NIVEAUX DE PRESERVATION NUMERIQUE

Domaine fonctionnel	Niveaux			
	Niveau 1 (connaître vos contenus)	**Niveau 2 (protéger vos contenus)**	**Niveau 3 (surveiller vos contenus)**	**Niveau 4 (pérenniser vos contenus)**
Stockage	Posséder deux copies complètes dans des lieux distincts. Documenter tous les supports de stockage où les contenus sont stockés. Utiliser des supports de stockage stables.	Posséder trois copies complètes avec au moins une copie à un emplacement géographique distinct. Documenter le stockage et les supports de stockage en indiquant les ressources et dépendances nécessaires à leur fonctionnement.	Posséder au moins une copie à un emplacement géographique présentant un type de menace différent de ceux des autres emplacements. Posséder au moins une copie sur un support de stockage différent. Surveiller l'obsolescence du stockage et des supports.	Posséder au moins trois copies dans des emplacements géographiques présentant des types de menaces différents. Augmenter la variété des supports de stockage pour éviter les points de défaillance uniques. Avoir un plan et mener des actions pour remédier à l'obsolescence des supports de stockage, des logiciels et du matériel informatique.
Intégrité	Vérifier l'information d'intégrité si celle-ci a été fournie avec les contenus. Générer une information d'intégrité si aucune information n'est disponible. Contrôler la présence de virus. Le cas échéant, mettre les contenus en quarantaine.	Vérifier l'information d'intégrité lors de la migration ou de la copie des contenus. Utiliser des bloqueurs d'écriture lors des travaux sur les supports originaux. Sauvegarder l'information d'intégrité et stocker la copie dans un emplacement distinct de celui des contenus.	Vérifier l'information d'intégrité à intervalles réguliers. Documenter les processus et les résultats des vérifications de l'information d'intégrité. Mener des audits d'intégrité à la demande.	Vérifier l'information d'intégrité à la suite d'événements ou d'activités spécifiques. Remplacer ou réparer les contenus corrompus le cas échéant.
Contrôle	Déterminer les agents humains et logiciels autorisés à lire, écrire, mettre à jour et supprimer les contenus.	Documenter les droits de lecture, d'écriture, de mise à jour et de suppression des agents humains et logiciels.	Identifier les agents humains et logiciels qui mènent des actions sur les contenus et journaliser ces actions.	Examiner périodiquement les journaux des opérations et des accès.
Métadonnées	Créer un inventaire des contenus. Y documenter les emplacements utilisés pour le stockage. Sauvegarder cet inventaire et en conserver au moins une copie à part des contenus eux-mêmes.	Stocker suffisamment de métadonnées pour connaître les contenus (possibilité de combiner les métadonnées administratives, techniques, descriptives, de préservation et structurelles).	Déterminer quel standard de métadonnées appliquer. Trouver et combler les lacunes dans les métadonnées pour se conformer à ces standards.	Archiver les actions de préservation associées au contenu et les occurrences de ces actions. Choisir et implémenter des standards de métadonnées.
Contenu	Documenter les formats de fichiers et toutes les autres propriétés essentielles (*significant properties*) des contenus, y compris les modalités et la date d'acquisition de cette documentation.	Vérifier les formats de fichiers et les autres propriétés essentielles (*significant properties*) des contenus. Développer des relations avec les créateurs de contenus pour encourager des choix de formats de fichiers durables.	Surveiller l'obsolescence et les évolutions des technologies dont dépendent les contenus.	Mener des opérations de migration, de normalisation, d'émulation, etc. pour s'assurer que les contenus restent acccessibles.

DOI 10.17605/OSF.IO/QGZ98

NDSA

NIVEAUX DE PRESERVATION NUMERIQUE

Niveaux	Domaine fonctionnel				
	Stockage	**Intégrité**	**Contrôle**	**Métadonnées**	**Contenu**
Niveau 1 (connaître vos contenus)	Posséder deux copies complètes dans des lieux distincts. Documenter tous les supports de stockage où les contenus sont stockés. Utiliser des supports de stockage stables.	Vérifier l'information d'intégrité si celle-ci a été fournie avec les contenus. Générer une information d'intégrité si aucune information n'est disponible. Contrôler la présence de virus. Le cas échéant, mettre les contenus en quarantaine.	Déterminer les agents humains et logiciels autorisés à lire, écrire, mettre à jour et supprimer les contenus.	Créer un inventaire des contenus. Y documenter les emplacements utilisés pour le stockage. Sauvegarder cet inventaire et en conserver au moins une copie à part des contenus eux-mêmes.	Documenter les formats de fichiers et toutes les autres propriétés essentielles (*significant properties*) des contenus, y compris les modalités et la date d'acquisition de cette documentation.
Niveau 2 (protéger vos contenus)	Posséder trois copies complètes avec au moins une copie à un emplacement géographique distinct. Documenter le stockage et les supports de stockage en indiquant les ressources et dépendances nécessaires à leur fonctionnement.	Vérifier l'information d'intégrité lors de la migration ou de la copie des contenus. Utiliser des bloqueurs d'écriture lors des travaux sur les supports originaux. Sauvegarder l'information d'intégrité et stocker la copie dans un emplacement distinct de celui des contenus.	Documenter les droits de lecture, d'écriture, de mise à jour et de suppression des agents humains et logiciels.	Stocker suffisamment de métadonnées pour connaître les contenus (possibilité de combiner les métadonnées administratives, techniques, descriptives, de préservation et structurelles).	Vérifier les formats de fichiers et les autres propriétés essentielles (*significant properties*) des contenus. Développer des relations avec les créateurs de contenus pour encourager des choix de formats de fichiers durables.
Niveau 3 (surveiller vos contenus)	Posséder au moins une copie à un emplacement géographique présentant un type de menace différent de ceux des autres emplacements. Posséder au moins une copie sur un support de stockage différent. Surveiller l'obsolescence du stockage et des supports.	Vérifier l'information d'intégrité à intervalles réguliers. Documenter les processus et les résultats des vérifications de l'information d'intégrité. Mener des audits d'intégrité à la demande.	Identifier les agents humains et logiciels qui mènent des actions sur les contenus et journaliser ces actions.	Déterminer quel standard de métadonnées appliquer. Trouver et combler les lacunes dans les métadonnées pour se conformer à ces standards.	Surveiller l'obsolescence et les évolutions des technologies dont dépendent les contenus.
Niveau 4 (pérenniser vos contenus)	Posséder au moins trois copies dans des emplacements géographiques présentant des types de menaces différents. Augmenter la variété des supports de stockage pour éviter les points de défaillance uniques. Avoir un plan et mener des actions pour remédier à l'obsolescence des supports de stockage, des logiciels et du matériel informatique.	Vérifier l'information d'intégrité à la suite d'événements ou d'activités spécifiques. Remplacer ou réparer les contenus corrompus le cas échéant.	Examiner périodiquement les journaux des opérations et des accès.	Archiver les actions de préservation associées au contenu et les occurrences de ces actions. Choisir et implémenter des standards de métadonnées.	Mener des opérations de migration, de normalisation, d'émulation, etc. pour s'assurer que les contenus restent acccessibles.

DOI 10.17605/OSF.IO/QGZ98