

# La gestion de l'information dans Teams

18 novembre 2022





## Table des matières

Introduction.....	5
1. Mise en place d'une gouvernance Teams.....	6
1.1 Établir une norme de stockage.....	7
2. Sécurité de l'information dans Teams .....	8
2.1 Déterminer les niveaux de confidentialité des documents.....	8
2.2 Définir les mesures de protection en fonction des niveaux de confidentialité des documents ....	9
2.3 La gestion des niveaux de confidentialité et la protection de l'information dans Microsoft 365	11
3. Règles de gestion d'une équipe Teams.....	11
3.1 Déterminer une stratégie de déploiement pour les clientèles cibles.....	12
3.2 Déterminer les règles à mettre en place pour la création des équipes Teams .....	12
3.3 Déterminer une architecture d'information pour les équipes Teams.....	13
3.4 Définir une convention de nommage des équipes Teams .....	15
3.5 Mise en place d'un plan de gestion du cycle de vie des équipes Teams .....	17
4. Conservation de l'information dans Teams .....	17
4.1 Règles de conservation pour les documents.....	18
4.2 Règles de conservation pour les conversations.....	18
4.3 Règles de conservation pour les enregistrements de réunions .....	19
4.4 Règles de conservation pour les plans de projets et les tâches .....	19
4.5 Règles de conservation pour les autres objets.....	19



## Introduction

Un groupe de travail du Sous-comité des archivistes (SC-A) du BCI a établi des principes directeurs et des paramètres pour la gestion de l'information institutionnelle dans Microsoft Teams ainsi que des balises pour son utilisation. Sans une gestion appropriée de Teams, les équipes Teams risquent de se multiplier de façon exponentielle, ce qui pourrait poser notamment des problèmes de repérage et de sécurité et engendrer des coûts supplémentaires pour le stockage des données.

Microsoft 365 étant le produit le plus utilisé dans les établissements universitaires québécois, ce chapitre porte sur la gestion de l'information dans Teams. Ces recommandations pourraient toutefois très bien s'appliquer à d'autres plateformes de collaboration similaires.

Ainsi, le SC-A émet des recommandations concernant les quatre (4) aspects suivants :

### Mise en place d'une gouvernance Teams

Pour l'établissement et la mise en place d'une gouvernance Teams, les recommandations portent sur la nécessité de considérer le cadre législatif et réglementaire existant, la définition de règles spécifiques qui tiennent compte des particularités de la plateforme, la nécessité d'un comité de gouvernance, ainsi que l'importance d'impliquer les bonnes parties prenantes et de définir clairement leurs rôles et responsabilités.

### Sécurité de l'information dans Teams

En matière de sécurité et de protection de l'information, les recommandations comprennent l'élaboration d'une norme de stockage, l'établissement d'une classification définissant des niveaux de confidentialité pour les renseignements contenus dans les documents et la mise en place de mesures de sécurité basées sur des fonctionnalités de Microsoft 365.

### Règles de gestion d'une équipe Teams

En vue de gérer efficacement une équipe Teams depuis sa création jusqu'à son archivage ou sa destruction, le SC-A émet des recommandations qui permettent de maintenir l'organisation et la cohérence des équipes dans Teams, ce qui inclut notamment les éléments à intégrer dans un plan de gestion du cycle de vie et dans un plan de fermeture d'une équipe Teams.

### Conservation de l'information dans Teams

Comme dans toute plateforme permettant le stockage de documents, des règles établissant des délais de conservation en fonction de la nature des informations doivent être mises en place. Les recommandations à ce sujet portent notamment sur les durées de conservation des documents, des conversations et des enregistrements de réunions stockés dans Teams.

## 1. Mise en place d'une gouvernance Teams

Pour assurer une gestion de l'information efficiente et optimale dans Teams, il est essentiel d'établir et de mettre en œuvre un plan de gouvernance qui déterminera l'utilisation de Teams (collaboration et/ou gestion documentaire) et les rôles et responsabilités des parties prenantes. Ce plan doit évidemment s'arrimer à la gouvernance informationnelle en place dans l'institution. L'utilisation de Teams comporte de nombreux avantages tels que l'augmentation de la productivité, la facilitation du travail collaboratif, l'accélération de la transformation numérique et l'utilisation de fonctionnalités permettant le stockage de données conforme et sécuritaire. Toutefois, afin de garder le contrôle sur le volume d'information utilisé dans Teams, il est impératif de mettre sur pied un plan de gouvernance.

Conformément aux exigences du cadre législatif<sup>1</sup>, la plupart des établissements universitaires disposent déjà de politiques, règlements et directives encadrant la collecte, le stockage, la gestion, l'utilisation, la transmission, la protection, la conservation et l'élimination de l'information institutionnelle, quel que soit le système dans lequel elle est stockée et exploitée. Au fil des années, les services d'archives universitaires ont également développé différents guides et outils pour assurer une saine gestion de l'information, dont les plus importants sont le plan de classification, le calendrier de conservation et la catégorisation des actifs informationnels. Il est clair que le cadre législatif et réglementaire ainsi que plusieurs des outils existants s'appliquent aussi à Teams. Cependant, l'utilisation d'une plateforme de collaboration pose des défis particuliers et il est nécessaire que des règles spécifiques soient définies et déployées. Ces règles concernent principalement la protection, l'organisation et la destruction en temps utile de l'information.

Au besoin, un comité de gouvernance peut être mis sur pied. Cependant, la gouvernance Teams peut également être assurée par un comité déjà en place dans l'institution (par exemple, un comité de gestion de l'information). En plus de définir les principes directeurs, le comité devra s'assurer que les parties prenantes clés soient clairement identifiées et mises à contribution. En effet, pour s'assurer de couvrir tous les volets de la gestion de l'information dans Teams, l'institution doit pouvoir compter sur une équipe multidisciplinaire d'expertes et experts, lesquelles et lesquels doivent intervenir le plus tôt possible dans le processus, idéalement en amont des projets. En plus des archivistes, devront notamment être impliqués des spécialistes en technologie de l'information, des conseillères et conseillers juridiques, des conseillères et conseillers en conformité et gestion de risques ainsi que des représentantes et représentants des unités propriétaires des données. Un des facteurs de succès de la mise en œuvre d'un plan de gouvernance Teams sera de bien déterminer les rôles et responsabilités de ces différentes parties prenantes.

---

<sup>1</sup> *Loi sur les archives*, R.L.R.Q. c. A-21.1; *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, R.L.R.Q., c. A-2.1; *Loi concernant le cadre juridique des technologies de l'information*, R.L.R.Q., c. C-1.1.

## 1.1 Établir une norme de stockage

Les établissements universitaires mettent à la disposition du corps étudiant et des membres du personnel plusieurs plateformes et solutions technologiques pour le stockage de l'information numérique : environnements numériques d'apprentissage, serveurs de fichiers, solutions infonuagiques (dont Microsoft 365), wikis et autres. Ces multiples options peuvent créer de la confusion chez l'utilisatrice ou utilisateur lorsque vient le temps d'enregistrer un document. Ainsi, l'établissement d'une norme de stockage permettra à chacune et chacun de déterminer facilement la meilleure façon et le meilleur endroit pour enregistrer ses documents.

Les objectifs de cette norme sont les suivants :

- Identifier quel type d'espace de stockage devrait être utilisé pour répondre à chacun des besoins ;
- Fournir des consignes quant à l'utilisation de diverses solutions ;
- Assurer la protection des renseignements personnels ou sensibles ;
- Assurer l'utilisation efficiente des diverses solutions tout en suivant les meilleures pratiques développées dans le domaine universitaire ;
- Assurer le respect des lois et règlements en vigueur et limiter les risques liés à l'utilisation non appropriée de l'information ;
- Définir des règles pour le stockage de l'information institutionnelle en infonuagique.

### Exemples d'application

La mise en place d'une norme de stockage permet aux membres des comités de gestion et aux personnes décideuses de mieux comprendre l'importance et le rôle des différentes plateformes de stockage. Il peut s'agir d'un levier pour l'établissement d'autres règles de gouvernance liées à la gestion et à la sécurité de l'information.

La norme de stockage peut découler de l'adoption d'une politique portant sur la gestion et la sécurité de l'information ou encore de la catégorisation des actifs informationnels.

## 2. Sécurité de l'information dans Teams

### 2.1 Déterminer les niveaux de confidentialité des documents

Le caractère confidentiel des documents varie largement en fonction de la nature des renseignements qu'ils contiennent. Certains sont de nature publique dès qu'ils sont achevés et publiés, comme les communiqués de presse ou un calendrier universitaire. D'autres, en revanche, contiennent des renseignements personnels ou confidentiels, lesquels ne doivent être accessibles qu'à des personnes spécifiques, comme un dossier de membre du personnel ou une entente en cours de négociation.

Pour être en mesure d'évaluer le degré de confidentialité des documents, il est recommandé d'établir une charte comportant différents niveaux de confidentialité déterminés en fonction des risques et de l'impact d'une divulgation non autorisée. Une fois définie, cette charte peut être appliquée aux outils de gestion documentaire comme le calendrier de conservation et/ou le plan de classification, pour que chaque série documentaire ou type de document se voie attribuer un niveau de confidentialité. En l'absence de tels outils, il est possible de procéder à un inventaire des documents pour chacune des unités. La catégorisation des actifs informationnels se définit comme le « processus permettant à l'organisme d'évaluer le degré de sensibilité de son information, dans le but d'en déterminer le niveau de protection eu égard aux risques encourus en matière de disponibilité, d'intégrité et de confidentialité (DIC) »<sup>2</sup>. Le livrable résultant de cette catégorisation est un exemple de charte<sup>3</sup>.

Évidemment, il est important que la charte de confidentialité soit simple afin que les utilisateurs puissent la comprendre et l'appliquer facilement.

La norme ISO 27001<sup>4</sup> suggère d'inclure quatre niveaux de classification dans la charte des niveaux de confidentialité :

1. Confidentiel (seulement les cadres supérieures et supérieurs y ont accès) ;
2. Restreint (la plupart des membres du personnel y ont accès) ;

---

<sup>2</sup> Secrétariat du Conseil du trésor, Guide de catégorisation de l'information, 2016, p.1.

[https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources\\_informationnelles/securete\\_information/categorisation\\_information.pdf](https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securete_information/categorisation_information.pdf)

<sup>3</sup> Il est important de noter qu'une telle charte couvre davantage que les simples aspects de confidentialité.

<sup>4</sup> Organisation internationale de normalisation. (2013), *ISO/IEC 27001 – Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences*. (ISO/IEC 27001), en ligne : <https://www.iso.org/fr/standard/54534.html>



3. Interne (l'entièreté des membres du personnel y a accès) ;
4. Information publique (tout le monde y a accès).

La classification des informations, qui comprend généralement trois (3) ou quatre (4) niveaux de confidentialité, est l'un des éléments clés pour garantir une protection adéquate de l'information. Il revient à chaque organisation de définir le niveau de granularité adéquat pour la protection de ses actifs informationnels. Cependant, il ne faut pas perdre de vue que plus le nombre de niveaux est réduit, plus les moyens de contrôle de sécurité de l'information sont diminués. À l'opposé, trop d'options de classification risquent d'embrouiller les utilisatrices et utilisateurs et de complexifier la gestion de l'information.

Il est important de déterminer les niveaux de confidentialité des documents afin d'appliquer pour chacun d'eux les mécanismes de sécurité appropriés.

#### Liens utiles

*What is ISO 27001 information classification ? (en anglais)*

<https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001>

En savoir plus sur la classification des données (documentation Microsoft)

<https://docs.microsoft.com/fr-ca/microsoft-365/compliance/data-classification-overview?view=o365-worldwide>

*Guidance on Information Confidentiality Classification, University of Waterloo (en anglais)*

<https://uwaterloo.ca/records-management/policy-46-guide/guidance-information-confidentiality-classification>

Guides de référence du Secrétariat du Conseil du trésor

<https://www.tresor.gouv.qc.ca/ressources-informationnelles/securite-de-linformation/directive-sur-la-securite-de-linformation-gouvernementale/guides-de-reference/>

## 2.2 Définir les mesures de protection en fonction des niveaux de confidentialité des documents

Les mesures de protection de l'information doivent être établies en fonction du niveau de confidentialité d'un document. En effet, il n'est pas nécessaire de protéger un communiqué de presse public, mais il en est tout autrement pour le dossier de membre

du personnel qui comprend de nombreux renseignements personnels. Les mesures de protection peuvent inclure les éléments suivants :

- Chiffrement pour les données en transit et/ou au repos ;
- Protection de documents par mot de passe ;
- Droits d'accès accordés en fonction de l'unité académique ou administrative d'appartenance.

Une norme de traitement des données devrait également être mise en place. Elle établit les rôles et responsabilités ainsi que les mécanismes de contrôle pour le traitement de toutes les informations gérées par l'établissement universitaire. Pour chaque niveau de confidentialité, cette norme devrait inclure des dispositions suivantes :

- Le lieu de stockage des documents numériques ;
- Le moyen utilisé pour la transmission de l'information ;
- L'indication du niveau de confidentialité dans les métadonnées du document, ou encore dans l'en-tête et/ou le pied de page de chaque document ;
- La méthode de destruction des documents numériques.

Les technologies de l'information étant en constante évolution, il est essentiel d'assurer une veille en continu et d'adapter aux besoins contemporains les moyens et les solutions mis en place en vue d'assurer la sécurité de l'information.

#### **Exemples d'application**

La charte des niveaux de confidentialité et les mesures de protection de l'information peuvent être intégrées dans un seul document afin de faciliter leur utilisation par les usagers et usagers.

Le plan de classification et le calendrier de conservation peuvent également être mis à jour pour inclure des indications sur les niveaux de confidentialité des documents.

#### **Liens utiles**

*Data Handling Standard, California State University, Fresno (en anglais)*  
<https://technology.fresnostate.edu/documents/DataHandlingStandard.pdf>

## 2.3 La gestion des niveaux de confidentialité et la protection de l'information dans Microsoft 365

Microsoft 365 offre une multitude de services et de fonctionnalités pour assurer la protection de l'information. Les détails sont disponibles sur le site web de Microsoft :

<https://docs.microsoft.com/fr-ca/microsoft-365/compliance/information-protection?view=o365-worldwide>

Les étiquettes de confidentialité dans Microsoft 365 permettent d'établir facilement les niveaux de sécurité et les mesures de protection selon le type de document. Les détails sont disponibles sur le site web de Microsoft :

<https://docs.microsoft.com/fr-ca/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

## 3. Règles de gestion d'une équipe Teams

Toutes les équipes Teams suivent le même cycle de vie, lequel comporte trois phases : création, maintenance et fermeture. Les recommandations de la présente section précisent les éléments essentiels à inclure dans un plan de gestion des équipes Teams. Ce plan tient compte des enjeux de sécurité et de conservation de l'information.

L'un des principaux enjeux soulevés par les institutions est la difficulté de maintenir l'organisation et la cohérence des équipes dans Teams. Le SC-A émet des recommandations pour résoudre les problèmes typiques rencontrés, dont voici quelques exemples :

- La prolifération des équipes Teams et de l'espace requis pour stocker leurs contenus ;
- L'absence d'une convention de nommage ;
- L'absence d'une architecture d'information standardisée ;
- Les membres inactives ou inactifs qui demeurent rattachées ou rattachés à des équipes Teams ;
- Les équipes Teams qui demeurent ouvertes malgré leur inactivité ;
- Les équipes Teams qui sont « orphelines », car elles n'ont plus de propriétaire.

### Liens utiles

Documentation de Microsoft sur les règles de gouvernance Teams (en anglais)

<https://docs.microsoft.com/en-us/microsoftteams/teams-overview>

*Governance quick start for Microsoft Teams* (en anglais)

<https://docs.microsoft.com/en-us/microsoftteams/teams-adoption-governance-quick-start>

*Governance for Microsoft Teams: A to Z—Jasper Oosterveld (MVP Microsoft) (en anglais)*  
<https://www.youtube.com/watch?v=oeTzsdWWDkA>

### 3.1 Déterminer une stratégie de déploiement pour les clientèles cibles

Une des premières étapes d'un projet Microsoft 365 est de déterminer quelles sont les clientèles cibles et quels sont les besoins spécifiques à chacune. Par la suite, une stratégie de déploiement pour chaque clientèle identifiée doit être établie et des règles de gestion des équipes Teams applicables doivent être définies. Par exemple :

#### Éudiantes et étudiants

Laisser la création de sites en libre-service, mais activer une règle d'expiration sur les sites afin que ceux-ci soient automatiquement détruits après une certaine durée d'inactivité.

#### Membres du personnel

Contrôler la création des sites afin de pouvoir gérer efficacement l'information au sein de l'institution. En effet, le contrôle des sites permet de mettre en place différentes règles de gestion, incluant des règles de gestion documentaire et d'autres options qui peuvent être intégrées dans le plan de gestion des sites.

### 3.2 Déterminer les règles à mettre en place pour la création des équipes Teams

Une fois la stratégie de déploiement définie pour chaque clientèle et afin d'éviter la prolifération des équipes Teams, il est recommandé de mettre en place des règles pour encadrer et contrôler la création des sites :

- Il est possible de ne pas laisser la création des équipes Teams en libre-service auprès de toutes les utilisatrices et tous les utilisateurs. Pour ce faire :
  - Définir parmi les clientèles cibles lesquelles seront autorisées à créer des équipes en libre-service ;
  - Retirer l'accès à la création d'équipes pour les autres clientèles.
- Pour les clientèles qui ne détiennent pas les permissions requises pour créer des sites, un formulaire de demande de création de sites peut être mis en place. Une fois complété, le document pourrait être acheminé à des super utilisatrices ou utilisateurs responsables de créer les sites, qui s'assureront de valider les éléments suivants avant de procéder :

- Un site similaire existe-t-il déjà ? Ou encore, existe-t-il un canal dans un site actif qui répond au même besoin ?
- Les critères requis pour la création d'un site sont-ils respectés ? (Voir le point 3.3)
- Si les critères sont respectés, la super utilisatrice ou le super utilisateur crée le site dans SharePoint à partir d'un modèle normalisé, puis crée l'équipe Teams et s'assure que les conditions suivantes soient remplies :
  - Le site est nommé en respectant la convention de nommage de l'organisation (voir le point 3.4) ;
  - Une ou un propriétaire de site et une ou un propriétaire secondaire sont bien nommés ou nommées ;
  - Les étiquettes de confidentialité sont bien appliquées (si cette fonction est activée dans l'organisation). Il est possible d'avoir plus d'une étiquette de confidentialité par équipe Teams.
  - Les règles de conservation sont appliquées.

#### Liens utiles

Documentation de Microsoft « Gérer les personnes autorisées à créer des groupes Microsoft 365 »

<https://docs.microsoft.com/fr-ca/microsoft-365/solutions/manage-creation-of-groups?view=o365-worldwide>

## 3.3 Déterminer une architecture d'information pour les équipes Teams

### Typologie des équipes Teams de l'organisation

Les contenus utilisés dans une équipe Teams sont majoritairement stockés dans un site SharePoint associé.

Il existe deux types de sites SharePoint : les sites de communication et les sites d'équipe ou de collaboration. C'est le type site d'équipe SharePoint qui est associé aux équipes Teams. Le type site d'équipe dans Teams se décline également en plusieurs sous-types selon la licence que possède l'organisation, c'est-à-dire une licence pour entreprise ou pour l'éducation).

Puisque chaque type d'équipe Teams a une vocation et des outils dédiés, il est important de définir les besoins et usages afin de mieux supporter les utilisatrices et utilisateurs :

- Déterminer quel type d'équipe Teams répond le mieux aux besoins des différentes clientèles, par exemple :
  - Équipes Teams « Éducation » :
    - Site de classe (corps enseignant) ;
    - Site de communauté de pratique ;
    - Site de département (personnel) ;
    - Site « Autres » : site étudiant, etc.
  - Équipes de collaboration « Autres », pour travailler, collaborer ou communiquer :
    - Site de direction et service ;
    - Site de projet ;
    - Site de comité.
- Définir les critères requis pour la création des sites, et ce, par type de sites, afin que les personnes autorisées à en créer disposent d'une aide à la décision quand une nouvelle demande est reçue.

### **Structure d'information dans les équipes Teams de l'organisation**

Le fait de normaliser les équipes Teams permet d'en simplifier la gestion, de faciliter le travail des super utilisatrices et utilisateurs et de favoriser l'adaptation des utilisatrices et utilisateurs.

- Pour chaque type de site, il est recommandé de concevoir un modèle qui servira pour la création de nouveaux sites et qui comprendra tous les éléments à normaliser :
  - Quels seront les onglets (outils) de base : Publications, Fichiers, Calendrier, Tâches, etc.
  - Comment seront structurées les bibliothèques de documents (Fichiers) ?
  - Comment sera arrimé le cycle de vie du site ?
  - Comment sera arrimée la gestion documentaire du site ?

### **Liens utiles**

Documentation de Microsoft sur les types d'équipes Teams Éducation

<https://support.microsoft.com/fr-fr/topic/choisir-un-type-d-%C3%A9quipe-%C3%A0-des-fins-de-collaboration-dans-microsoft-teams-0a971053-d640-4555-9fd7-f785c2b99e67>

Documentation de Microsoft sur la gestion documentaire dans les sites  
<https://support.microsoft.com/fr-fr/office/create-and-apply-information-management-policies-eb501fe9-2ef6-4150-945a-65a6451ee9e9>

Documentation de Microsoft sur l'utilisation de modèles pour créer les sites  
<https://docs.microsoft.com/en-us/microsoftteams/create-a-team-template>  
<https://support.microsoft.com/en-us/office/apply-and-customize-sharepoint-site-templates-39382463-0e45-4d1b-be27-0e96aeec8398>

### 3.4 Définir une convention de nommage des équipes Teams

La création d'une équipe Teams entraîne automatiquement la création d'un site SharePoint pour le stockage, d'un groupe de sécurité 365 et d'une adresse courriel dédiée au groupe. Le fait de ne pas encadrer la création des sites peut entraîner une prolifération des sites, des groupes de sécurité ainsi que des boîtes courriel et faire en sorte que les noms attribués soient plus ou moins significatifs ou compréhensibles.

Une fois le nom du site (URL) enregistré, il est possible de modifier le titre s'affichant sur la « tuile » dans la section « Équipes » de Teams, de façon à le rendre plus convivial.

Exemple : Sites Teams et groupes 365 correspondant sans convention de nommage			
Nom du site ↑ ↓	URL ↓	Nom du groupe ↑	Adresse de courriel du groupe
Tableau des présences (test)	.../sites/tableau	Tableau des présences (test)	: tableau @
Task force	.../sites/taskforce	Task force	: taskforce@
test	.../sites/test2	test	: test863@

#### Recommandations pour structurer les noms (URL) des sites

- Débuter le nom des sites par un préfixe correspondant au type de site (exemples : [ADM], [COURS], [ÉTUDIANT]). Cette façon de faire a pour avantages de regrouper et de différencier facilement les différents sites, en plus de permettre aux administratrices et administrateurs d'effectuer des recherches et de tenir des statistiques basées sur les types de sites.
- Ajouter des éléments normalisés obligatoires définis en fonction du type de site. Par exemple : nom du service [SERVICE] pour un site administratif ou sigle du cours [GRH1345] pour un site de classe.
- Ajouter d'autres informations jugées pertinentes, en respectant un nombre maximal de caractères.

### Exemple d'une convention de noms de sites

Types de site	Convention	Résultat
Sites des étudiant.e.s	[ÉTUDIANT]-[NOM-PRENOM]-[LIBRE]	ETUDIANT-Tremblay-Stephane-Mon_site
Site de cours	[COURS]-[SIGLE DU COURS]-[SESSION-ANNEE]-[ENSEIGNANT]-[NO GROUPE]	COURS-GRH1345-H2022-Laverdiere-Gr21
Site de direction Site de service	[ADM]-[ACRONYME DE LA DIRECTION] [ADM]-[ACRONYME DU SERVICE]	ADM-DA ADM-SRM
Site de comité	[COMITÉ]-[ACRONYME OU NOM DU COMITÉ]	COMITE-CA
Site de projet	[PRJ]-[SERVICE RESPONSABLE]-[ACRONYME OU NOM DU PROJET]	PRJ-RI-M365

L'utilisation d'une convention de nommage facilite grandement le repérage pour les utilisatrices et utilisateurs ainsi que la gestion des sites pour les administratrices et administrateurs.

Une licence Azure Premium ou Azure basic EDU permet de forcer les règles de nommage des sites. Cependant, en utilisant cette fonctionnalité, l'URL et le titre d'un site seront identiques. Seule une personne ayant le rôle d'administratrice globale ou administrateur global de la console Microsoft 365 pourra nommer les sites librement. Malgré ces contraintes, le fait que le système impose des règles de nommage aux utilisatrices et utilisateurs permet de diminuer le temps requis pour la création des sites et pour le monitoring.

Pour les établissements universitaires qui ont un très grand nombre de sites, il est possible d'utiliser Power Automate, Power Apps et Azure pour mettre en place un système de création de sites en libre-service. Ce système inclut une convention de nommage qui fonctionne automatiquement. Évidemment, l'utilisation de ces logiciels demande un certain investissement en ressources humaines et financières, mais celui-ci pourra être rapidement rentabilisé en raison du temps qu'il permet d'économiser pour le déploiement et la maintenance de Microsoft 365.

#### Liens utiles

Documentation de Microsoft sur la convention de nommage de sites Teams/SharePoint et des groupes 365

<https://docs.microsoft.com/fr-ca/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide>



### 3.5 Mise en place d'un plan de gestion du cycle de vie des équipes Teams

Les sites inactifs consomment de l'espace et des ressources inutilement puisqu'ils sont inutilisés. Afin de les contrôler, ainsi que pour s'assurer que les sites comprenant des documents institutionnels soient archivés, il est recommandé de mettre en place des règles permettant de gérer le cycle de vie des sites.

- Dans la console Azure de Microsoft 365, il est possible d'activer une règle d'expiration des sites. Celle-ci peut être configurée selon les besoins. En voici un exemple : *Après 365 jours, envoyer automatiquement une demande de destruction ou de renouvellement de site au propriétaire.*
- Il est recommandé d'utiliser les fonctionnalités offertes par Microsoft 365 ou celles d'une application tierce pour incorporer la gestion documentaire dans les équipes Teams. Ceci permettra notamment de mieux organiser l'information et de gérer le cycle de vie des contenus. Parmi les actions possibles, mentionnons :
  - A. Utiliser le plan de classification et le calendrier de conservation dans les sites ;
  - B. Effectuer un déclassement annuel des contenus dans les sites : détruire les contenus qui ont atteint leur fin de vie et archiver les contenus à conservation longue ou permanente ;
  - C. Archiver (si pertinent) et fermer les canaux des équipes Teams qui ne sont plus utiles ;
  - D. Archiver et fermer complètement le site (dans le cas d'un projet complété, par exemple).

#### Liens utiles

Documentation de Microsoft sur l'expiration des sites

<https://docs.microsoft.com/fr-ca/microsoft-365/solutions/microsoft-365-groups-expiration-policy?view=o365-worldwide>

Documentation de Microsoft sur le « *records management* » dans Microsoft 365 (en anglais)

<https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide>

## 4. Conservation de l'information dans Teams

Dans Teams, il est recommandé d'établir les durées de conservation selon les types d'objets en établissant des règles pour gérer la durée de vie des documents, des conversations, des enregistrements de réunions et des plans de projets et des tâches.

## 4.1 Règles de conservation pour les documents

Les documents doivent être conservés aussi longtemps que requis pour documenter les activités de l'établissement universitaire. Quels que soient leur format ou support (numériques, papier ou autres) et l'endroit où l'information est stockée (Teams, serveur de fichier, wiki, classeur pour les documents papier, etc.), les documents doivent avoir des durées de conservation normées. La durée de vie des documents est déterminée en fonction de leur contenu par le Calendrier de conservation de l'établissement universitaire.

Dans Microsoft 365, la console de gestion de la sécurité et de la conformité permet de paramétrer les règles de conservation. Idéalement, la ou le gestionnaire de document doit donc avoir accès à cette console.

### Liens utiles

Console de sécurité et conformité de Microsoft 365 (en anglais)

<https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-securitycompliance-center>

Création de règles de conservation dans Teams

<https://docs.microsoft.com/fr-ca/microsoftteams/retention-policies>

## 4.2 Règles de conservation pour les conversations

Outre le partage et l'enregistrement des documents, Teams permet d'échanger par clavardage (*chat* en anglais) et stocke les conversations automatiquement. Ces conversations doivent être de nature éphémère. En effet, toutes les informations qui documentent les activités de l'établissement universitaire et les prises de position doivent passer par un autre médium (par exemple, les courriers électroniques) et être conservées aussi longtemps qu'elles sont requises, conformément au Calendrier de conservation des documents de l'établissement universitaire.

Puisque les conversations Teams sont de nature éphémère, il est recommandé de les détruire après un certain temps, au maximum un (1) an. Ce laps de temps peut différer d'un établissement universitaire à un autre, en fonction des besoins.

La console de sécurité et de conformité permet de paramétrer la durée de la conservation des conversations dans Teams.

### **4.3 Règles de conservation pour les enregistrements de réunions**

Teams permet maintenant d'enregistrer les réunions. Contrairement aux conversations qui sont stockées automatiquement, les enregistrements des réunions se font manuellement par une personne présente à la rencontre.

Les enregistrements de réunions pour les instances et comités officiels devraient être détruits une fois le procès-verbal approuvé et signé.

Les enregistrements des autres réunions sont considérés comme des documents éphémères et devraient être détruits dès que possible. L'idéal est de créer une règle d'affaires déterminant la durée de conservation de l'enregistrement des réunions.

### **4.4 Règles de conservation pour les plans de projets et les tâches**

Microsoft 365 comprend un outil de gestion de projets et de tâches intégré notamment à Teams, nommé Planner (Tâches ou *Tasks* en anglais dans Teams).

Il est recommandé aux utilisatrices et utilisateurs qui ont recours à Planner dans Teams d'exporter leur plan de gestion de projet en format Excel, une fois le projet en question terminé, et de l'enregistrer dans leur dossier d'affaire avec les autres documents liés au projet. Une fois cette étape complétée, les plans dans Planner doivent être éliminés afin d'éviter qu'ils ne s'y s'accumulent.

### **4.5 Règles de conservation pour les autres objets**

Les documents, les conversations, les enregistrements de réunions et les plans de projets sont les éléments de base, mais Teams peut s'intégrer à plusieurs autres applications. Si ces applications sont utilisées par l'organisation, il serait important de définir des règles de conservation spécifiques pour les autres types d'objets qui sont créés.

Γ Γ

**BCI** ┘