SOP: Sensitive Data Disposal

Purpose:

The purpose of this SOP is to provide guidelines for the MSP to securely dispose of the company's sensitive data in compliance with the Department of Defense (DoD) 5220.22-M standard. This SOP ensures the protection of client data privacy and mitigates the risk of data breaches during the disposal process.

Scope:

This SOP applies to the MSP IT Support Team and all employees at the company.

Responsibilities:

Support Team: Responsible for executing the secure disposal process and maintaining the necessary documentation.

Employees: Responsible for alerting the Support Team to any emergent data disposal needs.

Prerequisites:

The Company has identified existing sensitive data including customer databases, PII, and proprietary software.

The Support Team has a shredder, commercial grade degausser and a USB bootable DBAN

Procedure:

Data Classification and Inventory:

- The Support Team shall classify data based on its sensitivity and importance to the client and the overall security of the systems.

- Maintain an updated inventory of storage media containing client data, including details such as serial numbers, types, and locations.

Selection of Secure Disposal Method:

- The company employees will alert the Support Team to data that needs to be disposed of.
- The Support Team will determine the appropriate secure disposal method based on the media type, client requirements, and DoD 5220.22-M guidelines.
- The preferred methods for secure disposal are secure erasure and physical destruction.

Storage Media	DoD 5220.22-M Clear Method
Magnetic Tape	Degauss
Magnetic Disk	Degauss or overwrite
Optical Disk	Overwrite**
DRAM	Overwrite or remove all power
EAPROM/EEPROM#	Full chip erase
Flash EPROM	Full chip erase
Programmable ROM (PROM)	Overwrite
Nonvolatile RAM (NOVRAM)	Overwrite or remove all power

Source: Bitraser.com

Secure Erasure:

- Utilize software solutions that comply with the DoD 5220.22-M Clear method for secure erasure.
- Follow the manufacturer's instructions and guidelines for using the secure erasure software.

- Perform multiple overwrites of the storage media with predetermined patterns to ensure complete data removal, as recommended by the DoD 5220.22-M standard.
    - The Support Team will utilize a bootable USB with DBAN to conduct overwrites.
- Keep records of the erasure process, including the date, time, erasure method used, and verification results.

Physical Destruction:

- If secure erasure is not feasible or not recommended for the storage media, physical destruction should be performed.
- Use appropriate methods for physical destruction, such as shredding, crushing, or disassembling the media.
- Engage certified third-party vendors or specialized equipment for physical destruction, if required.
- Document the physical destruction process, including the method used, date, time, and witness if applicable.

Verification and Quality Control:

- After erasure or destruction, perform a verification process to ensure the complete removal of data.
- Verify erasure by examining the storage media for any recoverable data using appropriate tools or software.
- In the case of physical destruction, ensure the media is irreversibly damaged and rendered unusable.
- Document the results of the verification process for each storage media.

Training and Awareness:

- Conduct training sessions for Support Team members involved in the secure disposal process, emphasizing the importance of data privacy, compliance, and the proper execution of the SOP.
- Ensure Support Team members are familiar with the secure erasure software and methods compliant with the DoD 5220.22-M standard.
- Regularly communicate and reinforce the secure disposal procedures and any updates or changes to the SOP.

Incident Management:

- Establish an incident management process to handle any security incidents, breaches, or failures related to the secure disposal process.
- In the event of an incident, promptly investigate and take necessary actions to mitigate the impact, restore security, and prevent future occurrences.
- Document and report incidents, including root cause analysis and remediation steps, to prevent similar incidents in the future.

References:

Department of Defense (DoD) 5220.22-M: National Industrial Security Program Operating Manual (NISPOM)

Definitions:

- MSP - Managed Service Provider
- IT - Information Technology
- SOP - "what, when, why"; could be multiple SOPs to support a specific policy
- DBAN - Darik’s Nuke and Boot

Revision History:

5/16/2023 -- "SOP: Data Back-up and Restoration” created by Jon McMullin