Disposal & Destruction Policy

Table of contents

1. Purpose, scope and users

The purpose of this document is to ensure that information stored on equipment and media is safely destroyed or erased.

This document is applied to the entire Information Security Management System (ISMS) scope, and to all personal data processing activities.

Users of this document are all employees of KubeNet.

2. Reference documents

- EU GDPR Article 32
- Information Security Policies
- Data Retention Policy

3. Disposal and destruction of equipment and media

All data and licensed software stored on mobile storage media (e.g. on CD, DVD, USB flash drive, memory card, etc.; but also on paper) and on all equipment containing storage media (e.g. computers, mobile phones, etc.) must be erased or the medium destroyed before it is disposed of or reused. The retention period is defined in the Data Retention Policy.

The person responsible for erasing data / destroying media must inform the owner of the asset in question about erasing /destroying data.

3.1. Equipment

Security Officer is responsible for checking and erasing data from equipment. Data must be erased factory reset the equipment but if the process is not secure enough considering the sensitivity of the data, then the storage medium must be destroyed.

3.2. Mobile storage media

Security Officer is responsible for erasing data from mobile storage media. Data must be erased [describe the technology used for erasing data from media], but if the erasure process is not secure enough considering the sensitivity of the data, then the storage medium must be destroyed.

3.3. Paper media

Employees of the organization handling individual documents are responsible for destroying paper documents. Paper documents are destroyed in paper shredders.

3.4. Erasure and destruction records; commission for the destruction of information

Records of erasure/destruction must be kept for all data classified as "Restricted" and "Confidential". Records must include the following information: information about the media, date of erasure/destruction, method of erasure/destruction, person who carried out the process.

All information classified as "Confidential" must be erased/destroyed in the presence of a commission consisting of persons authorized to access the information in question.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Disposal of Records Form	Locally saved under “Data protection” folder	Data Protection Officer	Only authorized persons may access the folder	Records are stored for a period of 5 years