New Era Technology, Inc. Clear Desk & Clear Screen Policy

Classification: Public

Clear Desk & Clear Screen Statement

New Era Technology, Inc., and its subsidiaries (collectively the "Company" or "New Era") is committed to reducing the risks of unauthorized access, loss of and damage to information on desks, screens and in other locations during and outside normal working hours.

We expect this policy to be upheld by all employees, (permanent, temporary, or contracted), including executives, officers, and directors of New Era.

Contents

Clear Desk & Clear Screen Statement 1

1. Terms and Definitions 3

2. Scope 3

Relationship to Local/Regional Policies 4

3. Roles and Responsibilities 4

4. Policy 5

5. Compliance, Monitoring and Enforcement 6

6. Acknowledgement 6

Document Information 7

Document History 7

Control of Hardcopy Versions 7

References 8

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“data”	are items of information.
“endpoint”	means any device that is physically an endpoint on a network. Laptops, desktops, mobile phones, tablets, printers, servers, and virtual environments can all be considered endpoints.
“information”	Information is processed, organized and structured data. It provides context for data and enables decision making process. Information can be collected, used, stored, reported, or presented in any format, on any medium.
“staff”, “users”, “personnel"	means those who are employed by New Era Technology on a fulltime, part-time, or temporary basis; those who access and / or utilize New Era Technology’s information resources, including, but not limited to employees, contractors, interns, third and external parties.
“we”, “our”, “New Era”, or “New Era Technology”	refers to New Era Technology, Inc., and its subsidiaries.
“work area”, “workspace" or “workstation”	Is an area in an office, whether permanent or temporary, where personnel perform daily work-related tasks; this might include a desk, writing area, computer, and storage area for documents.

2. Scope

This Policy applies to those who access, process, or store New Era Technology data, including paper documents and digital data. It applies to all of the organization’s employees, as well as to third-party agents authorized to access the data.

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 to 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 clear desk/screen 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 clear desk/screen standards.

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

4. Policy

This clear desk and clear screen policy is an important tool to ensure that all sensitive/confidential materials are removed from a user's workspace and locked away when the items are not in use, or a user leaves their workstation. It is one of the main strategies utilized when attempting to reduce the risk of security breaches in the workplace.

Components of this policy include the following:

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 a work area.

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	Clear Desk and Clear Screen Policy
Purpose	The purpose of this policy is to reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other locations during and outside normal working hours.
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	May 24, 2022	Approved release	CTO, Dir GRC
V1.1	Aug 9, 2023	Review	CTO, Dir GRC
V2.0	Sep 17, 2023	Annual review; classification & approvers update	CTO, Dir GRC
V3.0	Sep 20, 2024	Annual review, updates to sections 2,3,5,6	Dir GRC
V3.0	Oct 18, 2024	Approved release	CTO, Dir GRC

Control of Hardcopy Versions

The digital version of this document is the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. The printed version of this document is uncontrolled, and cannot be relied upon, except when formally issued by the Director of Governance, Risk and Compliance and /or the Chief Technology Officer and provided with a document reference number and revision in the fields below:

Document Ref.	**Rev.**	**Uncontrolled Copy**	**X**	**Controlled Copy**

References

Standard / Framework / Other	Title	Description
New Era GRC Policy	Security Policy	Policy to (a) protect New Era Technology and its customers' data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.
New Era GRC Policy	Acceptable Use Policy	Policy to establish acceptable practices regarding the use of New Era Technology Information Resources to protect the confidentiality, integrity, and availability of information created, collected, and maintained. Inappropriate use exposes New Era to risks, including virus attacks, loss of confidential data, compromise of network systems and services, and legal issues.
New Era GRC Policy	Asset Management Policy	Policy establishing the rules for the control of hardware, software, applications, and information used by New Era Technology.
New Era GRC Policy	Data Classification & Management Policy	Policy which provides a system for classifying and managing information resources according to the risks associated with its storage, processing, transmission, and destruction.
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.