Catégories : configuration de la plate-forme, utilisation d'une fonctionnalité Vitam

La gestion des archives classifiées avec la solution logicielle Vitam

La notion de classification dans la solution logicielle Vitam s'applique aux informations protégées au titre du secret de la défense nationale, en application de l'instruction générale interministérielle 1300 sur la protection du secret de la défense nationale.
La solution logicielle permet de déclarer les informations liées au niveau de protection des unités archivistiques et de les modifier lorsque le niveau de protection évolue dans le temps.
Elle offre également des fonctionnalités pour répondre aux obligations de cloisonnement sur des plates-formes distinctes des informations dont le niveau de protection du secret est différent, en s'assurant que le niveau de protection à accorder aux documents est cohérent avec le niveau de protection offert par la plate-forme.

Configuration des niveaux de classification de la plate-forme

De même que les archives physiques classifiées au titre du secret de la défense nationale sont conservées dans des magasins spécifiques bénéficiant de protections périmétriques et de contrôles d'accès particuliers, de même les archives électroniques bénéficiant d'une protection au titre du secret de la défense nationale doivent être conservées sur des plates-formes placées dans des environnements spécifiques assurant une protection adéquate.
Chaque plate-forme utilisant la solution logicielle Vitam peut déclarer les niveaux de protection pour lesquels elle est habilitée. Cette opération est réalisée par l'administrateur technique lors de l'installation de la plate-forme.
Les niveaux de classification sont paramétrés dans un fichier de positionnement des variables présenté dans la documentation d'installation.

```
classificationList: ["Non protégé","Secret Défense", "Confidentiel Défense"]
classificationLevelOptional: true
```

Dans l'exemple ci-dessus, la plate-forme accepte les unités archivistiques déclarant les niveaux de protection au titre du secret de la défense nationale suivants : Non protégé, Confidentiel Défense et Secret Défense. Elle accepte également les unités archivistiques ne déclarant pas de niveau de classification.

Il est possible de configurer autant de niveaux de classification que souhaité par plate-forme, en fonction des obligations réglementaires.

Il est important de bien indiquer si les unités archivistiques sans niveau de classification seront acceptées ou non. Il peut paraître préférable sur une plate-forme destinée à accueillir des informations de niveau Confidentiel Défense ou Secret Défense de ne pas accepter les unités archivistiques dont le niveau de protection est inconnu, pour des raisons de bonne gestion, mais cela signifie que tous les niveaux de l'arborescence devront porter des règles de classification, ce qui revient à classifier les pochettes de dossiers et sous-dossiers, de même que les documents qui y sont contenus. Dans la pratique, obliger à déclarer sur toutes les unités archivistiques des règles de classification peut aboutir à multiplier les procédures de déclassification et les éventuels conflits d'héritage de règles.

> Exemple : pour une structure qui dispose d'un plan de classement dans lequel sont rangés les documents au fur et à mesure de leur production ou à la fin d'une opération (opération de

maintien de la paix par exemple), si la plate-forme n'accepte pas d'unité archivistique dont le niveau de protection est inconnu, le plan de classement lui-même devra être classifié, quand bien même il ne contient pas d'autre information que « Journal des marches et opérations », « Chronos » ou « Documents comptables ». Chaque unité archivistique du plan devra déclarer un niveau de classification et un émetteur, propriétés qui pourront être héritées par les unités archivistiques rattachées.

Le niveau de protection peut varier dans le temps. Par exemple, un document sur une plate-forme Secret Défense peut être déclassé ou déclassifié. Il faut donc que la plate-forme sur laquelle il se trouve accepte des niveaux de protection inférieurs. Il est ainsi conseillé que la plate-forme qui conserve le Secret Défense puisse aussi accepter les unités archivistiques de niveau Confidentiel Défense et Non protégé et de même, la plate-forme Confidentiel Défense, les unités archivistiques de niveau Non protégé, dans l'attente de leur transfert vers la plate-forme de niveau de protection inférieur le cas échéant.

Déclaration du niveau de classification des unités archivistiques

Chaque unité archivistique prise en charge dans la solution logicielle Vitam peut déclarer dans ses métadonnées de gestion des éléments liés à sa classification (sous-bloc <ClassificationRule> du bloc <Management>) :

- un niveau de protection (balise <ClassificationLevel>),
- un émetteur de ce niveau de classification (<ClassificationOwner>),
- une date de réévaluation de la classification (<ClassificationReassessingDate>) ou une règle spécifique permettant de calculer une échéance de réévaluation de la classification (<Rule> et <StartDate>),
- ainsi que des mentions additionnelles de limitation du champ de diffusion (<ClassificationAudience>).

Le niveau de protection et l'émetteur sont obligatoires dès lors que l'unité archivistique déclare des éléments dans le sous-bloc <ClassificationRule>.

Les règles liées à la classification obéissent aux mêmes mécanismes d'héritage que les autres catégories de règles de gestion (cf. fiche Positionner des règles de gestion dans la solution logicielle Vitam). Il est toutefois recommandé de déclarer les éléments liés à la classification au niveau le plus bas de l'arborescence (niveau pièce) pour éviter qu'une unité archivistique hérite de niveaux de classification contradictoires.

Contrôle à l'entrée de l'adéquation entre le niveau de protection de la plate-forme et le niveau de protection des unités archivistiques

Un contrôle à l'entrée est effectué par la solution logicielle Vitam afin de vérifier que le niveau de protection des unités archivistiques déclaré dans le bordereau de transfert est conforme au niveau de protection apporté par la plate-forme.

La tentative d'import d'une unité archivistique dont le niveau de protection n'est pas conforme aux valeurs autorisées sur la plate-forme déclenchera une alerte de sécurité qui sera transmise à l'administrateur technique de la plate-forme. L'entrée sera alors rejetée.

Pour que ce contrôle puisse être effectué, la plate-forme doit déclarer les niveaux de classification

qu'elle peut accepter et le niveau de classification des unités archivistiques doit être précisé dans le bordereau de transfert.

Nota bene : Le niveau de protection de la plate-forme et le niveau de classification des unités archivistiques doivent être strictement équivalents : sur une plate-forme déclarant un niveau « Secret Défense », les unités archivistiques déclarant un niveau de classification « secret défense » ou « Secret Defense » par exemple seront rejetées.

Utilisation des tenants*

Il peut être intéressant sur une plate-forme accueillant des documents classifiés d'utiliser des **tenants*** pour séparer les archives électroniques en fonction de leur champ de diffusion.

> Exemple : si l'entité conserve des informations sur un support classifié qui doivent pouvoir être contrôlées par un partenaire dans le cadre d'un accord de sécurité, ces informations peuvent être versées sur un tenant distinct de celui utilisé pour les informations strictement réservées à l'entité.

Modification des informations de classification

Le niveau de classification, de même que les autres éléments du bloc <ClassificationRule>, peut faire l'objet d'une modification pour tenir compte des évolutions du niveau de protection de l'unité archivistique.

Cette opération de modification peut être faite de manière unitaire ou en masse.

Toute modification du niveau de classification porté en propre par l'unité archivistique entraîne une historisation en base de données des données du bloc <ClassificationRule> et la création d'une nouvelle version de l'unité archivistique dans le journal du cycle de vie.

La mise à jour des propriétés et règles spécifiques doit respecter le modèle de données. Ainsi, il n'est pas possible de supprimer uniquement le champ <Classification Level> ou le champ <ClassificationOwner> qui sont des champs obligatoires dans le bloc <ClassificationRule>.

Comme à l'entrée, un contrôle est effectué sur l'adéquation entre le niveau de classification accepté par la plate-forme et le niveau déclaré par l'unité archivistique. Si le niveau déclaré n'est pas conforme aux valeurs attendues par la plate-forme, la modification sera en échec.

La configuration de la plate-forme peut ne pas permettre la présence d'unités archivistiques sans niveau de classification.

En cas de réévaluation du niveau de classification conduisant à rehausser le niveau de protection d'un document au-delà du niveau de protection autorisé pour la plate-forme, il conviendra de changer d'abord le document de plate-forme avant de modifier son niveau de classification pour que la modification ne soit pas rejetée.

Constitution du registre des documents classifiés

Il est recommandé de constituer un registre des informations sur support classifié en dehors de la solution logicielle Vitam. Ce registre pourra permettre de faire un récolement annuel des documents classifiés présents sur la plate-forme par rapport à un état extérieur.

Pour cela, il convient de lancer périodiquement une requête recherchant parmi les dernières opérations d'entrée les unités archivistiques déclarant une règle de classification et remontant toutes

les informations utiles pour l'alimentation du registre : identifiant système, titre, numéro d'enregistrement, niveau de classification, émetteur de la classification, volumétrie des **objets techniques*** liés…

Récolement des documents classifiés

La fonctionnalité d'**audit d'existence*** permet de s'assurer périodiquement de la présence des documents classifiés sur la plate-forme.

Pour cela, il convient de lancer un audit d'existence à partir des identifiants système des unités archivistiques listés dans le registre des documents classifiés que l'administrateur fonctionnel aura constitué.