USJ 1875

Université Saint-Joseph de Beyrouth

جامعة القدّيس يوسف في بيروت

Data Destruction Policy

(The French text of this Policy was approved by the University Board during its 217th meeting on February 22, 2023)

Purpose (Aim, Benefits, and Framework)

This policy is designed to ensure the safe deletion of data that is no longer of use to Saint Joseph University of Beirut (hereinafter referred to as “the University”).

This policy ensures that outdated information is properly destroyed and rendered irretrievable in order to guarantee its confidentiality and to optimize disk space on the University’s hardware.

This policy applies to all information processed by the University, including information that the University produces, receives or retains in carrying out its activities.

This policy covers all data (used in teaching, research and administration) stored on any medium and in any format, including both soft and hard copy files. The term “data” refers to original documents, back-up copies, photocopies, etc.

Administrator	Chief Information Security Officer, hereinafter referred to as “CISO”.
Roles	**Duties**
Users	Anyone with access to University data must comply with this policy and ensure that information belonging to the University and no longer required is disposed of appropriately.
STI	The Information Technology Office (hereinafter referred to as “STI”) must destroy all information stored on computer equipment before disposing of it, in order to ensure that said data has become irretrievable.
CISO	The CISO oversees compliance with and application of this policy.
Beneficiaries	Staff, faculty and students.

Description

Hard Copies

- Documents intended for public viewing and therefore containing no sensitive data can be recycled.
- Documents not intended for public viewing (for internal use only) should be torn.
- Documents containing sensitive information, particularly personal data, should be shredded. If a shredder is not available, they should be torn into small, unreadable pieces and disposed of in separate garbage cans.

Soft Copies

- Documents intended for public viewing and therefore containing no sensitive data should only be deleted.
- Documents not intended for public viewing (for internal use only) should be deleted and the Recycle Bin of the computer should be emptied.
- Documents containing sensitive information, particularly personal data, should be deleted. The Recycle Bin of the computer should be emptied, and in collaboration of the STI, said documents should be destroyed and made irretrievable, using specific tools if needed.

IT Equipment

- IT equipment (*computers, laptops, tablets, etc.*), including removable storage media (*hard disks, USB keys, CDs, DVDs, etc.*) containing professional data and no longer of use to their owners who wish to dispose of them, must be returned to STI to destroy all the information stored on them, thus rendering said data irretrievable.
- All IT equipment belonging to the University and on which data is stored is by default considered to be handling sensitive data. Therefore, all equipment must undergo appropriate physical destruction by STI prior to disposal.
- When data destruction is impossible, equipment must be physically destroyed beyond repair, so that the information stored on it becomes irretrievable.
- When computer equipment is to be disposed of by the University for re-use, the relevant supervisor must check with STI that all professional data has been completely destroyed prior to disposal.
- Photocopiers and printers which store data during use must also undergo the same information destruction process prior to disposal.
- STI must keep a record of how the equipment was destroyed: physical destruction of the equipment or destruction of the soft copies it holds.

Online Data

Documents containing sensitive data and deleted from the cloud (OneDrive, Google Drive, etc.) should also be removed from the Recycle Bin of the cloud. Do not rely on the automatic deletion feature available on some platforms.

Norme, conseil, références	ISO 27001:2013