1. Purpose

The purpose of this policy is to establish procedures for the secure reuse and destruction of data storage media to:

- Prevent unauthorized disclosure of sensitive information, including client data, proprietary marketing strategies, and employee information.
- Ensure compliance with relevant data protection regulations and contractual obligations.
- Minimize the risk of data breaches and reputational damage.
- Ensure that all media is sanitized or destroyed in a manner appropriate to the sensitivity of the data it contains.

2. Scope

This policy applies to all employees, contractors, and temporary staff of Corporate Communications, Inc. who handle, manage, or are responsible for the disposal or reuse of any data storage media. This policy covers all electronic and physical media owned, leased, or used by the agency, including but not limited to:

- **Electronic Media:**
    - Hard disk drives (HDDs) and solid-state drives (SSDs) in computers, servers, and external storage devices
    - USB flash drives and other removable storage devices
    - Optical media (CDs, DVDs, Blu-rays)
    - Memory cards (SD, microSD, etc.)
    - Mobile devices (smartphones, tablets)
    - Cloud storage accounts (when decommissioning or migrating data)
- **Physical Media:**
    - Paper documents
    - Printed materials
    - Other media containing sensitive information

3. Policy

3.1 General Principles

- All data storage media must be handled and disposed of in a secure manner.
- The sensitivity of the data stored on the media must be considered when determining the appropriate method for reuse or destruction.
- Employees are responsible for adhering to this policy and reporting any concerns or incidents to the IT department or designated security officer.
- Data must be destroyed in such a way that it cannot be read or reconstructed by any means.
- The disposal of media must be documented, including the date, method of destruction/sanitization, and the individual responsible.

3.2 Media Reuse

- **Internal Reuse:** When media is to be reused within the agency (e.g., reassigning a computer to a

different employee), the data on the media must be sanitized to the appropriate level for the sensitivity of the data.
- **External Reuse:** Media containing sensitive information must not be reused outside the agency (e.g., donation, sale) unless it has been sanitized to the highest level.
- Prior to reuse, media should be inspected for damage that could hinder the sanitization process. Damaged media should be destroyed.

3.3 Media Destruction

- Media that is no longer needed and cannot be securely reused must be destroyed.
- The method of destruction must be appropriate to the type of media and the sensitivity of the data it contains, as outlined in Section 4.
- Destruction should be carried out by authorized personnel only.
- For sensitive or confidential data, destruction must be witnessed and documented by at least two authorized individuals.

3.4 Methods of Sanitization and Destruction

The following methods are approved for sanitizing and destroying data storage media:

- **Electronic Media:**
  - **Low-Level Formatting:** Overwrites the media with a pattern of ones and zeros. Suitable for media with non-sensitive data and internal reuse.
  - **Data Wiping Software:** Uses software to overwrite the media multiple times with complex patterns, meeting industry standards (e.g., NIST 800-88). Acceptable for internal reuse and some cases of external reuse where the data is moderately sensitive.
  - **Degaussing:** Exposes magnetic media (HDDs, tapes) to a strong magnetic field, rendering the data unreadable. Effective for making media unusable but does not guarantee complete data removal on damaged drives.
  - **Physical Destruction:**
    - **Shredding:** For electronic media (SSDs, USB drives, etc.), use an electronic media shredder that reduces the media to small, unreadable particles or third-party destruction company (Iron Mountain)
    - **Drilling/Crushing:** Physically damaging the media to the point of complete destruction.
    - **Incineration:** Burning the media in a controlled environment.
- **Physical Media:**
  - **Shredding:** Use a cross-cut shredder to destroy paper documents and other printed materials or third-party destruction company (Iron Mountain)
  - **Incineration:** Burning the media in a controlled environment.

3.5 Data Sensitivity Levels

The following data sensitivity levels should be used to determine the appropriate sanitization and destruction methods:

- **Public:** Information that is freely available to the public. Low-level formatting/deletion is usually sufficient.

- **Internal:** Information for use within the agency only. Data wiping software or degaussing is recommended. Physical destruction may also be used.
- **Confidential:** Sensitive information that could harm the agency or its clients if disclosed. Data wiping software (multiple passes) and physical destruction are required.
- **Highly Confidential:** Extremely sensitive information, such as client data, financial records, or trade secrets. Secure data wiping (highest standard) and physical destruction are required. Destruction must be witnessed and documented.

3.6 Documentation

- A record of all media destruction activities must be maintained. The record should include:
  - Date of destruction
  - Type of media
  - Method of destruction/sanitization
  - Description of the data contained on the media
  - Name(s) of the person(s) performing or witnessing the destruction
  - Any relevant serial numbers or identifiers
- Records should be retained for 7 years.

3.7 Compliance

- This policy is designed to comply with all applicable data protection laws and regulations.
- Employees are responsible for ensuring that their actions comply with this policy & all relevant laws.
- Violations of this policy may result in disciplinary action, up to and including termination of employment, as well as legal consequences.

3.8 Training and Awareness

- All employees will receive training on this policy and their responsibilities regarding media reuse and destruction.
- Periodic reminders and updates will be provided to ensure ongoing compliance.

3.9 Exceptions

- Any exceptions to this policy must be approved in writing by agency owner.
- Requests for exceptions must include a detailed justification & assessment of potential risks.

3.10 Review and Updates

- This policy will be reviewed and updated periodically, or as needed, to reflect changes in technology, data protection laws, and the agency's needs.
- Employees will be informed of any changes to this policy.

Revision History

04/25/2025

- Originated