



5 étapes pour une bonne gouvernance

Comment les documents autogérés peuvent simplifier la gouvernance
des informations

Soyons honnêtes : la gouvernance des informations ne vous passionne probablement pas.

C'est justement pour cela qu'elle devrait être mise en place de façon efficace et transparente, afin que vos employés se concentrent sur des objectifs plus motivants d'innovation et de croissance de l'activité.

ÉTAPE 1.

Étape 1 : Ne le reportez pas à demain, passez à l'action.

Les entreprises évitent la question de la gouvernance des informations pour de nombreuses raisons. Elles ont pourtant beaucoup de raisons de s'y atteler.

Les solutions de gestion de contenu modernes et centralisées dans le cloud (avec des documents autogérés) peuvent rendre la conformité plus intuitive pour les employés, et permettre une collaboration sécurisée.

En d'autres termes, une conformité facilitée permet une réelle collaboration sécurisée.



Raison pour ne pas aborder la gouvernance :

"Les outils existants/ antérieurs sont complexes et génèrent des coûts d'entretien élevés."

"Nos employés devraient pouvoir se concentrer sur le développement de l'entreprise, et non sur les problèmes de conformité."

"Il est difficile de gérer les différents types de contenu sur l'ensemble des périphériques et des plates-formes."



Une très bonne raison d'aborder le sujet :

Créez un système d'enregistrement transparent sans interruption des flux de travail.

- Pas d'archives papier
- Une solution centralisée

Protégez-vous contre le partage non autorisé.

- Un employé sur quatre charge des données sensibles dans le cloud
- Un fichier sur trois est partagé avec un utilisateur qui n'est pas le propriétaire

Moins de problèmes et de risques.

- Protection des ressources/ données de l'entreprise.

Étape 2 : Impliquez toutes les parties prenantes.

Confier la gestion de la gouvernance des informations à une seule personne au sein de votre organisation est certes une bonne idée. Mais vous aurez certainement besoin de convaincre plusieurs responsables de votre organisation, chacun avec un intérêt et des besoins spécifiques.



Gestionnaires de la conformité et des archives :

Assurez un suivi des réglementations et des politiques internes les plus importantes en matière de conformité et de conservation de la documentation.



Équipe juridique :

Surveillez les besoins en termes de preuves électroniques pour réduire au minimum les coûts et les risques juridiques.



Informatique et sécurité :

Confirmez les niveaux de classification de sécurité et d'autres exigences concernant la protection des documents sensibles.



Utilisateurs finaux :

Préservez leur capacité à accomplir des tâches en éliminant les problèmes liés à la sécurité, à la gouvernance et aux exigences en termes de conformité.

Étape 3 : Déterminez quels contenus peuvent être autogérés.

Les documents autogérés protègent le contenu sensible en appliquant automatiquement les règles pertinentes que vous mettez en place. Vous pouvez personnaliser ces règles avec des niveaux de classement spécifiques, des durées de conservation et des délais avant suppression, des règles de partage externe, des conservations légales, etc.

Voici une liste de vérification pratique pour personnaliser vos politiques de gouvernance de contenu.

■ Niveaux de classification :
Choisissez parmi plusieurs niveaux, chacun associé à une politique de sécurité spécifique.

■ Règles de conservation :
Définissez une période donnée de conservation du contenu, et établissez des actions pour supprimer le contenu après la période de conservation.

■ Politique de suppression des données :
Déterminez qui est autorisé à supprimer de façon permanente les éléments de la corbeille, et mettez en place un archivage automatique des e-mails relatifs aux activités utilisateur.

■ Accès aux documents :
Définissez les politiques de partage avec des listes blanches et des listes noires de collaboration.

■ Assistance dans le processus de demande de preuves électroniques :
Mettez en place des conservations légales pour préserver le contenu lors de procédures de preuves électroniques (eDiscovery), et conservez des journaux d'audit des modifications de contenu par les employés.

■ Sécurité des périphériques :
Exigez le chiffrement des terminaux pour l'accès aux contenus, restreignez l'accès aux seuls appareils d'entreprise, et contrôlez l'accès aux contenus mobiles.

■ Politique de conformité :
Configurez des politiques en conformité avec les réglementations applicables dans votre domaine d'activité ainsi que le Règlement Général sur la protection des données (GDPR).

ÉTAPE 4.

Étape 4 : Faites simple.

La simplicité est une stratégie de gouvernance des informations parfaitement valable. Un partage de fichiers simple et sécurisé permet effectivement à vos employés de se concentrer sur leurs objectifs commerciaux, qu'il s'agisse du recrutement de nouveaux clients ou de la mise sur le marché d'innovations révolutionnaires.

Voici comment les entreprises visionnaires maintiennent une gouvernance simple et transparente :

Documents autogérés.

Ils facilitent la conservation pour les utilisateurs et les administrateurs. Il n'y a plus besoin de migrer les fichiers vers un répertoire/ système de conservation distinct. Votre règle de conservation s'applique simplement à chaque document, même si un utilisateur en déplace un accidentellement dans un autre emplacement.

Preuves électroniques.

Les conservations légales sont mises en œuvre sans aucune conséquence sur les utilisateurs, et sans aucune action requise de leur part.

Indicateurs de classement.

Des signaux visuels permettent aux employés d'identifier les données sensibles de leur document. Si un fichier dépasse un seuil donné de confidentialité, son partage externe est automatiquement bloqué, pour soulager l'utilisateur de cette tâche.

Box Governance offre une solution de prévention des pertes de données (DLP) simple et efficace. Ce service nous permet d'établir des listes blanches et noires de domaines, ce qui s'avère incroyablement utile en termes de collaboration.

— Paul Falor, DSI,
North Highland Consulting

En tant que compagnie d'assurance, nous traitons beaucoup d'informations sensibles. Il est impressionnant de constater à quel point la classification de sécurité nous permet de classer des fichiers sensibles à grande échelle, et de les protéger tout en appliquant des règles de partage qui éduquent nos utilisateurs.

— Jon Wooten, responsable informatique,
Engle Martin & Associates

Étape 5 : Parlez-nous.

Box vous permet d'accéder facilement aux contenus et outils de collaboration à partir de n'importe quel appareil, avec les niveaux de sécurité, d'évolutivité et de contrôle administratif requis par les équipes informatiques. Simplification de la gestion de contenu, responsabilisation des équipes : Box vous aide à travailler plus intelligemment et plus rapidement que jamais.

Box aide plus de 69 000 entreprises, dont General Electric, AstraZeneca, Eurostar, ICADE et Schneider Electric à accéder à leurs informations sensibles dans le cloud et à les gérer de manière sécurisée. Et en l'espace d'une année, pas moins de 500 entreprises ont commencé à utiliser Box Governance pour simplifier la gouvernance de leurs informations et simplifier la mise en conformité.

Pour en savoir plus sur Box : rendez-vous sur www.box.com pour organiser une consultation, ou appelez-nous au 01 70 37 71 77.