

LES 3 REGLES A RESPECTER

Un manque de rigueur dans le traitement de l'information peut conduire à des PREJUDICES IRREPARABLES.

Pour le Groupe PSA PEUGEOT CITROËN la maîtrise de l'information s'inscrit dans le management de la Prévention et Gestion des Risques.

Il s'agit pour chacun, dans toutes les situations de travail, d'identifier et d'évaluer les risques encourus pour les traiter à la source en appliquant la **règle de trois** :

1^{ère} règle : L'évaluation des informations

Elle consiste à identifier la valeur de l'information traitée. Quelles sont les conséquences en cas de perte ?

Est-ce réparable et à quelles conditions ?

Est sensible, toute information quel qu'en soit le support (oral, écrit, matériel, physique ou électronique) dont la divulgation, la perte, la détérioration ou le manque de disponibilité est susceptible de porter préjudice à l'entreprise.

La sensibilité des informations détermine les règles d'élaboration, de diffusion, de publication, de conservation ou de destruction ...

2^{ème} règle : La classification des informations

Il s'agit de définir les conditions d'accès à cette information.

Est-elle réservée à des personnes nominativement identifiées ou accessible à tous ?

Les niveaux de classification sont les suivants :

USAGE INTERNE

L'information est accessible à l'ensemble du personnel du Groupe PSA PEUGEOT CITROËN et aux partenaires autorisés. Sa divulgation ou son altération n'entraîne qu'une gêne au fonctionnement normal de l'entreprise, sans conséquence durable.

CONFIDENTIEL

L'information est réservée aux personnes, entités ou partenaires qui en ont besoin d'en connaître pour agir. Sa divulgation ou son altération peut entraîner des préjudices importants mais réparables.

CONFIDENTIEL RESTREINT

L'information est réservée aux personnes nommément désignées qui en ont besoin pour agir. Sa divulgation ou son altération peut entraîner des préjudices irréparables ou dont l'impact sera visible au niveau des résultats de l'entreprise.

3^{ème} règle : La protection des informations

A chaque classe de confidentialité correspondent des dispositifs de protection qu'il convient de mettre en œuvre en fonction de chacune des situations particulières que nous rencontrons.

Elle s'obtient par une classification des « **zones sensibles** » et par des bonnes pratiques dans les différentes « **situations de vie** » de nos activités.

LES ZONES SENSIBLES

La sensibilité des informations que les zones contiennent détermine un niveau de classification. Chacun doit connaître la classification d'une zone qui détermine ses droits d'entrée.

La classification des zones est faite sous la responsabilité de leur propriétaire, en liaison avec le responsable sécurité et incendie.

Zone Interne au Groupe PSA PEUGEOT CITROËN

Toutes les zones de travail du Groupe PSA PEUGEOT CITROËN, sauf celles dévolues à l'accueil du public.

Zone avec accès réglementé

Ces zones sont réservées aux personnes qui doivent y accéder pour des raisons professionnelles. Les principes de contrôle d'accès sont déterminés par le propriétaire de la zone.

Zone avec accès réservé

L'accès à ces zones est réservé à des personnes nommément désignées par le propriétaire de la zone. Ces zones doivent être protégées spécifiquement par un contrôle d'accès unitaire.

LES SITUATIONS DE VIE



La protection des documents

Un système de classification appliqué aux documents permet de mettre en place des mesures de protection adaptées à la sensibilité des informations.

Le niveau de l'information évalué par son propriétaire permet au rédacteur et à ses destinataires de l'utiliser (communication, reproduction, archivage, destruction) dans les meilleures conditions de sécurité.



L'utilisation des moyens de communication

Protéger les informations c'est aussi prendre en compte les risques associés à l'utilisation des moyens de communication et l'ergonomie du poste de travail.

Les restrictions et précautions relatives aux moyens de communication sont définies suivant la classification appliquée aux documents.



La protection des locaux

Dans le cas où la protection à la source et au poste de travail n'est pas possible ou suffisante, il convient de protéger le local dans lequel l'information est traitée. Les règles d'accès au local doivent être définies en fonction du niveau le plus élevé de confidentialité des informations contenues.

A cette fin les lieux de production, d'échange, de traitement et de conservation des informations sensibles doivent être répertoriés, classifiés et protégés afin d'en garantir l'accès aux seules personnes autorisées.



La protection et l'utilisation des systèmes d'information

Chacun doit apprendre à mieux maîtriser les nouvelles technologies, les outils Internet/Intranet et à protéger les informations contre les virus et les attaques informatiques.

Les dossiers partagés, les mots de passe, la messagerie, les pièces jointes ... toute information peut souffrir d'une erreur de manipulation, d'une inattention ou d'une trop grande confiance. De tels incidents peuvent avoir des conséquences dommageables.

Il est indispensable de respecter les règles établies. En cas de doute, contacter son pilote informatique.



Les transports de produits ou de matériels

Les protections doivent correspondre au niveau de confidentialité des objets transportés.

Elles doivent aussi prendre en considération les dangers spécifiques aux zones géographiques traversées et les contraintes imposées aux moyens de transport (chargement initial, ruptures de charges, déchargement final...).



La communication externe

Tout échange avec un média ou un organisme extérieur doit obtenir l'aval de la Direction de la Communication de l'Entreprise qui a compétence pour vous conseiller.



Le personnel en déplacement

L'information est susceptible d'être « exportée » au-delà de l'entreprise, à l'occasion de missions qui vous sont confiées.

Les mesures de prévention et de protection dans le cadre de vos déplacements sont essentielles.



La prévention des risques dans le cadre d'un partenariat

Les relations avec nos partenaires (coopérations avec un autre groupe automobile, fournisseurs ...) sont régies par des dispositifs contractuels adaptés aux multiples informations échangées.

Ces contrats sont autant de moyens d'identifier les données sensibles et de prévenir les risques qu'elles encourrent dans le cadre de nos coopérations.



N'hésitez pas à aborder ces sujets avec vos correspondants PSA PEUGEOT CITROËN : acheteur, chef de projet, technicien.

7 BASIQUES ...

1. **PROTEGER** les informations n'est pas un sujet « pour les autres » : quelle que soit notre responsabilité hiérarchique soyons nous-mêmes exemplaires.
2. **EVALUER** le degré de confidentialité des informations que nous recevons et que nous traitons.
3. **RESPECTER** nos clauses de confidentialité et le devoir de réserve.
4. **LIMITER** la transmission d'informations non directement liées à notre mission.
5. **MAITRISER** les outils de la communication (transmission, reproduction ...).
6. **PROTEGER** (en permanence) notre matériel informatique, nos accès et nos fichiers.
7. **DETRUIRE** les informations et les objets confidentiels qui ne nous sont plus utiles.

GLOSSAIRE

> Besoin d'en connaître

Critère fondamental selon lequel une personne ne peut avoir connaissance d'une information classifiée que dans la mesure ou l'accomplissement de sa mission l'exige.

Ce besoin d'en connaître doit être entendu comme une obligation liée aux fonctions exercées et non comme un droit personnel à prendre connaissance des informations.

> Confidentialité

Propriété d'une information ni disponible, ni divulguée aux personnes, entités ou processus non autorisés en raison de sa valeur.

> Devoir de réserve

Obligation vis-à-vis de soi-même et de l'entreprise, de ne pas s'engager imprudemment, et de se garder de tout excès dans ses propos ou dans ses jugements.

> Disponibilité

Propriété d'une information ou d'un système qui définit son accessibilité en temps voulu, pour couvrir le besoin de savoir des personnes autorisées ou permettre la réalisation des fonctions de ce système. L'indisponibilité peut résulter de circonstances exceptionnelles (dégât des eaux, incendie ...), de destruction volontaire (malveillance, vol, ...) ou simplement d'erreur de manipulation ou de dysfonctionnement dans la procédure d'accès.

> Habilitation

Procédure de contrôle préalable d'une entreprise, d'une personne ou d'un matériel pour connaître ses capacités à avoir accès à des informations classifiées afin d'accomplir une mission suivant des conditions pré-définies.

> Intégrité

Garantie qu'une information n'a pas été modifiée ou détruite d'une façon non autorisée. Les méthodes d'obtention, les logiques ou les outils de traitement peuvent provoquer une perte d'intégrité de l'information.

> Risque

Combinaison d'un danger et d'un enjeu.

> Sûreté

Pour une information sensible, garantie de confidentialité, de disponibilité et d'intégrité.

LISTE D'INFORMATIONS SENSIBLES

Cette liste **INDICATIVE** est destinée à faciliter la mise en œuvre de la protection des informations.

Sont à considérer en niveau « CONFIDENTIEL » ou niveau « CONFIDENTIEL RESTREINT », selon la vue d'ensemble constituée (*), les informations ...

... relatives aux Projets, aux événements de la Vie Série et au Plan Produit	<ul style="list-style-type: none"> ➤ Les dates de lancement ou permettant de le déduire (jalons) ➤ Les caractéristiques et performances des Produits ➤ Les cadences prévues ➤ Les prix par fonction, par module, par organe, par pièce ➤ Le déroulement des Projets ➤ Les ressources mobilisées ➤ Le contenu des contrats stratégiques passés avec les fournisseurs ➤ Les faits marquants
... sur le style intérieur et extérieur des Produits avant lancement y compris restylage	<ul style="list-style-type: none"> ➤ Vues d'ensemble ... ➤ Sous ensembles ... <p>... sous forme numérique ou physique</p>
... sur les Innovations	<ul style="list-style-type: none"> ➤ Les thèmes d'études eux mêmes ➤ Les thèmes et les fournisseurs pour lesquels il y a accord de confidentialité ➤ Les thèmes conduisant à dépôt de brevet, potentiel ou en cours, et leur contenu ➤ Les projets qui les intégreront ➤ Les dates de mise sur le marché
... sur le niveau de Qualité	<ul style="list-style-type: none"> ➤ Résultats au cours du Projet, en production ➤ Résultats qualité en clientèle ➤ Vulnérabilités potentielles du produit commercialisé (robustesse antivol, algorithmes de codage, ...) ➤ Traitement des modernisations sur parc et en clientèle

(*) Des informations éparses peuvent prendre de la valeur lorsqu'elles sont rassemblées.

Le niveau de protection résultant sera d'autant plus élevé.

Pour en savoir plus : <http://b2b.psa-peugeot-citroen.com>

Ce document est destiné exclusivement aux fournisseurs du groupe PSA PEUGEOT CITROËN.

La Maîtrise de l'information



Dans le cadre de partenariats avec ses fournisseurs, le Groupe PSA PEUGEOT CITROËN développe des échanges permanents d'informations qu'il est indispensable de protéger par une attitude rigoureuse et responsable pour en garantir la confidentialité.

Ce document présente les principes de comportements développés par le Groupe PSA PEUGEOT CITROËN pour mieux maîtriser l'information, en complément des clauses contractuelles.

Ces principes s'appliquent aussi bien en interne, pour le personnel du Groupe, qu'à ses fournisseurs qui doivent protéger les informations qui leur sont confiées par PSA PEUGEOT CITROËN.

Ces derniers doivent aussi se protéger pour garantir leur propre pérennité.

L'INFORMATION est un bien immatériel qui représente un ENJEU MAJEUR pour nos Entreprises