Sécurité informatique
–
Politique de classification des informations

A. Introduction et objet

Cette politique fait partie de l'ensemble des politiques de Modulaire Group, elle précise leur application pour la France, mais en cas de conflit les politiques de Modulaire Group (sur https://www.modulairegroup.com/corporate-policies), prévaudront.

Algeco et ses collaborateurs ont la responsabilité de protéger la confidentialité, l'intégrité et la disponibilité des informations critiques et sensibles, quelle qu'en soit la forme (électronique, imprimée, verbale, etc.). Cette politique a pour objet de souligner l'importance d'une classification et d'une conservation appropriées des informations et de donner des directives de conservation des informations pour différents types de données au sein de l'environnement d'Algeco.

B. Champ d'application

Cette politique s'applique aux informations créées, reçues, traitées et/ou stockées sur des ressources d'information d'Algeco et s'applique aux procédures suivies par les collaborateurs (qu'ils soient en contrat à durée déterminée, en contrat à durée indéterminée ou temporaires), administrateurs, dirigeants, consultants, bénévoles, membres du conseil et des comités, et autres personnes travaillant pour Algeco, y compris les sous-traitants, les travailleurs intérimaires et tout le personnel affilié à des tiers (collectivement, les « utilisateurs ») dans le cours normal des activités.

C. Énoncé de la politique

Algeco a pour politique de classer les informations en fonction de leur sensibilité. L'organisation doit ensuite mettre en œuvre des mesures adaptées au niveau de la fonction commerciale pour garantir la confidentialité, l'intégrité et la disponibilité de ces informations en fonction de leur classification. Les classifications créées prennent en compte ce qui suit :

a. Informations pouvant être transmises à toute personne extérieure à Algeco ;
b. Informations à usage interne et de nature confidentielle ; et
c. Informations qui sont de nature extrêmement sensible et dont l'accès ou la possession non autorisé(e) peut mettre en danger Algeco.

Quel que soit le niveau de classification des informations, le principe du « besoin d'en connaître » doit être appliqué à toutes les informations. Le « besoin d'en connaître » est un principe général qui garantit que l'accès à l'information n'est accordé qu'aux personnes ayant besoin d'accéder à l'information pour accomplir leurs tâches ou leurs objectifs.

De plus, les principes suivants sont à prendre en compte en ce qui concerne la classification des informations :

- L'information ne doit pas être surclassée : cela implique la mise en place de mesures contraignantes qui s'avéreraient inutiles.
- La valeur de l'information peut évoluer dans le temps : son niveau de confidentialité doit être réévalué régulièrement.
- Certaines informations ne sont sensibles que pendant une période définie. Dans ce cas, la date et l'heure à partir desquelles les informations sont déclassifiées doivent être indiquées.
- L'accumulation d'informations non sensibles peut devenir sensible.

D. Exigences et dispositions générales

Le système de classification des données repose sur les catégories de classification suivantes.

- **Public** : Informations mises à la disposition du public librement et sans réserve, sans aucune implication pour Algeco. Exemples - brochures sur les produits et services, informations sur l'entreprise accessibles au public, bulletins d'information externes et rapports financiers publics réglementaires, etc.

- **Confidentiel société :** Informations générées au sein de l'organisation pour ses opérations, telles que les flux de processus métier, les informations système, les politiques et les normes, les informations dans les tickets, les commandes des clients, le matériel de formation, les procédures d'exploitation, les informations organisationnelles, les détails du contrat ou du budget pour les projets, les documents comptables, les barèmes de prix, les rapports financiers, les dessins de conception et les tableaux de bord des résultats commerciaux, etc.

- **Confidentiel tiers :** Informations qui contiennent généralement des informations reçues de clients, de fournisseurs et de partenaires, ou de toute autre organisation (dans le cours normal des activités) sous quelque forme que ce soit pour traitement, y compris les coordonnées bancaires, les informations de carte de crédit, d'autres informations confidentielles ou personnelles, etc.

- **Soumis à restriction** : Informations extrêmement sensibles et soumises à restrictions et qui sont généralement accessibles à quelques personnes sélectionnées au sein de l'organisation. Il s'agit par exemple des données financières d'entreprise, des données RH des collaborateurs, des secrets commerciaux (par exemple les campagnes à venir), de toute information relative à un litige en cours, des procès-verbaux des réunions du conseil/comité et de la communication liée, des plaintes éthiques, des rapports d'audit/d'évaluation des risques, des clés de chiffrement et des informations classifiées de clients, fournisseurs ou partenaires, etc.

Par défaut, toutes les informations internes doivent être classées « **Confidentiel société** » sauf reclassement ultérieur à un niveau supérieur ou inférieur.

Les documents classés « **Confidentiel tiers** » ou « **Soumis à restriction** » devront avoir un cartouche de classification. Le cartouche de classification doit être inséré sur la couverture de chaque document. Une note de bas de page « Diffusion autorisée selon la classification » devrait être ajoutée.

Voici les bonnes pratiques à adopter pour utiliser un **cartouche de classification** :

- *Pour les documents sortants :*
  - **L'auteur du nouveau document** doit utiliser les modèles de documents d'entreprise et établir le niveau de confidentialité de son document à l'aide du cartouche de classification
  - **L'expéditeur d'un document existant** est chargé d'ajouter le cartouche de classification au document et d'établir son niveau de confidentialité.

- *Pour les documents entrants :*
  - **Si le document est classifié** : des recommandations de confidentialité appropriées doivent être appliquées
  - **Si le document n'est pas classifié et provient d'un tiers (avec un code de conduite existant)**, le document doit être adressé à un seul destinataire chargé :
    - du référencement du document entrant
    - d'envoyer un accusé de réception si nécessaire
    - d'établir le niveau de confidentialité du document à l'aide du cartouche de classification.

E. Mesures de protection

Pour chaque catégorie de classification, des mesures appropriées sont définies et doivent être mises en œuvre en fonction de la sensibilité à l'information.

	Confidentiel société	**Confidentiel tiers**	**Soumis à restriction**
Stockage électronique	Contrôle d'accès logique	Contrôle d'accès logique	Protégé par un code confidentiel (mot de passe)
Stockage sous format papier	Politique du bureau rangé	Politique du bureau rangé	Verrouillé sous clé
Impression et copie	Politique de l'imprimante rangée : le document n'est imprimé qu'en cas de besoin et systématiquement récupéré à l'imprimante Utiliser le « Mode confidentiel »	Politique de l'imprimante rangée : le document n'est imprimé qu'en cas de besoin et systématiquement récupéré à l'imprimante Utiliser le « Mode confidentiel »	L'impression et la copie sont interdites
Envoi vers l'extérieur	Respect du principe du « besoin d'en connaître » Ne pas diffuser sans un accord de non-divulgation	Respect du principe du « besoin d'en connaître » Ne pas diffuser sans un accord de non-divulgation	Le document est joint, protégé par un code confidentiel (mot de passe) Communiquer le mot de passe par un autre processus
Destruction	Les documents doivent être déchiquetés	Les documents doivent être déchiquetés	Déchiquetage et/ou formatage physique des supports magnétiques avant destruction ou recyclage

F. Normes de conservation

Les durées de conservation des informations sont indiquées dans la Procédure de conservation des données personnelles d'Algeco, dont une copie peut être obtenue auprès du service juridique et des risques ou dans SharePoint.

G. Applicabilité et exceptions

Cette politique s'applique à tous les collaborateurs d'Algeco (qu'ils soient en contrat à durée déterminée, en contrat à durée indéterminée ou temporaires), administrateurs, dirigeants, consultants, bénévoles, membres du conseil et des comités, et autres personnes travaillant pour Algeco, y compris les sous-traitants, les travailleurs intérimaires et tout le personnel affilié à des tiers.
Les demandes d'exception peuvent être soumises pour examen par la direction selon les politiques et normes subordonnées à cette politique. Ces exceptions sont limitées dans le temps, demandées par écrit et approuvées par le comité de sécurité informatique.

H. Application

Tout(e) violation ou non-respect de cette politique et des politiques et normes de sécurité de l'information connexes peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement.

Cette politique a été émise en février 2021, et mise à jour en octobre 2023.