New Era Technology, Inc. Media Sanitization & Destruction Policy

Classification: Public

Media Sanitization & Destruction Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to protecting the proper disposal / sanitization / destruction of media (physical or electronic) at New Era Technology.

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

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
“asset”, “information asset”	means any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware, software, applications and (confidential) information. Assets must be protected from illicit access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the organization[1].
“data”	are items of information.
“disposal” or “destruction”	The terms 'disposal' and 'destruction' are used interchangeably, but disposal does not always mean destruction; both ensure the IT assets, or any confidential information are disposed of, destroyed or sanitized in a way that information cannot be retrieved later.
“media”	Includes, but is not limited to: (1) electronic storage devices, including computer hard drives and transportable digital memory media, such as magnetic tapes, disks, or USB flash drives; (2) transmission media used to exchange information already in electronic form, such as private networks, the Internet, and the physical movement of transportable memory devices; and (3) **printouts** onto which information is recorded, stored, or printed within an information system
“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, Inc., and its subsidiaries.

[1] https://en.wikipedia.org/wiki/Asset_(computer_security)

2. Scope

This policy applies to all New Era Technology personnel with access to New Era Technology's information assets – hardware, software, applications and (confidential) data. This policy applies to all equipment and applications that processes, stores, and/or transmits New Era Technology information.

This Policy applies to New Era Technology personnel who are responsible for the use, purchase, implementation, and/or maintenance of New Era Technology's Information Resources and it applies to all equipment and applications that processes, stores, and/or transmits New Era Technology information.

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 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 media sanitization and destruction management standards.

If any additional media sanitization and destruction 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.

New Era Technology IT personnel will ensure that arrangements are made for the secure disposal or reuse of resources (e.g., equipment, data storage, files, memory).

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

Overview

Media reuse and destruction practices must be conducted in compliance with the methods defined in this Policy.

1. Media that may contain confidential or internal information must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
2. All decommissioned media must be stored in a secure area prior to destruction.
3. Media reuse and destruction practices must be tracked and documented.
4. All information must be destroyed when no longer needed, included encrypted media.
5. Dispose assets only through approved waste handlers or recyclers, and in a manner that complies with applicable regulations; obtain a certificate of destruction when data has remained on the asset.
6. Damaged equipment must undergo a risk assessment to determine whether the items need to be physically destroyed rather than sent for repair or discarded.
7. Whole-disk encryption is recommended as it reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed.

Media Disposal

All decommissioned media must be stored in a secure area prior to disposal.

Electronic and/or physical media must be disposed of by one of the following methods:

1. **Overwriting (at least 3 times)** – an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
2. **Degaussing** – a method to magnetically erase data from magnetic media.
   Two types of degaussing exist:
   a. strong magnets and
   b. electric degausses.
   Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
3. **Destruction** – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.
4. **Shredded** using an IT approved, commercial grade shredder.

5. **Placed in locked shredding bins** for an IT approved external party with adequate controls and experience to come on-site and cross-cut shred, either witnessed by New Era Technology personnel throughout the entire process, or a Certificate of Data Destruction provided by the external party for record.
6. **Incineration** using incinerators of an IT approved external party with adequate controls and experience or witnessed New Era Technology personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel; a Certificate of Data Destruction must also be provided by the external party for record.

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	Media Sanitization and Destruction Policy
Purpose	The purpose of this policy is to outline the proper disposal / sanitization / destruction of media (physical or electronic) at New Era Technology. These rules are in place to protect sensitive and confidential information, employees and New Era Technology. Inappropriate disposal of New Era Technology information and media may put New Era Technology, its personnel and its customers at risk.
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	Internal

Document History

VERSION CONTROL			
Revision	**Date**	**Record of Changes**	**Approved /Released By**
V1.0	Nov 3, 2022	Approved release	CTO, Dir GRC
V2.0	Sep 17, 2023	Annual review; classification & approvers update	CTO, Dir GRC
V3.0	Oct 8, 2024	Annual review, updates to sections 2-6	Dir GRC, EVP XoC
V3.0	Oct 22, 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 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.
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.