Université Saint-Joseph de Beyrouth
جامعة القدّيس يوسف في بيروت

Politique de destruction des données

(Texte approuvé par le Conseil de l'Université lors de sa 217e réunion en date du 22 février 2023)

Objet (objectif, avantages, cadre)

L'objectif de cette politique est de garantir la suppression en toute sécurité des données qui ne sont plus utiles pour l'Université Saint-Joseph de Beyrouth (ci-après : l'Université).

Cette politique veille à ce que les informations périmées soient correctement détruites et rendues irrécupérables afin de garantir leur confidentialité. Elle permet également d'optimiser l'espace disque des ressources de l'Université.

Cette politique s'applique à toutes les informations traitées par l'Université, y compris les informations créées, reçues ou conservées par l'Université dans le cadre de ses activités.

Cette politique couvre toutes les données (utilisées dans l'enseignement, la recherche et l'administration) stockées sur n'importe quel support et sous tout format, y compris les fichiers électroniques et les documents sur papier. Le terme « données » désigne les documents originaux, ainsi que toutes les copies de backup, photocopies, etc.

Gérant	Responsable de la sécurité des systèmes d'information (Chief information security officer-CISO, ci-après le RSSI)
Rôles	**Responsabilités**
Utilisateurs	Toute personne ayant accès aux données de l'Université doit se conformer à la présente politique et s'assurer que les informations appartenant à l'Université et qui ne sont plus requises soient éliminées de manière appropriée.
STI	Le Service de technologie de l'information (ci-après STI) est responsable de la destruction de toutes les informations stockées sur les équipements informatiques avant de s'en débarrasser et ce afin de garantir que lesdites données sont devenues irrécupérables.
RSSI - CISO	Le RSSI est responsable de la vérification du respect et de l'application de cette politique.
Bénéficiaires	Membres du PSG, enseignants et étudiants

Description

Documents sur support papier

- Les documents publics ne contenant aucune donnée sensible peuvent être recyclés.
- Les documents non publics (internes à l'Université) doivent être déchirés.
- Les documents contenant des informations sensibles, notamment des données à caractère personnel, doivent être déchiquetés. En cas de non disponibilité de déchiqueteuse, ils doivent être déchirés en de petits morceaux illisibles et jetés dans des corbeilles séparées.

Documents électroniques

- Les fichiers publics ne contenant aucune donnée sensible doivent être uniquement supprimés.
- Les fichiers non publics (internes à l'Université) doivent être supprimés et vidés de la corbeille de l'ordinateur.
- Les fichiers contenant des informations sensibles, notamment des données à caractère personnel, doivent être supprimés, vidés de la corbeille de l'ordinateur et détruits en collaboration avec le support du STI qui pourrait utiliser des outils spécifiques pour rendre ces documents irrécupérables.

Equipements informatiques

- Les équipements informatiques (*ordinateur, portable, tablette, etc.*) y compris les supports amovibles de stockage (*disque dur, clé USB, CD, DVD, etc.*) contenant des données professionnelles et non plus utiles à leurs propriétaires qui souhaitent en disposer doivent être envoyés au STI pour détruire intégralement les informations qui y sont stockées, les rendant ainsi irrécupérables.
- Tous les équipements informatiques appartenant à l'Université et sur lesquels des données sont stockées sont considérés par défaut traitant des données sensibles. Par conséquence, tous ces équipements doivent subir une destruction physique appropriée par le STI avant leur élimination.
- Lorsque la destruction des données est impossible, l'équipement doit être physiquement détruit de manière irréparable, de façon à ce que les informations qui y sont stockées soient détruites de façon irrécupérable.
- Lorsqu'un équipement informatique doit être aliéné par l'Université pour sa réutilisation, le responsable concerné doit s'assurer avec le STI que les données professionnelles ont été complètement détruites avant toute aliénation.
- Les photocopieuses et les imprimantes qui stockent des données lors de leur utilisation doivent subir également le même processus de destruction des informations avant leur élimination.
- Le STI doit conserver un enregistrement précisant la manière dont les équipements ont été détruits : destruction physique de l'équipement ou destruction des documents électroniques y conservés.

Données en ligne

- Les documents contenant des données sensibles et supprimés du cloud (*OneDrive, Google Drive, etc.*) doivent être éliminés également de la corbeille. Il ne faut pas compter sur la suppression automatique qui existe dans certaines plateformes.

Norme, conseil, références	ISO 27001:2013