

Michael Scott Paper Company

Media Destruction Policy

Revised January 2024

Purpose

Michael Scott Paper Company's Media Destruction Policy aims to establish guidelines and procedures for the secure destruction of media containing sensitive or confidential information to prevent unauthorized access, disclosure, or misuse.

Scope

The scope of this Media Destruction Policy extends to all individuals who handle or have access to sensitive information stored on various forms of media within the organization.

Responsibilities

Management: It is the responsibility of management to ensure that adequate resources are allocated for the proper destruction of media containing sensitive information.

Employees: All employees must adhere to the procedures outlined in this policy for the secure destruction of media.

IT Department: The IT department is responsible for implementing and maintaining procedures for the secure destruction of digital media, including the use of specialized software tools if necessary.

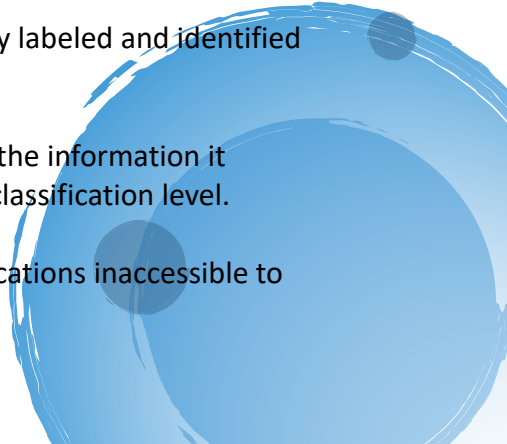
Security Officer: The security officer shall oversee compliance with this policy and conduct periodic audits to ensure adherence to established procedures.

Procedures

Identification: All media containing sensitive information must be clearly labeled and identified as such.

Classification: Media should be classified according to the sensitivity of the information it contains. Different destruction methods may be required based on the classification level.

Secure Storage: Media awaiting destruction must be stored in secure locations inaccessible to unauthorized personnel.



Destruction Methods:

Physical Destruction: Media should be physically destroyed using methods such as shredding, pulverizing, or incineration. This applies to both electronic and physical media. The Michael Scott Paper Company has a contract in place with an external vendor to shred hard drives and is who should be used to shred retired hard drives.

Data Wiping: For digital media, data wiping using certified software tools must be performed to ensure complete erasure of sensitive information. Multiple passes may be necessary to overwrite data effectively.

Documentation: A record of media destruction activities, including the date, method, and personnel involved, must be maintained for audit and compliance purposes.

Third-Party Destruction: If outsourcing media destruction services to third-party vendors, contracts must include provisions for compliance with this policy and verification of proper destruction methods.

Sanctions

Failure to comply with the Media Destruction Policy may result in disciplinary action, which will be administered in accordance with the corporation's Human Resources procedures. This can range from formal warnings and mandatory cybersecurity training to temporary suspension of access privileges and, in severe cases, termination of employment or contractual relationship. Additionally, individuals may be subject to prosecution for any illegal activities under applicable local, state, national, or international laws. This is to underscore the critical nature of cybersecurity and everyone's role in maintaining the safety and integrity of our corporate digital assets. Sanctions will be enforced impartially and consistently to all parties covered by the policy, with severity proportional to the extent of the policy violation.

Definitions

Media: Any physical or digital storage device including, but not limited to, hard drives, solid-state drives (SSDs), magnetic tapes, optical discs, USB drives, memory cards, and any other portable storage devices.

Sensitive Information: Any information that, if disclosed, could result in harm to individuals, the organization, or its stakeholders. This includes, but is not limited to, personally identifiable information (PII), financial data, trade secrets, proprietary information, and intellectual property.