Table 1 : Version 1 du “Niveaux de Préservation Numérique »

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Niveau 1 (Protéger vos données) | Niveau 2 (Connaître vos données) | Niveau 3 (Surveiller vos données) | Niveau 4 (Réparer vos données) |
| Stockage et implantations géographiques  | * Deux copies complètes non colocalisées
* Pour les données sur des supports hétérogènes (disques optiques, disques durs…) extraire le contenu du support et le copier dans le système de stockage
 | * Au moins trois copies complètes
* Au moins une copie dans un lieu géographiquement distinct
* Documenter le système de stockage et ses supports et ce qui est nécessaire pour les utiliser
 | * Au moins une copie dans un lieu géographique soumis à des menaces de nature différente
* Des processus de surveillance de l’obsolescence du système de stockage et de ses supports
 | * Au moins trois copies dans des lieux géographiques soumis à des menaces de nature différente
* Avoir un plan complet en place pour garder les fichiers et les métadonnées sur des supports ou des systèmes accessibles à tout moment
 |
| Intégrité des fichiers et sûreté des données | * Vérifier l’intégrité des fichiers au versement si cette information a été fournie avec le contenu
* Créer une information d’intégrité si elle n’a pas été fournie avec le contenu
 | * Vérifier l’intégrité pour tous les versements
* Utiliser des bloqueurs d’écriture pour travailler sur des supports originaux
* Faire un contrôle anti-virus pour les contenus à haut-risque
 | * Vérifier l’intégrité à intervalle régulier
* Maintenir des journaux sur l’information d’intégrité ; fournir un rapport d’audit à la demande
* Être en mesure de détecter les données corrompues
* Faire un contrôle anti-virus pour tous les contenus
 | * Vérifier l’intégrité en réponse à des événements ou des activités spécifiques
* Être en mesure de remplacer/réparer des données corrompues
* S’assurer qu’il n’existe aucun individu qui ait un accès en écriture à toutes les copies
 |
| Sécurité de l’information | * Identifier qui a les droits en lecture, écriture, déplacement et suppression sur les fichiers individuels
* Restreindre le nombre de ceux qui ont ces droits sur les fichiers individuels
 | * Documenter les restrictions d’accès aux contenus
 | * Maintenir des journaux sur les individus qui ont réalisé des actions sur les fichiers, y compris les suppressions et les actions de préservation
 | * Réaliser des audits sur les journaux
 |
| Métadonnées | * Inventorier le contenu et ses emplacements dans le système de stockage
* S’assurer de la sauvegarde de l’inventaire sur un système de stockage distinct
 | * Enregistrer les métadonnées administratives
* Enregistrer les métadonnées de transformation et les journaux d’événements
 | * Enregistrer les métadonnées techniques et descriptives dans un formalisme standard
 | * Enregistrer les métadonnées de pérennisation dans un formalisme standard
 |
| Formats de fichiers | * Quand il est possible d’influer sur la création des fichiers numériques, encourager l'utilisation d'un nombre limité de formats et codecs ouverts et connus.
 | * Inventorier les formats de fichiers utilisés
 | * Surveiller les problématiques d’obsolescence de formats de fichiers
 | * Réaliser des migrations de format, de l’émulation et toutes autres activités du même type, dès que nécessaire
 |