New Era Technology, Inc. Incident Response Policy

Classification: Public

Incident Response Statement

New Era Technology, Inc., and its subsidiaries (collectively the "Company" or "New Era") is committed to upholding the requirements for dealing with information security incidents.

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
"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, Inc., 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 to 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) 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.

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 objective of this Policy is to ensure a consistent and effective approach to New Era Technology's management of information security incidents, including communication on security events and weaknesses.

Events and incidents are not mutually exclusive; all incidents are events, but not all events are incidents.

An information security event is any occurrence related to assets or the environment indicating a *possible* compromise of policies or failure of controls, or an unmapped situation that can impact security.

An Information security incident is a security event that compromises the integrity, confidentiality, 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.

If there is an actual (or suspected) information security incident or breach, it is essential that New Era takes prompt action to mitigate the risks of potential harm to individuals, damage to operational business, and financial, legal and reputational costs. Where information security incidents are not reported, or where reports are delayed, the consequences can be severe and include:

- Damage or disruption to corporate systems.
- Damage and distress to individuals.
- Monetary penalties from regulators (including very significant fines for breaches of data protection).
- Harm to New Era's reputation and subsequent erosion of trust.
- Loss of business assets.
- Increased risk of fraud or identity theft.

Incident Response Team (IRT)

- An Incident Response Team (IRT) will be established; consisting of legal experts, risk managers, and other department managers that should be involved in decisions related to incident response.
- The IRT is responsible for:
  - Ensuring that incident response activities are carried out in accordance with legal, contractual, and regulatory requirements.
  - Internal and external communications pertaining to information security incidents.
  - Ensuring that personnel are trained on how to report a potential incident.
- The IRT will respond to identified cyber security incidents following the Incident Response Plan.

Incident Response Lead

- An Incident Response Lead will be appointed to manage New Era Technology incident response activities.
- The Incident Response Lead will assemble and oversee the Incident Response Team (IRT).
- The Incident Response Lead is responsible for appropriately reporting incidents to New Era Technology's Cyber Insurance Provider (when applicable), to applicable executives and to the IRT.

Incident Response Plan (IRP)

- The Incident Response Lead is responsible for overseeing the creation, implementation, and maintenance of an Incident Response Plan (IRP).
- The Incident Response Plan must be tested by the IRT no less than annually.

Incident Reporting

- Management must provide a means for all personnel to report potential incidents. Reporting methods must ensure that a potential incident is promptly escalated to the appropriate person(s).
- IT is responsible for monitoring event logging, vulnerability management, and other logs for suspicious activities.

- All reported incidents must be assessed by a member of the IRT to determine the threat type and activate the appropriate response procedures. All members of the IRT must be familiar with how to assess and escalate a potential incident.
- The Incident Response Lead must report the incident to executive leadership.
- Managers / Senior leadership must report any potential breaches and/or incidents involving customer data to the Incident Response Team (IRT) promptly.

Notification and Communication

- The IRT is responsible for ensuring that notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements take place in a timely manner.
- All Information concerning an incident is considered confidential, and at no time should any information be discussed with anyone outside of New Era Technology without approval of executive management.
- Personnel
  - Personnel must be notified whenever an incident or incident response activities may impact their work activities.
  - Internal communications must aim to avoid panic, avoid the spread of misinformation, and notify personnel of appropriate communication channels.
- Interaction with Law Enforcement
  - Interaction between law enforcement and emergency services personnel must be coordinated by the Incident Response Lead or a member of the IRT.
  - Legal must be consulted in communications with law enforcement.
- Customers and Partners
  - All customers and partners who are affected by the incident must be notified according to applicable contract language, service level agreements (SLAs), applicable statutes and/or regulations.
  - Communications with customers and partners must be consistent, with the same or similar message delivered to each.
- Regulatory Authorities
  - Only members of the IRT are permitted to discuss the nature and/or details of an incident with any regulatory agencies.
  - The IRT must contact regulators as required or as soon as practical
- Public Media
  - The IRT or executive management will assign a designated spokesperson responsible for communication with the media.
  - Inquiries from media agencies must be directed to the designated spokesperson and the IRT.

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	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 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	Oct 2, 2024	Annual review, updates to sections 2-6	Dir GRC, SVP Corp A&E
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	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 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.