Vulnerability Management Policy

Classification: Public

Vulnerability Management Policy Statement

New Era Technology ("New Era" or "the Company") is committed to implementing the necessary requirements to ensure that vulnerability management and remediation processes protect Company information assets, maintain system integrity, and comply with applicable Company policies and procedures.

This Policy applies to all individuals responsible for supporting, managing, or executing vulnerability management and remediation 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 timely identification, prioritisation, and remediation of vulnerabilities.

New Era will implement and maintain controls to ensure that:

- Approved methods and processes are used for vulnerability identification, assessment, and remediation.
- Critical systems and data are protected against exploitation and maintained in a secure state to minimise risk and prevent unauthorised access.
- Vulnerability management activities comply with legal, regulatory, and Company requirements, including regular monitoring, reporting, and validation of remediation actions.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“compensating controls”	Compensating controls are alternative security measures implemented to reduce risk when the primary control (such as applying a patch) is not immediately feasible. These controls provide equivalent or enhanced protection and may include actions such as disabling vulnerable services, applying network segmentation, increasing monitoring, or implementing strict access restrictions until the primary control can be applied.
“data”	are items of information.
“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.
“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.
“vulnerability”	A vulnerability is a weakness or flaw in a system, application, process, or control that could be exploited by a threat actor or result in unauthorized access, data compromise, or disruption of services. Vulnerabilities may arise from software defects, misconfigurations, inadequate security controls, or human error.
“we”, “our”, “New Era”, or “New Era Technology”	refers to New Era Technology and its subsidiaries.

2. Scope

The New Era Technology Vulnerability Management Policy applies to individuals who are involved in the configuration, maintenance, or expansion of the New Era Technology network infrastructure.

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 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 network management standards.

If any additional network 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 access management policies. The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

Asset Inventory

To maintain visibility and accountability, all assets must be accurately recorded and managed throughout their lifecycle. Refer to New Era Technology's **Asset Management Policy** for detailed requirements.

1. Maintain a comprehensive inventory of all assets, including software vendor, product name, version, deployment state, classification (criticality and sensitivity), and responsible owner.
2. Include physical, virtual, and cloud-based assets in the inventory.
3. Update inventory regularly and verify accuracy during audits and management reviews.

Vulnerability Identification

Proactive identification of vulnerabilities is essential to reduce risk exposure and maintain system integrity.

1. Monitor trusted sources (vendor advisories, vulnerability databases, threat intelligence feeds) and validate their authenticity.
2. Conduct automated vulnerability scans at defined intervals (e.g., monthly internal, quarterly external) and after significant changes.
3. Perform regular penetration tests of the internal and external networks.
4. Correct exploitable vulnerabilities found during scans and re-test to confirm remediation.
5. Track vulnerabilities in third-party libraries and source code.
6. Require suppliers to report vulnerabilities and include this obligation in contracts.
7. Establish secure channels for internal and external vulnerability reporting and define response timelines.

Vulnerability Evaluation

Effective evaluation ensures prioritization of remediation efforts based on risk and business impact.

1. Analyze and validate vulnerability reports using a formal risk scoring methodology (e.g., severity, exploitability, impact).
2. Assess risk based on technical severity and business impact.
3. Document findings, decisions, and risk acceptance in the vulnerability management system for traceability.

Remediation and Mitigation

Timely remediation and mitigation measures safeguard critical systems and maintain operational resilience.

1. Implement a formal patch and update management program with defined processes.
2. Test and document all changes before deployment, including rollback plans.

3. Prioritize remediation for high-risk systems and maintain audit trails.
4. Use only legitimate sources for updates and validate integrity of update packages.
5. When patches are unavailable, implement compensating controls to reduce risk exposure. Examples include workarounds, disabling vulnerable services, applying network segmentation, and enhancing monitoring. Effective compensating controls may also be used to deprioritize those vulnerabilities, allowing remediation efforts to focus on higher-risk vulnerabilities without compensating measures.
6. Communicate critical vulnerabilities promptly to relevant stakeholders.

Monitoring and Reporting

Comprehensive monitoring and reporting to provide traceability and support continuous improvement.

1. Capture vulnerability management activities, including identification, evaluation, and remediation steps.
2. Ensure Operations teams managing vulnerabilities have access to reports.
3. Store vulnerability reports with integrity controls (e.g., hashing, version control).

Integration with Incident Management

Coordinated response ensures vulnerabilities are addressed as part of broader security incident handling. Refer to New Era Technology's **Incident Response Policy** for detailed requirements.

1. Align vulnerability management with incident response procedures.
2. Define escalation paths for vulnerabilities that could lead to incidents.
3. Share vulnerability data with the incident response team for coordinated action and joint post-incident reviews.

Cloud Services

Cloud service providers must meet contractual obligations for vulnerability management and demonstrate compliance. Refer to New Era Technology's **Cloud Computing and Vendor Management Supplier Security** policies for detailed requirements.

1. Ensure cloud service providers manage vulnerabilities in their resources as per contractual obligations.
2. Include right-to-audit provisions and require evidence of compliance through independent assessments.
3. Review provider compliance reports regularly and validate remediation timelines.

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	Vulnerability Management Policy
Purpose	The purpose of this document is to establish a structured approach to identify, evaluate, and remediate technical vulnerabilities in information systems to prevent exploitation and maintain security for New Era.
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	Jan 2026	Approved release	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 Policy	Change Management/Control Policy	Policy establishing the rules for the creation, evaluation, implementation, and tracking of changes made to New Era Technology Information Resources.
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.
New Era GRC Policy	Encryption Policy	Policy establishing rules for acceptable use of encryption technologies relating to New Era Technology Information Resources.
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.