establish acceptable practices regarding the use of New Era Technology Information Resources to protect the confidentiality, integrity, and availability of information created, collected, and maintained. Inappropriate use exposes New Era to risks, including virus attacks, loss of confidential data, compromise of network systems and services, and legal issues.
New Era GRC Document	Incident Response Plan	Document describing New Era Technology's security Incident Response (IR) plan to respond to physical and electronic information security incidents.
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.