Identity & Access Management (IAM) Policy

Classification: Public

Identity & Access Management Policy Statement

New Era Technology and its subsidiaries (collectively the "Company" or "New Era") are committed to upholding 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.

This Policy applies to all individuals who access New Era Technology Information Resources, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All users are expected to adhere to the principles of least privilege, accountability, and secure access management, ensuring that access is granted only as necessary for the performance of assigned duties and is regularly reviewed and updated in line with organizational and regulatory requirements.

New Era will implement and maintain controls to ensure that:

- Access to information resources is authorized, documented, and regularly reviewed.
- User identities are uniquely assigned and managed throughout their lifecycle.
- Access rights are promptly adjusted or revoked upon role changes or termination.
- Authentication and authorization mechanisms are robust and aligned with industry best practices.
- All access activities are monitored and logged to support security, compliance, and audit requirements.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
"authentication"	refers to, but is not limited to passwords, PKI (public key infrastructure) certificates, biometric readings, ID cards.
"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 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.
"we", "our", "New Era", or "New Era Technology"	refers to New Era Technology and its subsidiaries.

2. Scope

This Policy applies to all New Era Technology's remote workers, permanent and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals who are responsible for managing New Era Technology Information Resource access, and those granted access privileges, including special access privileges, to any New Era Technology Information Resource.

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 access management 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 identity and access management standards.

If any additional access 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 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.

New Era Technology Information Technology (IT) is responsible for managing identity and access management activities for New Era Technology systems.

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

Access Control

1. Prior to access being provided to New Era Technology Information Resources and/or New Era Technology-affiliated resources, a legitimate business requirement must be justified.
2. New Era Technology Information Resources must have corresponding ownership responsibilities identified and documented.
3. Access to confidential information is based on a "need to know".
4. Access to Information Systems must be logged or recorded.
5. Access to the New Era Technology network must include a secure log-on procedure.
6. Workstations and laptops must force an automatic lock-out after a pre-determined period of inactivity.
7. Documented user access rights and privileges to Information Resources must be included in disaster recovery plans whenever such data is not included in backups.

Account Management

1. All personnel must acknowledge in writing they have received and agree to adhere to the New Era Technology Security Policy and Acceptable Use Policy, and any other New Era policies deemed applicable by the organization.
2. All accounts created must have an associated and documented request and approval.
3. Separation of duties must exist between access requests, access authorization, and access administration.
4. Information Resource owners are responsible for the approval of all access requests.
5. User accounts and access rights for all New Era Technology Information Resources must be reviewed and reconciled at least annually, and actions must be documented.
6. All accounts must be uniquely identifiable using the username assigned by New Era Technology IT and include verification that redundant user IDs are not used.
7. All accounts, where able, must integrate with New Era Technology Identity Providers (enforcing New Era authentication standards).
8. Only the level of access required to perform authorized tasks may be approved, following the concept of "least privilege".
9. Whenever possible, access to Information Resources should be granted to user groups/roles, not granted directly to individual accounts.
10. Shared accounts should not be used. Where shared accounts are required, their use must be documented and approved by the Information Resource owner and use compensating controls to ensure non-repudiation.

11. User account set up for third-party cloud computing applications used for sharing, storing, and/or transferring New Era Technology confidential or internal information must be approved by the resource owner and documented.
12. Access rights must be modified promptly upon user role changes to reflect the new role.
13. Creation of user accounts and access right modifications must be documented and logged.
14. Any accounts that have not been accessed within a predetermined period will be disabled.
15. According to the New Era Technology employee termination (offboarding) process, accounts must be disabled promptly following employment termination.
16. System Administrators or other designated personnel:
    a. Are responsible for modifying and/or removing the accounts of personnel whose role changes within New Era Technology or are separated from their relationship with it.
    b. Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
    c. Must have a documented process for periodically reviewing existing accounts for validity.
    d. Are subject to independent audit review.
    e. Must provide a list of accounts for the systems they administer when requested by authorized New Era Technology IT management personnel.
    f. Must cooperate with authorized New Era Technology Information Security personnel investigating security incidents at the direction of New Era Technology executive management.

Administrator/Special Access

1. Administrative/Special access accounts must have account management instructions, documentation, and authorization.
2. Administrative/Special access accounts must employ multi-factor authentication for all account logins.
3. Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
4. Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work performed (i.e., user account vs. administrator account).
5. Shared Administrative/Special access accounts should only be used when no other option exists.
6. The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department, or leaves New Era Technology altogether.
7. If a system has only one administrator, a password escrow procedure must be in place so that someone other than the administrator can gain access to the administrator account in an emergency.

8. Special access accounts for an internal or external audit, software development, software installation, or other defined need must be administered according to the New Era Technology authentication standards.

Authentication

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:
    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.
9. Passwords must be stored in the corporate IT-approved password management system.
10. All default passwords should be immediately updated, and unnecessary default accounts removed or disabled before installing a system on the network.
11. Administrators/Special Access users must not circumvent the New Era Technology authentication standards for the sake of ease of use.
12. Users must not circumvent password entry (i.e., use hardcoded passwords) in client software.
13. Computing devices must enable a password-protected screensaver.
14. New Era Technology IT Support must adhere to standard processes and procedures when facilitating password management.

Authentication Guidelines

Users are required to follow good security practices in the selection and use of passwords, such as:

- Passwords with a minimum length of 10 characters.
- Use a mix of alpha-numeric characters (A-S, a-s, 0-9), Minimum of at least one upper- and lower-case character, and symbols (*, #, %, etc.).
- Free of multiple consecutive identical, all-numeric, or all-alphabetic characters.
- Use Passphrases (i.e.., D0g#Truck@p3NC1L).
- Not based on anything somebody else could easily guess or obtain using person-related information, e.g., names, telephone numbers, dates of birth, etc.

All users must:

1. Keep passwords confidential.
2. Avoid keeping a record (e.g., paper, software file, or hand-held device) of passwords unless this can be stored securely in an approved method.
3. Change passwords whenever there is any evidence or indication of possible system or password compromise, elevated risk, or as defined by organizational policy, and must never be re-used or recycled.
4. Change temporary passwords at the first log-on.
5. Only use a single password to access multiple services, systems, or platforms where they have been assured that an elevated level of protection has been established for storing the password within each service, system, or platform (i.e. Single Sign On (SSO)).
6. Not use the same password for business and non-business purposes.
7. Not include passwords in any automated log-on process, e.g., stored in a macro or function key.
8. Expect that sessions will be logged out after 15 minutes of inactivity.

Remote Access

1. New Era Technology provides secure remote access connectivity in various ways:
    a. Collaboration tools (i.e., Microsoft Teams, Microsoft Sharepoint, etc.).
    b. Virtual Private Networks (VPNs).
    c. Remote Monitoring and Management tools (N-Central, Take Control).
    d. Internet-facing services and applications.
    e. Software-as-a-Service (SaaS) platforms.
2. New Era Technology personnel must contact the IT help desk to:
    a. Connect to an existing remote access service.
    b. Obtain approval to add a remote access method into the New Era environment.
3. All remote access connections to New Era networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.

4. New Era personnel accessing systems remotely are responsible for ensuring their mobile device is compliant with the New Era Technology Mobile Devices and BYOD (Bring Your Own Device) Policy.
5. Remote users may connect to New Era networks only after formal approval by the requestor's manager and/or New Era IT.
    a. Remote access to Information Resources must be logged/recorded by IT.
6. Authorized users shall protect their login and password, even from family members.
7. Non-New Era Technology computer systems that require network connectivity must conform to all applicable New Era IT standards and must not be connected without prior written authorization from IT Management.
8. Secure remote access must be strictly controlled.
9. Remote sessions must be terminated after a defined period of inactivity.
10. Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.
11. All hosts connected to New Era's internal networks via remote access technologies must be compliant with applicable policies within the Security Framework.
12. Personal equipment used to connect to New Era's networks must meet the requirements of company-owned equipment for remote access – see New Era Technology's Mobile Devices and BYOD (Bring Your Own Device) Policy.

Vendor Access

1. Vendor access must be uniquely identifiable, provide non-repudiation, and comply with all existing New Era Technology policies.
2. External vendor access activity must be tracked.
3. All vendor maintenance equipment on the New Era Technology network that connects to the outside world via the network, telephone line, or leased line and all New Era Technology Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.

5. Compliance, Monitoring and Enforcement

This Policy is intended for all New Era businesses, in all countries.

New Era Technology seeks to proactively prevent and mitigate instances of non–compliance with this Policy.

Compliance is measured through various methods, including but not limited to risk assessments, business tool reports, internal and external audits, etc.

Any breaches or concerns, including ethical concerns or potential breaches in our commitment to information and data protection standards, should be reported as soon as possible through our Whistleblowing Policy.

Any need for improvements will be applied as soon as possible. Employees are encouraged to offer their feedback on this Policy if they have any suggestions for how it may be improved. Feedback of this nature should be addressed to GRC@neweratech.com.

Any exception to this Policy must be approved by the CTO, CIO, and / or Director of Governance, Risk, and Compliance in advance.

Personnel found to have intentionally violated this Policy may be subject to disciplinary action, up to and including termination of employment and other penalties as set forth herein. New Era Technology reserves the right to pursue any, and all, legal and civil action in connection with any such violation.

Any vendor, consultant, or contractor found to have violated this Policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

6. Acknowledgement

Those in receipt of this Policy acknowledge its receipt and understanding of its contents; and that New Era Technology expressly reserves the right to change, modify, or delete its provisions without notice.

Document Information

Reference	Security Framework
Title	Identity and Access Management (IAM) Policy
Purpose	The purpose of the New Era Technology IAM Policy is to establish 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.
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 responsible for managing New Era Technology Information Resource access and those granted access privileges.
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	Aug 2023	Review	Dir GRC
V2.0	Sep 2023	Annual review, classification & approvers update	CTO, Dir GRC
V3.0	Oct 2024	Annual review, updates to sections 2-6	Dir GRC, SVP Corp A&E, EVP XoC
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	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	Encryption Use Policy	Policy to establish the 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.