Media Sanitization & Destruction Policy

Classification: Public

Media Sanitization & Destruction Policy Statement

New Era Technology and its subsidiaries (collectively the “Company” or “New Era”) are committed to implementing the necessary requirements to ensure that media disposal, sanitisation, and destruction processes protect Company information, uphold information security, and comply with applicable Company policies and procedures.

This Policy applies to all individuals responsible for handling, managing, or disposing of media (physical or electronic) within New Era Technology, including permanent, temporary, and contracted employees, as well as executives, officers, and directors. All users are expected to act responsibly and in accordance with established procedures to ensure the secure and compliant destruction of Company information assets.

New Era will implement and maintain controls to ensure that:

- Approved methods are used for the secure disposal of physical and electronic media in accordance with Company standards and all applicable regional, national, regulatory, contractual, and government requirements.
- Media containing sensitive or confidential information is destroyed in a manner that prevents unauthorised recovery.
- Disposal activities comply with legal, regulatory, and Company retention requirements.

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 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 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 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), 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.

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

To safeguard Company information assets, the following requirements shall be met in accordance with Company standards and all applicable regional, national, regulatory, contractual, and government requirements:

1. Secure Sanitization or Destruction
    a. Media that may contain confidential, regulated, government-related, or general business information must be securely sanitized or destroyed before reuse, redeployment, or disposal using an approved method appropriate to the data classification and jurisdiction.
    b. Encrypted media must also be destroyed when no longer required, unless cryptographic erase is expressly permitted by applicable regional, regulatory, or contractual requirements.
2. Secure Storage Prior to Disposal
    a. All decommissioned media must be stored in a secure, access-controlled area until sanitisation or destruction is completed.
3. Risk Assessment for Damaged Equipment
    a. Damaged equipment must undergo a documented risk assessment to determine whether physical destruction is required instead of repair or standard disposal, considering data sensitivity and regional or governmental requirements.
4. Mandatory Encryption
    a. Whole-disk encryption is recommended on devices storing Company data to reduce risk during disposal or redeployment.
5. Documentation and Auditability
    a. All sanitization and destruction activities must be logged, including date, method used, responsible personnel, and supporting evidence (e.g., certificates of destruction).
    b. Records shall be retained in accordance with Company retention requirements and applicable legal or regulatory obligations.
6. Chain of Custody
    a. When using external vendors, a documented chain of custody must be maintained from transfer to final destruction.
    b. A Certificate of Data Destruction must be obtained from the vendor for all outsourced destruction activities.
7. Approved Disposal Channels
    a. Assets must only be disposed of through Company-approved waste handlers, recyclers, or destruction providers, in compliance with applicable environmental, regulatory, and data-protection requirements.

Approved Media Disposal Methods

Electronic and/or physical media must be disposed of by one of the following approved methods below, selected based on:

- Data classification
- Media type
- Regional, national, government, regulatory, or contractual requirements.

Where regional or governmental standards apply, those requirements must be met or exceeded, including (but not limited to):

- United States: U.S. Government or Department of Defense-aligned requirements (e.g. DoD or NIST-based standards)
- United Kingdom: UK Government security classifications and NCSC/HMG-aligned requirements
- Other jurisdictions: Local statutory, regulatory, or government-mandated data sanitization requirements

Where requirements differ, the most stringent applicable standard shall apply.

1. Secure Overwrite
    a. Use an IT-approved secure erase tool that meets industry standards for data sanitisation and any applicable regional or government requirements.
    b. Overwriting shall completely replace existing data with random or defined patterns sufficient to prevent recovery using appropriate forensic techniques.
    c. Tools used for this purpose must produce a verification report confirming successful data erasure.
2. Cryptographic Erase
    a. For encrypted media, securely and permanently delete all encryption keys to render data irretrievable.
    b. Cryptographic erase must only be used where permitted by the applicable regional, regulatory, or government standard and where encryption strength and key management are sufficient.
3. Degaussing
    a. Magnetically erase data from magnetic media using an approved, commercial-grade degaussing device suitable for the media type and compliant with applicable regional or governmental requirements.
    Note: Common household magnets are insufficient for effective degaussing and must not be used.

   b. Where required by applicable standards, degaussed media must subsequently be physically destroyed.
4. Physical Destruction
   a. Physically dismantle media through crushing, shredding, or incineration to ensure platters, chips and storage components are destroyed beyond recovery.
   b. Shredding must be performed:
      - Using an IT-approved commercial-grade shredder, or
      - By an authorized external party under supervision or supported by a Certificate of Data Destruction.
   c. Incineration must be conducted:
      - By an IT-approved external party with adequate controls and experience, and
      - Either witnessed by Company personnel or verified through a Certificate of Data Destruction.

Verification

After sanitisation or destruction, verification must be performed and documented to confirm that data cannot be recovered in line with the applicable method, standard, and regional requirement.

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	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 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	Nov 2022	Approved release	CTO, 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, 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	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 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.