7 conseils pour gÃ©rer ses documents.
Suite Bureautique
PostÃ© par : JulieM
PubliÃ©e le : 24/1/2022 13:00:00

Des informations correctement organisÃ©es et protÃ©gÃ©es sont impÃ©ratives pour maintenir des processus dâentreprise efficaces. Malheureusement, les collaborateurs perdent souvent beaucoup de temps Ã chercher les bons documents.

Entre les dossiers mal structurÃ©s, les multiples versions dâun mÃªme document, les e-mails non triÃ©s ou, pire encore, les archives papier, les entreprises, en plus de perdre un temps prÃ©cieux, risquent dâenfreindre les rÃ¨glementations en cours sur la protection des donnÃ©es.

Mettre en place un systÃ¨me de gestion des documents sÃ»r et convivial est indispensable, et plus simple quâil nây parait. Pour bien dÃ©marrer la nouvelle annÃ©e, Toshiba TFIS, leader sur le marchÃ© de la gestion documentaire et de lâimpression bureautique, partage sa vision des sept bonnes pratiques Ã appliquer dÃ¨s aujourdâhui pour assurer une bonne gestion documentaire en 2022.

Conseil nÂ°1 :

Classez et ordonnez les informations et les donnÃ©es

Il faut Ã©viter que les donnÃ©es et les documents papier soient dispersÃ©s. Et cela ne concerne pas que les documents papier mais aussi les informations numÃ©risÃ©s et les donnÃ©es issues dâautres sources dâinformations (e-mails, ERP,â¦) . La base dâun classement intelligent des informations consiste Ã enregistrer tous les documents de maniÃ¨re structurÃ©e, dans un systÃ¨me dâarchivage unique et centralisÃ©. Une telle structure permet aux utilisateurs autorisÃ©s dâaccÃ©der rapidement aux informations dont ils ont besoin.

Conseil nÂ°2 :

Attribuez des droits dâaccÃ¨s et de cryptage

Un bon pas vers une meilleure protection des documents consiste Ã dÃ©finir des droits dâaccÃ¨s. Cela permettra par exemple Ã un responsable RH dâaccÃ©der aux CV des collaborateurs, sans que ces documents soient accessibles Ã toute lâentreprise.

Pour intensifier la sÃ©curitÃ©, il est Ã©galement possible de recourir au cryptage, afin que seul le destinataire puisse ouvrir et modifier les fichiers. Pour mettre en place des droits dâaccÃ¨s, il faut dâabord rendre lâauthentification obligatoire avant lâaccÃ¨s au systÃ¨me de gestion. Cette Ã©tape permettra dâattribuer les droits, en fonction des profils, mais aussi de voir qui a ouvert et modifiÃ© les fichiers.

Il est Ã©galement impÃ©ratif de verrouiller le trafic entre les systÃ¨mes et les composants au moyen de certificats. Les hackers ne pourront dÃ¨s lors pas intercepter de donnÃ©es critiques, telles que les mots de passe ou informations financiÃ¨res.

Conseil nÂ°3 :

RÃ©lisez des sauvegardes

Piratage, corruption des donnÃ©es ou encore perte de donnÃ©es consÃ©cutive Ã un incendie ou Ã une erreur humaineâ¦ les risques de dÃ©faillance du systÃ¨me informatique sont prÃ©sents. Pour Ã©viter les pertes de documents en cas de panne, les sauvegardes sont indispensables.

Et ces derniÃ¨res doivent avoir lieu chaque jour. Pour ce faire, tous les logiciels de gestion des documents possÃ¨dent au moins deux niveaux de back-up : en local (disque dur externe ou serveur sur site) et dans le cloud, par exemple. Les sauvegardes doivent Ã©galement Ãªtre testÃ©es rÃ©guliÃ¨rement pour assurer leur fiabilitÃ©.

Conseil nÂ°4 :

Protection antivirus

Des virus peuvent sâ□□infiltrer dans des documents et pÃ©nÃ©trer ainsi dans lâ□□appareil local des diffÃ©rents utilisateurs. Ces virus arrivent souvent par le biais dâ□□un lien ou dâ□□une piÃ¨ce jointe ouverte par un collaborateur, par exemple.

Dans le cadre dâ□□un ransomware, les hackers verrouillent les fichiers grÃ¢ce au cryptage et exigent dâ□□obtenir une ranÃ§on pour les dÃ©crypter. Pour Ã©viter cette situation, il est important de mettre en place les systÃ¨mes antivirus proposÃ©s par les solutions de gestion documentaire. Il rÃ©duira ainsi les probabilitÃ©s dâ□□attaques rÃ©ussies.

Conseil nÂ°5 :

Une politique de conservation des documents rigoureuse

En vertu de la loi, certains documents doivent Ãªtre conservÃ©s plusieurs annÃ©es, puis dÃ©truits. Il peut sâ□□agir de documents administratifs, auxquels sâ□□applique un dÃ©lai de conservation de 7 ans, ou de donnÃ©es personnelles, soumises Ã un dÃ©lai de 5 ans.

Autrefois, ce dÃ©lai obligeait les entreprises Ã conserver des archives papier consÃ©quentes, pour ensuite Ã dÃ©truire chaque document page par page. De nos jours, la gestion des documents peut sâ□□effectuer de maniÃ¨re numÃ©rique. Mais les rÃ¨gles de conservation nâ□□ont pas changÃ©. Il convient donc de dÃ©finir au sein de votre systÃ¨me de gestion des documents Ã quel moment ces derniers seront supprimÃ©s dÃ©finitivement. Vous Ã©viterez ainsi â□□ dans le pire des cas â□□ des poursuites judiciaires.

Conseil nÂ°6 :

Signature Ã©lectronique

Pour sÃ©curiser vos documents Ã 100 % et faciliter la gestion documentaire, il est possible dâ□□opter pour des processus de validation et de signatures Ã©lectroniques. En vertu des Electronic Identities And Trust Services (eIDAS), accords permettant lâ□□utilisation de contrÃ´les dâ□□identitÃ© numÃ©riques fiables et uniformes Ã travers lâ□□Europe, une signature Ã©lectronique prÃ©sente la mÃªme validitÃ© quâ□□une signature manuscrite.

Cela permet dâ□□empÃªcher la manipulation des documents, puisquâ□□un Trust Service Provider autorisÃ© dÃ©livre alors un certificat numÃ©rique et authentifie le signataire. Automatiser le workflow permet par ailleurs aux utilisateurs de signer automatiquement leurs documents de maniÃ¨re Ã©lectronique dans leurs processus.

Conseil nÂ°7 :
Conservez les modifications

Enfin, il est important de conserver les modifications apportÃ©es Ã vos documents. Dâ□□une part, cela permet de reconstituer lâ□□historique dâ□□un document. Dâ□□autre part, les utilisateurs seront certains de travailler sur la derniÃ¨re version en date du document, Ã©vitant bien des allers-retours.

Cela Ã©vitera que ces derniers nâ□□apportent des modifications Ã des versions obsolÃ¨tes et lâ□□historique de ces modifications sera soigneusement conservÃ©, avec lâ□□identitÃ© de ceux qui les ont apportÃ©es.

Ces sept conseils permettent de mettre en place un systÃ¨me de gestion documentaire efficace, sÃ©curisÃ© et facilitant la collaboration Ã lâ□□Ã¨re du travail hybride, entre prÃ©sentiel et distanciel.Â