Acceptable Use Policy

Classification: Public

Acceptable Use Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to protecting the confidentiality, integrity, and availability of all information created, collected, and maintained by the Company. This Policy establishes standards for the responsible and secure use of New Era Technology's information resources to ensure compliance with applicable laws and Company policies.

This Policy applies to all individuals who access or utilise Company information resources, including:

- Permanent, temporary, and contracted employees
- Executives, officers, and directors
- Contractors and third parties
- External parties such as customers, partners, and suppliers

All users are expected to act responsibly and in accordance with established procedures to safeguard Company information assets.

New Era will implement and maintain controls to ensure that:

- Information resources are used only for authorised business purposes.
- Access is granted based on role and monitored for compliance.
- Prohibited activities (e.g., unauthorised sharing, misuse, or illegal actions) are clearly defined and enforced.
- Periodic reviews validate adherence to acceptable use standards.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
"AI"	Artificial Intelligence (AI) applies advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions.
"AUP"	means Acceptable Use Policy
"BYOD"	means Bring Your Own Device; pertains to non-corporate issued devices, i.e., smart phones, tablets, laptops workstations/desktops.
"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.
"MAM"	refers to the set of technologies, policies, and processes used to secure, manage, and control access to business applications and their data on mobile devices, regardless of whether the device is company-owned or personally owned (BYOD).
"MDM"	means Mobile Device Management of corporate and non-corporate devices.
"mobile device"	means a smart phone, tablet, laptop, etc.
"staff", "users", "personnel"	means those who are employed by New Era Technology on a full-time, 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 (which may include customers, partners and suppliers).
"we", "our", "New Era", or "New Era Technology"	refers to New Era Technology and its subsidiaries.

2. Scope

This Policy outlines acceptable use for New Era Technology information resources including, but not limited to, computers, internet, email, and personal mobile devices (registered under New Era Technology's "Mobile Devices and BYOD (Bring Your Own Device) Security Policy").

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 Acceptable Use Policy (AUP) 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 AUP 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 AUP standards.

If any additional acceptable use 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

This Acceptable Use Policy (AUP) sets out acceptable behaviours and responsibilities to protect company assets, data, and reputation.

Key Do's and Don'ts

DO

- Comply with all New Era Technology policies and applicable laws.
- Lock your screen when leaving your workstation; enable auto-lock.
- Secure sensitive documents (lock away or encrypt) when not in use.
- Report incidents immediately (data loss, unauthorised access, policy violations) to GRC, your manager, or IT Helpdesk.
- Use approved software and tools only – get IT approval before installing anything.
- Use strong passwords and enable Multi-Factor Authentication (MFA).
- Encrypt confidential data when transmitting over public networks.
- Complete security training within 30 days of hire and annually.
- Follow BYOD rules – ensure MDM/MAM is installed and security controls are active.
- Be transparent with AI use – verify facts, avoid bias, and comply with data privacy laws.
- Dispose of confidential documents securely (cross-cut shredding or approved vendor).
- Escort visitors in secure areas and badge in/out properly.

DON'T

- Share passwords, tokens, or access cards with anyone.
- Install unapproved software or change system configurations.
- Disable security features on company or BYOD devices.
- Store company data on personal accounts or devices without MDM/MAM.
- Use Company resources for personal financial gain or illegal activities.
- Input confidential or regulated data into unapproved AI tools.
- Access or transmit offensive, indecent, or obscene material.
- Auto-forward emails outside company systems or use personal email for work.
- Use VPNs to bypass sanctions restrictions or conceal location.
- Leave sensitive documents or devices unattended in the office or remote workspace.
- Publish confidential information on social media or misrepresent your role.
- Connect unknown removable media without IT approval.

General Responsibilities

- Comply with all New Era Technology policies and applicable laws.
- Seek clarification from the Director of Governance, Risk and Compliance (GRC) if requirements are unclear.
- Report harmful events or policy violations immediately to Governance, Risk and Compliance (GRC), a manager, or the IT Helpdesk.

Incident Reporting

Report any suspected or confirmed incidents promptly to the IT Helpdesk, a manager, or GRC, including:

- Technology Incident: Failure, interruption, or loss of availability of Information Resources.
- Data Incident: Loss, theft, or compromise of company information.
- Unauthorised Access: Any attempt or actual unauthorised access to systems or data.
- Facility Security Incident: Damage or unauthorised access to company premises.
- Policy Violation: Breach of any New Era Technology policy, standard, or procedure.

Prohibited Activities

Personnel must not:

- Harass, threaten, impersonate, or abuse others.
- Degrade system performance or deny authorised access.
- Circumvent security measures or exploit vulnerabilities.
- Install unapproved software or change system configurations.
- Run unauthorised security tools (e.g., password crackers, port scanners).
- Access, create, store, or transmit offensive, indecent, or obscene material.
- Use Company resources for personal financial gain or illegal activities.

Software and System Changes

- Do not install or use software unless approved by the CIO or delegate.
- Do not alter operating system configurations or install new operating systems without prior approval.
- Contact IT Helpdesk for clarification or to initiate requests.

Intellectual Property

- All inventions, intellectual property, and proprietary information created on company time or using Company resources belong to New Era Technology.
- Respect all legal protections for patents, copyrights, trademarks, and IP rights.

Monitoring and Privacy

- Information created, sent, received, or stored on Company systems is not private.
- New Era Technology may monitor, log, and review all usage for compliance and security purposes.

Artificial Intelligence (AI) Acceptable Use

- Authorised Use: Generative AI tools may only be used for approved business purposes.
- Approval: AI platforms and integrations require review and approval by the CIO or delegate.
- Security: Apply secure configurations, updates, and vulnerability testing.
- Data Privacy: Do not input sensitive or confidential data into unapproved AI tools.
- Responsible Use: Verify facts, avoid bias, and ensure outputs align with company values.
- Incident Reporting: Report AI-related security incidents promptly.

Sanctions Compliance

This Sanctions Compliance Acceptable Use policy supplements New Era's Acceptable Use policy.

- Do not use company systems to violate sanctions laws.
- Accessing company systems from sanctioned countries is prohibited without written HR approval.
- VPN use to bypass sanctions restrictions is strictly forbidden.
- Violations may result in suspension, investigation, termination, and legal action.

Sanction Compliance Statement

New Era Technology is committed to conducting business ethically and in compliance with sanctions established and implemented by international governing bodies such as the United Nations' UN Security Council (UNSC), and those in the regions in which we operate, for example:

- US - Office of Foreign Assets Control (OFAC)
- UK – Foreign, Commonwealth & development Office (FCDO) and Office of Financial Sanctions Implementation (OFSI)
- EU – Sanctions Map
- Australia - Department of Foreign Affairs and Trade (DFAT)

Access Control and Authentication

- Access is granted on a "need-to-know" basis.
- Use only authorised credentials; do not share passwords or authentication tokens.
- MFA is mandatory for remote access.
- Report lost or stolen access cards or tokens immediately.

Refer to New Era Technology's **Identity & Access Management (IAM) Policy** for detailed requirements.

Clear Desk and Clear Screen

- Lock workstations when unattended; enable automatic screen lock.
- Secure sensitive documents and devices when not in use.
- Shred confidential documents using approved methods.
- Apply the same security practices when working remotely.

Refer to New Era Technology's **Clear Desk & Clear Screen Policy** for detailed requirements.

Data Security

- Use approved encrypted communication for confidential data.
- Do not use unapproved cloud services.
- Dispose of electronic media securely.
- Avoid discussing confidential information in public spaces.

Refer to New Era Technology's **Encryption, Cloud Computing, Media Sanitization & Destruction and Remote Worker Security policies** for detailed requirements.

Email and Electronic Communication

- Do not auto-forward emails outside Company systems.
- Do not use personal email accounts for Company business.
- Exercise caution with links and attachments.
- Use discretion in Out of Office messages; avoid sensitive details.

Internet Usage

- Internet use must be business-related.
- Prohibited activities include gaming, streaming media, personal social media, and accessing inappropriate content.

Mobile Devices and BYOD (Bring Your Own Device)

- BYOD is allowed only with formal IT approval.
- Devices must comply with MDM (Mobile Device Management)/MAM (Mobile Application Management) security controls.
- Report lost or stolen devices within 24 hours.
- Do not root/jailbreak devices or disable security features.
- Company data must not be stored on personal accounts or devices without MDM and/or MAM.

Refer to New Era Technology's **Mobile Devices and BYOD (Bring Your Own Device) Policy** and **Mobile Device Management (MDM) and Mobile Application Management (MAM) Policy** for detailed requirements.

Physical Security

- No recording devices in secure areas.
- Badge in/out of access-controlled areas; no tailgating.
- Visitors must be escorted at all times.

Removable Media

- Use only with IT approval and encryption.
- Personally owned removable media is prohibited.
- Report loss or theft immediately.

Security Training and Awareness

- Complete security awareness training within 30 days of hire and annually thereafter.
- Acknowledge receipt and compliance with all security policies

Refer to New Era Technology's **Security Awareness & Training Policy** for detailed requirements.

Social Media

- Do not misrepresent your role or disclose confidential information.
- Include disclaimers when posting in a personal capacity.
- Obtain approval before creating accounts representing New Era Technology.

Voicemail

- Do not disclose confidential information in voicemail greetings or messages.
- Do not access another user's voicemail without written authorisation.

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	Acceptable Use Policy
Purpose	The purpose of this policy is 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.
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	Aug 2022	Approved release	CTO, Dir GRC
V1.1	Oct 2022	Revised BYOD section	CTO, Dir GRC
V2.0	Sep 2023	Annual review, approvers update	CTO, Dir GRC
V3.0	Oct 2024	Annual review, updates to sections 2-6, AI AUP inclusion, BYOD updates	CTO, Dir GRC, SVP Corp A&E
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	Mobile Devices and BYOD (Bring Your Own Device) Policy	Policy describing the conditions under which New Era Technology personnel may use corporate owned/provided mobile devices as well as their own personal mobile devices for business purposes. This policy covers mobile phones, tablets, and laptops.
New Era GRC Policy	Mobile Device Management (MDM) and Mobile Application Management (MAM) Policy	Policy describing guidelines and procedures for the secure and responsible use of mobile devices and business applications within New Era.
New Era GRC Policy	Clear Desk and Clear Screen Policy	Policy to reduce the risks of unauthorized access, loss of, and damage to information on desks, screens, and in other locations during and outside regular working hours.
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 Use Policy	Policy establishing rules for acceptable use of encryption technologies relating to New Era Technology Information Resources.
New Era GRC Policy	Identity and Access Management (IAM) Policy	Policy establishing the requirements necessary to ensure that access to and use of New Era Technology Information Resources is managed in accordance with business requirements, information security requirements, and other New Era Technology policies and procedures.
New Era GRC Policy	Remote Access Policy	Policy defining the rules and requirements for connecting to New Era Technology's networks from any host (cell phones, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damage that may result from unauthorized use of company resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

New Era GRC Policy	Remote Worker Security Policy	Policy establishing the rules and conditions under which short and long-term remote working may occur in order to maintain acceptable practices regarding the use and protection of 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.