New Era Technology, Inc. Acceptable Use Policy

Classification: Public

Acceptable Use Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to protecting the confidentiality, integrity, and availability of information created, collected, and maintained.

We expect this policy to be upheld by all personnel- employees (permanent, temporary, or contracted; including executives, officers, and directors of New Era), contractors, third parties and external parties (including, but not limited to customers, partners, and suppliers) who access and/or utilize New Era Technology’s information resources.

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.
"Generative AI", "Gen AI"	Generative AI (Gen AI) refers to AI techniques that learn a representation of artifacts from data, and use it to generate brand-new, unique artifacts that resemble but don't repeat the original data. These artifacts can serve benign or nefarious purposes. Generative AI can produce totally novel content (including text, images, video, audio, structures), computer code, synthetic data, workflows and models of physical objects. Generative AI also can be used in art, drug discovery or material design
"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.
"Large Language Module", "LLM"	A large language model (LLM) is a specialized type of artificial intelligence (AI) that has been trained on vast amounts of text to understand existing content and generate original content.
"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, Inc., 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 the 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 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) 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

Acceptable Use

1. Personnel are responsible for complying with New Era Technology policies when using New Era Technology Information Resources and/or on New Era Technology time. If requirements or responsibilities are unclear, please seek assistance from the Director, GRC.
2. Personnel, as representatives of New Era, are responsible for complying with this Policy whilst involved in any customer or supplier engagements when using New Era Technology, customer and / or supplier Information Resources and /or on New Era Technology, customer and /or supplier time.
3. Personnel must promptly report harmful events or policy violations involving New Era Technology assets or information to the Director of Governance, Risk and Compliance, to their manager, or to a member of the New Era IT Technology team. Events include, but are not limited to, the following:
    a. **Technology incident**: any potentially harmful event that may cause a failure, interruption, or loss in availability to New Era Technology Information Resources.
    b. **Data incident**: any potential loss, theft, or compromise of New Era Technology information.
    c. **Unauthorized access incident**: any potential unauthorized access to a New Era Technology Information Resource.
    d. **Facility security incident:** any damage or potential unauthorized access to a New Era Technology-owned, leased, or managed facility.
    e. **Policy violation**: any potential violation of this or other New Era Technology policies, standards, or procedures.
4. Personnel must not purposely engage in activities that may:
    a. harass, threaten, impersonate, or abuse others,
    b. degrade the performance of New Era Technology Information Resources,
    c. deprive authorized New Era Technology personnel access to a New Era Technology Information Resource,
    d. obtain additional resources beyond those allocated, or
    e. circumvent New Era Technology computer security measures.
5. Personnel must not download, install, or make use of any software (including without limitation software, freeware, trial software, or commercial software or any software that is owned or supplied by an employee or third party to New Era Technology's computer systems or devices) unless it has been approved, in advance, by New Era Technology's Chief Technology Officer, or delegate, unless this activity is part of the personnel's regularly assigned New Era Technology job duties. Contact the IT Helpdesk for any clarification.
6. Personnel must not change the operating system configurations or install new operating systems on any New Era Technology computer systems or other IT assets. If any of those changes are necessary,

personnel must obtain prior approval from the New Era Technology's Chief Technology Officer or delegate before making any of those changes. Contact the IT Helpdesk to initiate requests.

7. Personnel must not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, New Era Technology personnel must not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any New Era Technology Information Resource unless this activity is part of personnel regularly assigned New Era Technology job duties.
8. All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on New Era Technology time and/or using New Era Technology Information Resources are the property of New Era Technology.
9. New Era Technology Information Resources are provided to facilitate company business and must not be used for personal financial gain.
10. Personnel are expected to cooperate with incident investigations and any regulatory bodies' investigations.
11. Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using New Era Technology Information Resources.
12. Personnel must not intentionally access, create, store or transmit material that New Era Technology may deem to be offensive, indecent, or obscene.

Artificial Intelligence (AI) Acceptable Use

This AI Acceptable Use policy supplements New Era's Acceptable Use policy above,

1. **Authorized Use**: Generative AI tools and platforms may only be used for business purposes approved by the organization. Such purposes may include content generation for marketing, product development, research, or other legitimate activities.
    a. AI and LLM platform usage and/or integration into existing tools will require review and approval by the New Era Technology's Chief Technology Officer, or delegate.
    b. All vendors must be reviewed in accordance with the New Era Vendor Management Supplier Security Policy and an impact analysis must be completed before New Era Technology's Chief Technology Officer, or delegate will consider usage.
    c. Generative AI tools and platforms must be configured securely, following industry best practices and vendor recommendations. This includes ensuring the latest updates, patches, and security fixes are applied in a timely manner.

i. Regular vulnerability assessments and security testing must be conducted on generative AI tools and platforms to identify and address any security weaknesses or vulnerabilities.

d. Appropriate logging and auditing mechanisms must be implemented to capture activities related to generative AI usage. These logs must be regularly reviewed to detect and respond to any suspicious or unauthorized activities.

2. **Authorized Access**: Access to generative AI tools, platforms, or related systems may be restricted to authorized personnel only. Users must not share their access credentials or allow unauthorized individuals to use the generative AI tools on their behalf.
    a. Strong authentication mechanisms, such as multi-factor authentication (MFA), must be implemented for accessing generative AI tools and platforms. Passwords used for access must be unique, complex, and changed regularly.
3. **Compliance with Laws and Regulations & Data Privacy**: All users of generative AI must comply with applicable laws, regulations, and ethical guidelines governing intellectual property, privacy, data protection, and other relevant areas.
    a. Users must handle any personal, sensitive, or confidential data generated or used by generative AI tools in accordance with all relevant laws, regulations, and industry standards, such as data protection and privacy regulations (e.g., GDPR, PIPEDA, CCPA) and financial industry guidelines (e.g., PCI DSS).
    b. Encryption and secure transmission must be employed.
    c. Inputting sensitive, or confidential organization data into unapproved AI application/system/tools is prohibited.
    d. A DLP (Data Loss Protection) solution must be implemented and used to stop data leaks from AI.
4. **AI Usage Incident Reporting**: Any suspected or confirmed security incidents related to generative AI usage should be reported promptly to the Director of Governance, Risk and Compliance, to their manager, or to a member of the New Era IT Technology team (as defined under section 4 – Acceptable Use).
5. **Intellectual Property Rights:** Users must respect and protect intellectual property rights, both internally and externally. Unauthorized use of copyrighted material or creation of content that infringes on the intellectual property of others is strictly prohibited.

Responsible AI Usage

Users are responsible for ensuring that the generated content produced using generative AI aligns with New Era's values, ethics, and quality standards. Generated content must not be used if it is misleading, harmful, offensive, or discriminatory.

Personnel who are using approved AI software/applications must use AI responsibly every time:

- **Evaluate** the initial output to see if it meets the intended purpose and your needs and continues to comply with applicable laws, regulations, and ethical guidelines governing intellectual property, privacy, data protection, and other relevant areas.
- **Verify** facts, figures, quotes, and data using reliable sources to ensure there are no hallucinations or bias.
- **Edit** your prompt and ask follow-up questions to have the AI improve its output.
- **Revise** the results to reflect your unique needs, style, and/or tone. AI is a great starting point but should not be a final product.
- **You** are responsible for everything you create with AI. Always be transparent about how you have used these tools.

Access Control

1. Access to information is based on a "need to know".
2. Personnel are permitted to use only those network and host addresses issued to them by New Era Technology IT and must not attempt to access any data or programs contained on New Era Technology systems for which they do not have authorization or explicit written consent.
3. All remote access connections to internal New Era Technology networks and/or environments must be made through approved remote access methods (i.e., virtual private networks (VPNs). Please contact New Era IT for guidance or assistance.
4. Personnel must not divulge access information to anyone not expressly authorized to receive such information, including IT support personnel.
5. Personnel must not share their personal authentication information, including:
    a. Account passwords,
    b. Personal Identification Numbers (PINs),
    c. Security Tokens (i.e., Smartcard),
    d. Multi-factor authentication information
    e. Access cards and/or keys,
    f. Digital certificates,
    g. Similar information or devices used for identification and authentication purposes.
6. Access cards and/or keys that are no longer required must be returned to local office IT designates or office managers for deactivation in the applicable system(s).
7. Lost or stolen access cards, security tokens, and/or keys must be reported to local office IT designates or office managers as soon as possible for deactivation in the applicable system(s).

Authentication / Passwords

1. All Personnel are required to maintain the confidentiality of authentication information.
2. Any group/shared authentication information must be maintained solely among the authorized members of the group.
3. All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following New Era Technology authentication guidelines (per the Identity and Access Management Policy):
    a. Must meet all requirements, including minimum length, complexity, and reuse history.
    b. Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
    c. Must not be the same passwords used for non-business purposes.
4. Unique passwords must be used for each system where shared accounts are utilized.
5. User account passwords must not be divulged to anyone. New Era Technology support personnel must never ask for user account passwords.
6. If the security of a password is in doubt, compromised or discovered, the password must be immediately changed, and the security incident reported to New Era Technology IT support.
7. Security tokens (i.e., Smartcard) must be returned on demand or upon termination of the relationship with New Era Technology if issued.
8. Where other authentication mechanisms other than passwords are used (i.e., security tokens, smart cards, certificates, etc.), the authentication mechanism must be assigned to an individual, and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.

Clear Desk and Clear Screen

1. All computer workstations and laptops, regardless of data classification, must be locked or logged out when the workspace or laptop is unoccupied, requiring at least a username and password to unlock.
2. Users are required to ensure that all information classified as internal or confidential in hardcopy or electronic form is secure in their work area before leaving for the day by ensuring documents or devices are physically locked away or encrypted.
3. Any hardcopy information classified as internal or confidential must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
4. File cabinets and other containers storing hardcopy documents containing information classified as internal or confidential must be kept closed and locked when not in use or when not attended.
5. Keys used for access to containers storing hardcopy documents containing information classified as internal or confidential must not be left accessible at an unattended desk.

6. Offices or suites with information classified as internal or confidential must be locked when the space is unoccupied if the information is not otherwise secure.
7. Unattended mobile devices and laptops containing or accessing information classified as internal or confidential must be appropriately protected (by physically locking them (i.e., locking cable) or locking them away (i.e., in a drawer/cabinet) unless they are encrypted with whole disk or equivalent encryption.
8. Passwords may not be written down and left in any accessible location, such as on a sticky note near a computer workstation or in password notebooks.
9. Printouts containing information classified as internal or confidential must be removed from printers promptly.
10. Upon disposal, hardcopy documents containing information classified as internal or confidential must be shredded utilizing shredders with crosscut or confetti-cut cutting patterns or shredded by a third party that provides certificates of destruction. If documents are being utilized in a work-from-home environment, documents need to be kept secure per this policy until it is feasible to return the documents to a New Era Technology office for proper disposal.
11. Whiteboards containing information classified as internal or confidential must be erased before leaving the work area.

Data Security

1. Personnel must use approved encrypted communication methods whenever sending confidential information over public computer networks (Internet). Please contact IT for guidance or assistance.
2. Confidential information transmitted via a mail service must be secured in compliance with the Data Classification and Management Policy.
3. Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
4. Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity (classification) per the Data Classification and Management Policy.
5. Personnel are strongly advised not to engage in confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
6. Confidential information must be transported either by a New Era Technology employee or a courier approved by IT Management.
7. All electronic media containing confidential information must be securely disposed of. Please contact IT for guidance or assistance.

Email and Electronic Communication

1. Auto-forwarding electronic messages outside the New Era Technology internal systems is prohibited.

2. Electronic communications must not misrepresent the originator or New Era Technology.
3. Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
4. Accounts must not be shared without prior authorization from New Era Technology IT, except for corporate email calendars and related calendaring functions.
5. Employees must not use personal email accounts to send or receive any New Era Technology information.
6. Any personal use of New Era Technology provided email must not:
    a. Involve solicitation.
    b. Be associated with any political entity.
    c. Have the potential to harm the reputation of New Era Technology.
    d. Forward chain emails.
    e. Contain or promote anti-social or unethical behavior.
    f. Violate any ordinances, including, but not limited to, primary legislation, local, state, provincial, federal, or international laws or regulations.
    g. Result in unauthorized disclosure of New Era Technology confidential information.
    h. Or otherwise violate any other New Era Technology policies.
7. Personnel must only send confidential information using approved secure electronic messaging solutions.
8. Personnel must use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
9. Personnel must use discretion in disclosing confidential or internal information in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information, or other sensitive data.

Internet

1. The Internet must not be used to communicate New Era Technology confidential or internal information unless the confidentiality and integrity of the information is ensured, and the identity of the recipient(s) is established.
2. Use of the Internet with New Era Technology networking or computing resources must only be used for business-related and manager-approved team-building activities. Unapproved activities include, but are not limited to:
    a. Recreational games,
    b. Streaming media,
    c. Personal social media,
    d. Accessing or distributing pornographic or sexually oriented materials,

e. Attempting or making unauthorized entry to any network or computer accessible from the Internet.
f. Or otherwise violate any other New Era Technology policies.

3. Access to the Internet from outside the New Era Technology network using a New Era Technology-owned computer must adhere to all the same policies that apply to use from within New Era Technology facilities.

Mobile Devices and BYOD (Bring Your Own Device)

This Policy should be read in conjunction with, and is not meant to replace, the New Era Technology Mobile Device Management (MDM) Policy located on the New Era Intranet.

Overview

- The use of a personally owned mobile device to connect to the New Era Technology network is a privilege granted to employees only upon formal approval of IT Management.
- New Era Technology confidential information must only be stored on compliant BYOD devices (see section *BYOD Requirements)*.
- Theft or loss of any device that has been used to create, store, or access confidential or internal information must be reported to a member of the New Era IT Technology team immediately.
- All mobile devices must adhere to the BYOD Security requirements in section *BYOD Security*.
- All mobile devices must meet the BYOD requirements in section *BYOD Requirements*.
- All personnel are expected to use mobile devices in an ethical manner.
- New Era Technology IT Management may use MDM security controls for mobile devices without warning to maintain the security and integrity of New Era Technology Information Resources.
- New Era Technology IT support for personally owned mobile devices is limited to assistance in complying with this policy. New Era Technology IT support may not assist in troubleshooting device itself or device usability issues.
- The use of personally owned devices must be in compliance with all other New Era Technology policies.
- New Era Technology reserves the right to revoke personally owned mobile device use privileges in the event that personnel do not abide by the requirements outlined in this policy.

BYOD Use

BYOD covers the use of a personal device for work purposes. This includes accessing the following corporate resources:

- New Era Technology email, calendars, address books/contacts, and
- New Era Technology business applications or cloud services used and approved by IT Management.

New Era Technology IT reserves the right to decline use for a BYOD device deemed a security risk. Approved BYOD devices will have MDM (mobile device management) installed on them – see the New Era Technology Mobile Device Management (MDM) Policy.

Messages, documents, and data originating from New Era Technology, transmitted or received on New Era Technology provisioned infrastructure are Company property.

Personnel are not authorized to save or transfer sensitive business data to their personal accounts or on personal devices without MDM.

Personnel must use a professional voice greeting on their voicemail or when answering a call on any device used for New Era Technology business, including any personal mobile device.
The New Era Technology IT department will configure the BYOD device and implement security controls as it deems necessary, at its discretion, to protect the integrity of New Era Technology Information Resources. This configuration can usually be completed remotely. Such security controls may include, but are not limited to:

- Encryption,
- Password protection,
- Remote wipe capability of those applications with access to New Era Technology Information Resources,
- Inactivity timer, and
- Data removal after multiple invalid password entries.

As per the corporate Mobile Device Management (MDM) Policy, New Era Technology reserves the right to use MDM in order to maintain security of New Era Technology data; or should the device be lost or stolen; or in the event that the employment relationship is terminated by the employee or by New Era Technology.

- BYOD devices must not be used for any illegal or unlawful purpose, including transmitting violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful material.
- BYOD devices must not be used to harass, intimidate, or otherwise annoy anyone.
- New Era Technology will not be held liable for damages related to inappropriate use of BYOD devices by any New Era Technology personnel or their families.

New Era Technology will not:

- Assume any financial responsibility for BYOD devices or technologies except as agreed with New Era Technology HR / Finance departments.
- Be held liable for damages related to inappropriate use of personal devices by employees, contractors, or their families.
- Be held responsible, in any way, for the contractual terms, physical device, MDM and/or any personal data stored on the device.
- New Era Technology will not reimburse personnel for the following expenses:

- BYOD initial cost, maintenance, or replacement.
- Connectivity charges, including Wi-Fi hotspot usage.
- Insurance.
- Expenses related to restoring BYOD if lost, corrupted (e.g., malware, incompatible applications, changes to the operating system), or damaged.

The employee must maintain a clear record of all documentation related to contracts, invoices, and monthly statements for the mobile device and services if they choose to use their plan and provider. These documents must be held for seven (7) years for financial audit purposes; otherwise, the employee may risk creating a tax issue if an audit occurs.

BYOD Security

- All devices that access New Era Technology email must have a PIN or other authentication mechanism enabled.
- BYOD devices must not be used for any illegal or unlawful purpose, including transmitting violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful material.
- BYOD devices must not be used to harass, intimidate, or otherwise annoy anyone.
- New Era Technology will not be held liable for damages related to inappropriate use of BYOD devices by any New Era Technology personnel or their families.
- Personnel must not:
  - "Root '' or "jailbreak" a BYOD to free it from pre-defined limitations. This process modifies the system files and can result in an unstable and insecure device.
  - Modify BYOD hardware and/or software beyond the installation of updates provided by the device maker or service provider.
  - Disable BYOD protection systems such as passwords, encryption, firewalls, et cetera without the approval of the New Era Technology IT department.

BYOD Requirements

Any device being used for BYOD must meet the following standards as a minimum:

- Latest updates are installed as soon as available.
- All personally owned laptops and/or workstations that connect to the New Era Technology network must have approved virus and spyware detection/protection software and active personal firewall protection.
- Ability to install and activate the mandatory New Era Technology MDM.

BYOD Changes

Personnel must inform New Era Technology IT if any of the following occurs:

- A new BYOD is acquired and needs access to New Era Information Resources.

- A BYOD is taken out of service and is no longer used.
- The user's role changes requiring a change in access (e.g., individual changes positions or goes on a leave of absence).

BYOD Support

New Era Technology IT will not support the device outside the approved office productivity applications.

It is the New Era Technology personnel's responsibility to ensure that they are familiar with the device they choose to use and obtain their own training resources in order to successfully use and maintain the device.

New Era Technology personnel must ensure that they can obtain support through their provider and have the relevant contact information available to them should an issue arise.

BYOD – Damaged, Lost or Stolen

Lost or stolen devices must be reported immediately (within 24 business hours) to the employee's manager and to a member of New Era Technology IT team; in addition, law enforcement may also need to be notified.

If the device is damaged, lost, or stolen, it will be the responsibility of New Era Technology personnel to obtain a replacement device. Failure to maintain a device will result in the cancellation of any previously approved reimbursement plan.

Physical Security

1. Photographic, video, audio, or other recording equipment, such as cameras and cameras in mobile devices, is not allowed in secure areas.
2. Personnel must badge in and out of access-controlled areas. Piggybacking, tailgating, door propping, and any other activity to circumvent door access controls are prohibited.
3. Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times.
4. Eating or drinking are not allowed in data centers. Caution must be used when eating or drinking near workstations or information processing facilities.

Privacy

1. Information created, sent, received, or stored on New Era Technology Information Resources is not private and may be accessed by New Era Technology IT employees at any time, under the direction of New Era Technology executive management and/or Human Resources, without knowledge of the user or resource owner.
2. New Era Technology has the right to monitor, log, and block any and all use of New Era Technology computer and data communication systems by New Era Technology personnel, for purposes

including, but not limited to, internet sites, social media, chat, and newsgroups visited, file downloads, and any or all communications sent and received

3. New Era Technology may log, review, and otherwise utilize any information stored on or passing through its Information Resources.
4. Systems Administrators, New Era Technology IT, and other authorized New Era Technology personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges must not access files and/or other information that is not specifically required to carry out an employment-related task.

Removable Media

1. The use of removable media for storage of New Era Technology information must be supported by a reasonable business case.
2. All removable media use must be approved by New Era Technology IT prior to use.
3. Personally owned removable media use is not permitted for storage of New Era Technology information.
4. Personnel are not permitted to connect removable media from an unknown origin without prior approval from New Era Technology IT.
5. Confidential and internal New Era Technology information must not be stored on removable media without the use of encryption.
6. All removable media must be stored in a safe and secure environment.
7. The loss or theft of a removable media device that may have contained any New Era Technology information must be reported to the New Era Technology IT team.

Security Training and Awareness

1. All new personnel must complete an approved security awareness training prior to, or at least within 30 days of, accessing any New Era Technology Information Resources.
2. All personnel, including third parties and contractors must be provided with, or have access to relevant information security policies to allow them to properly protect New Era Technology Information Resources.
3. All personnel must be provided with and acknowledge in writing that they have received and agree to adhere to the New Era Technology Security Policy and this Acceptable Use Policy, and any other New Era policies deemed applicable by the organization.
4. All personnel must complete annual security awareness training at least annually.

Social Media

1. Communications made with respect to social media must be made in compliance with all applicable New Era Technology policies.
2. Personnel are personally responsible for the content they publish online.
3. Creating any public social media account intended to represent New Era Technology, including accounts that could reasonably be assumed to be an official New Era Technology account, requires the permission of New Era Technology Executive Management in conjunction with the Marketing department.
4. When discussing New Era Technology or New Era Technology-related matters, you must:
    a. Identify yourself by name,
    b. Identify yourself as a New Era Technology representative, and
    c. Make it clear that you are speaking for yourself and not on behalf of New Era Technology unless you have been explicitly approved to do so.
5. Personnel must not misrepresent their role at New Era Technology.
6. When publishing New Era Technology-relevant content online in a personal capacity, a disclaimer must accompany the content. An example disclaimer could be: "The opinions and content are my own and do not necessarily represent New Era Technology's position or opinion."
7. Content posted online must not violate any applicable laws (i.e., copyright, fair use, financial disclosure, or privacy laws).
8. The use of discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, or marital status, or any other legally recognized protected basis under any ordinances, including, but not limited to: primary legislation, local, state, provincial, federal, or international laws or regulations; in published content that is affiliated with New Era Technology, will not be tolerated.
9. Confidential information, internal communications, and non-public financial or operational information may not be published online.
10. Personal information belonging to customers may not be published online.

Voicemail

1. Personnel must use discretion in disclosing confidential or internal information in voicemail greetings, such as employment data, internal telephone numbers, location information, or other sensitive data.
2. Personnel must not access another user's voicemail account unless it has been explicitly authorized in writing.
3. Personnel must not disclose confidential information in voicemail messages.

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	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 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 16, 2022	Approved release	CTO, Dir GRC
V1.1	Oct 31, 2022	Revised BYOD section	CTO, Dir GRC
V2.0	Sep 17, 2023	Annual review, approvers update	CTO, Dir GRC
V3.0	Oct 7, 2024	Annual review, updates to sections 2-6, AI AUP inclusion, BYOD updates	CTO, 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	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) Policy	Policy describing guidelines and procedures for the secure and responsible use of mobile devices 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 the 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 damages 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 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.