DIRECTION DES SERVICES À L'ENTREPRISE GROUPE

# POLITIQUE RENAULT DE MAITRISE DE LA SECURITE DE L'INFORMATION

Version 1.0 – VF – Mars 2010

| | | |
|---|---|---|
| TITRE DU DOCUMENT | **POLITIQUE RENAULT DE MAITRISE DE LA SECURITE DE L'INFORMATION** | ETAT : **APPLICABLE** |

Document existant en français et anglais ….

| | | | |
|---|---|---|---|
| EMETTEUR | **DIRECTION DES SERVICES A L'ENTREPRISE GROUPE** | CENTRE DE COUT | **12900** |

| | |
|---|---|
| CHAMP D'APPLICATION | **GROUPE RENAULT** |

| | |
|---|---|
| CONFIDENTIALITE | **DIFFUSION INTERNE - PROPRIÉTÉ RENAULT** |

**MISE A DISPOSITION/DIFFUSION DU DOCUMENT**

| | |
|---|---|
| NOM DE LA SOURCE | **AER – Armoire Electronique Renault** |
| ADRESSE | *(Lien Intranet)* |

**HISTORIQUE DES VERSIONS** (la V1 et les 2 versions les plus récentes doivent rester sur le document)

| | DATE DE MISE A JOUR | REDACTEUR(S) |
|---|---|---|
| V1.0 | **Mars 2010** | **B.LALANDE** |
| | | |
| | | |

| |
|---|
| PROCHAINE MISE A JOUR : **Révision annuelle** |

| | NOM | FONCTION |
|---|---|---|
| REDACTEUR | **Bruno LALANDE** | **Directeur du Programme Maîtrise de l'Information** |
| REFERENT | **Alain PERRAUD** | **Responsable protection de l'information - DPG** |
| VALIDEUR | **Patricia MULLER** | **Directeur des Services à l'Entreprise Groupe** |
| APPROUVE PAR : | **Michel GORNET** | **Directeur Général Adjoint – DGA/FL** |

# SOMMAIRE

RENAULT

Boulogne, le 11 mars 2010
N° 2010/24

L'information est une ressource vitale de notre entreprise. La capacité à partager la bonne information, entre nous et avec nos partenaires, est un facteur-clé de notre performance.

Etant une richesse de l'entreprise, l'information est aussi une cible. Des cas de fuites encore trop nombreux viennent régulièrement nous alerter sur nos vulnérabilités.

Le respect de la confidentialité est l'une des règles fondamentales édictées dans le code de déontologie de Renault. Il nous appartient à tous d'être vigilants quant à la protection des données sensibles de l'entreprise, pour éviter des divulgations ou utilisations frauduleuses qui porteraient atteinte à la situation, à l'avantage compétitif et à l'image du Groupe.

La maîtrise de l'information passe par la diffusion et l'application générales d'un ensemble cohérent de règles et de moyens simples d'accès et d'utilisation. C'est le but de la nouvelle Politique Renault de Maîtrise de la sécurité de l'information, construite en cohérence avec celle de Nissan, et adaptée au contexte des technologies actuelles de l'information.

Je compte sur chaque manager pour en expliquer les règles, les mettre en œuvre et en contrôler l'application.

---

*Information is a vital resource of our company. Ability to share the right information, within the company and with our partners, is a key-factor of our performance.*

*Being a wealth, information is also a target. Cases of leakage are still too numerous, and alert us to our vulnerabilities.*

*Respect for confidentiality is one of the basic rules of the Code of good conduct of Renault. It is up to all of us to be watchful to the protection of our company's sensitive data, to avoid any disclosure or fraudulent misuse, which could be damaging to the situation, competitive advantage or reputation of the Group.*

*Information security control requires the diffusion and general application of a coherent set of rules and means, easy to access and to use. This is the purpose of the new Renault Policy of Information Security Management, built in coherence with Nissan's one, and updated to the context of today's information technologies.*

*I am counting on you, as a manager in this company, to explain these rules, and implement and check their application in your operational area.*

Carlos GHOSN
Président Directeur Général

# 1 – Synthèse

- La politique Renault de maîtrise de l'information s'applique à l'ensemble du Groupe Renault.

  Elle concerne :

  - les 3 dimensions de la sécurité de l'information : Confidentialité, Intégrité et Disponibilité
  - toutes les formes d'information : documents papier, données numériques, objets physiques, informations orales

- Elle répond à 5 axes de priorités :

  - Assurer la continuité opérationnelle des fonctions vitales
  - Favoriser la performance par la mise à disposition de la bonne information aux bons utilisateurs
  - Protéger les informations stratégiques, les projets et le savoir-faire
  - Assurer la conformité réglementaire et législative
  - Renforcer la culture sécurité : sensibiliser et former le personnel aux risques et aux bons réflexes à acquérir

- Elle s'exprime par :

  « Partager la bonne information au bon niveau de sécurité »

  et repose sur 7 principes :
  - Promouvoir la loyauté vis-à-vis de l'entreprise
  - Identifier et protéger les données confidentielles
  - Impliquer les managers
  - Cadrer les projets de partenariat
  - Piloter avec une vision d'ensemble, en se référant à la norme ISO 27001
  - Penser Alliance
  - Pérenniser l'organisation, par le Système de Management de la Sécurité de l'Information

- Elle s'appuie sur 5 fondamentaux :

  - Les codes de conduite
    - Code de déontologie
    - Charte du bon usage des outils informatiques

  - La norme de classification des informations ; elle définit 4 classes de confidentialité :
    - A : stratégique
    - B : critique
    - C : sensible
    - interne

  - Les réflexes de comportement
    - dans les relations et les déplacements
    - sur les sites de Renault
    - dans l'utilisation des outils informatiques

  - Les responsabilités du manager

  - La Politique de Sécurité des Systèmes d'Information

## 2 – Définitions et périmètre d'application

La politique Renault de maîtrise de la sécurité de l'information s'applique à l'ensemble du Groupe Renault. Elle s'applique en entreprise étendue, dans le fonctionnement interne comme dans les échanges avec l'ensemble des partenaires du Groupe.

Elle est construite en cohérence avec celle de Nissan, pour faciliter le partage et les échanges d'informations au sein de l'Alliance.

Elle s'inscrit dans le cadre général
- de la politique de management de Renault : Renault Management Way
- du système de gouvernance du Groupe : Compliance Committee, Management Global des Risques

De façon générique, la maîtrise de l'information se décline selon 3 dimensions principales :
- Confidentialité : propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés ;
- Intégrité : propriété de protection de l'exactitude et de l'exhaustivité des données ;
- Disponibilité : propriété d'être accessible et utilisable à la demande par une entité autorisée.

Elle concerne toutes les formes d'informations :
- les documents papier
- les documents ou données numériques
- les objets physiques : prototypes, maquettes
- les informations orales.

## 3 – La Politique et ses Objectifs

### 3.1 – Les objectifs

Renault définit 5 axes de priorités :

- Assurer la continuité opérationnelle des fonctions vitales
- Favoriser la performance par la mise à disposition de la bonne information aux bons utilisateurs
- Protéger les informations stratégiques, les projets et le savoir-faire
- Assurer la conformité réglementaire et législative
- Renforcer la culture sécurité : sensibiliser et former le personnel aux risques et aux bons réflexes à acquérir

### 3.2 – Les principes

La Politique Renault de Maîtrise de la sécurité de l'Information s'exprime par :
« Partager la bonne information au bon niveau de sécurité »

Elles repose sur les principes suivants :

- Promouvoir la loyauté vis-à-vis de l'entreprise : les informations sont une partie importante du patrimoine de l'entreprise ; les collaborateurs en sont responsables et sont tenus au devoir de discrétion vis-à-vis de l'extérieur ;

- Identifier et protéger les données confidentielles : les Directions identifient de façon sélective les informations réellement critiques ou stratégiques ; celles-ci doivent être protégées par les moyens correspondant à leur degré d'enjeu ;

- Impliquer les managers : les managers sont les principaux animateurs de la démarche, en donnant l'exemple par leur attitude personnelle et en contrôlant la mise en application ;

- Cadrer les projets de partenariat : dans les projets menés avec des partenaires extérieurs à l'Alliance, le respect des intérêts mutuels des deux partenaires impose de préciser dès le départ les limites entre les informations qui seront partagées et celles qui ne le seront pas ;

- Piloter avec une vision d'ensemble, en se référant à la norme ISO 27001, pour assurer un niveau de traitement cohérent entre les différents domaines, avec un équilibre Comportements / Technique / Contrôle ;

- Penser Alliance : les règles et outils cohérents au sein de l'Alliance permettent le traitement cohérent des informations établies en commun ou échangées avec le partenaire ;

- Pérenniser l'organisation : le Système de Management de la Sécurité de l'Information garantit le maintien de l'organisation et son évaluation régulière.

## 3.3 – Les responsabilités

- de l'Entreprise : définir la politique et les règles, mettre à disposition les moyens : outils, formations, modes de contrôle ; ces rôles sont assurés en particulier par la Direction de la protection du Groupe et la Direction des Systèmes d'Information Renault, en relation avec la Direction des Ressources Humaines Groupe, la Direction Juridique, la Direction de la Communication et la Direction de l'Audit ;

- des Directions d'établissement : mettre en œuvre les moyens de sûreté, de sécurité informatique, de gestion RH, de communication, de contrôle ;

- des Directions opérationnelles : définir la classification des informations, doter les équipes des moyens, animer ;

- des managers, chacun à son niveau : former les collaborateurs, contractualiser avec les partenaires extérieurs, donner l'exemple, contrôler ;

- des collaborateurs : connaître et appliquer les règles, alerter sur les incidents ou les anomalies.

# 4 – Les Fondamentaux

Les références majeures sur lesquelles s'appuie la Politique sont :

- les codes de conduite
- la norme de classification
- les réflexes de comportement
- les responsabilités du manager
- la Politique de Sécurité des Systèmes d'Information

## 4.1 – Les codes de conduite

Les codes de conduite établissent les règles de base que chaque collaborateur est tenu de connaître et de respecter :

- Code de déontologie
- Charte du bon usage des outils informatiques

Le manquement à ces règles peut faire l'objet de sanctions disciplinaires.

## 4.2 – La norme de classification

La norme de classification, partagée avec Nissan, établit les niveaux de classification de confidentialité des informations.

Elle s'applique à toutes les informations traitées au sein du groupe, à l'exception de celles explicitement destinées à la publication externe.

Les niveaux de classification sont marqués sur les documents, et déterminent les moyens de protection à utiliser.

La norme est définie par la Règle de classification des informations, référencée RPIF-INFOR-2009-0002, dont la synthèse est rappelée ci-dessous :

4.2.a Grille de classification

La classe de confidentialité est déterminée à partir du niveau d'enjeu :

| **Classification ➔** | **Interne** | **C** | **B** | **A** |
|---|---|---|---|---|
| **Enjeux en cas de fuite d'information** | Risque faible, mais une communication non autorisée à l'extérieur représenterait une divulgation gratuite du savoir-faire, ou pourrait perturber la communication externe de l'entreprise | Risque de perte réelle, mais limitée | Risque de perte significative pour l'entreprise, par désavantage commercial, crise d'image, mise en cause judiciaire, ou autre.. | Risque de perte ou de crise majeure, de nature à impacter le résultat financier ou la valorisation boursière. |
| **Règles générales** | Accès libre à toute personne ayant un statut de résident sur un site ou accédant à l'Intranet Renault. L'information reste toutefois de propriété Renault et ne doit pas être communiquée hors du groupe, sauf mention spécifique. | Accès restreint à une population limitée (ex: direction, métier, projet...) | Accès restreint de façon individuelle nominative aux personnes ayant strictement besoin d'utiliser l'information. Les destinataires peuvent copier ou rediffuser l'information, avec l'accord de leur hiérarchie. Les flux d'échange d'informations doivent être protégés. | Accès restreint à un petit nombre de personnes habilitées. Les personnes autorisées sont averties de leur responsabilité et s'engagent sur la confidentialité. Les supports d'information sont systématiquement protégés. La retransmission de l'information est soumise à décision de l'autorité propriétaire. |

4.2.b Marquage des documents

Le marquage destiné à la protection figure en bas du document, et se compose de deux éléments :

- Pour tous les documents : « **PROPRIETE RENAULT »**
Ce marquage doit figurer sur tous les documents créés par le personnel (permanent ou temporaire) de Renault dans le cadre de ses fonctions, à l'exception de ceux qui sont destinés à la publication externe de Renault.
La fonction de ce marquage est d'établir la propriété intellectuelle de Renault, et d'inciter tous les utilisateurs éventuels, internes ou externes, à prendre les précautions nécessaires dans l'utilisation du document.

- Pour les documents classifiés A, B ou C : « **CONFIDENTIEL** » accompagné de la case indiquant la classe de confidentialité **A**, **B** ou **C** .

4.2.c Moyens de protection des informations confidentielles

Les moyens de protection à utiliser sont fonction du niveau de classification, et du type de support d'information. Ils sont décrits dans l'instruction « Tableau des solutions techniques », régulièrement mises à jour par la DPG et la DSIR en fonction de l'évolution des risques et des technologies.

## 4.3 – Les réflexes de comportement

La maîtrise de l'information dépend en premier lieu du niveau d'implication et des attitudes adoptées par les collaborateurs de l'entreprise.

Les réflexes de comportement liés à la sécurité de l'information sont rappelés dans le guide de maîtrise de l'information. Ils concernent en particulier :

- Dans les relations et les déplacements :
    - respecter le devoir de discrétion sur les informations de l'entreprise ;
    - adopter un comportement discret dans les lieux publics ;
    - protéger les documents et les supports d'information transportés.

- Sur les sites de Renault :
    - porter son badge en permanence et respecter les contrôles d'accès aux locaux ;
    - recevoir les visiteurs autant que possible en dehors des zones de travail, et les accompagner en permanence pendant leur passage dans les zones de travail ;
    - ranger son poste de travail en tenant en sécurité les documents et le matériel.

- Dans l'utilisation des outils informatiques
    - tenir strictement personnels ses codes d'accès ;
    - protéger le réseau informatique Renault-Nissan en n'installant pas de logiciel ou d'équipement non autorisé sur son poste ou sur le réseau Renault, et en ne connectant son poste professionnel à Internet que par l'accès fourni par le réseau Renault ;
    - assurer la sauvegarde et la confidentialité des données traitées, en respectant les consignes de protection correspondant à leur niveau de classification.

## 4.4 – Les responsabilités du manager

Chaque manager, pour l'entité dont il a la charge, a un rôle déterminant à jouer dans la maîtrise de l'information.

Il exerce les responsabilités suivantes :
- classifier par niveaux de sensibilité les informations traitées dans son entité, en se référant aux tableaux de classification établis par sa Direction ;
- diffuser les règles de protection auprès de ses collaborateurs ;
- doter ses collaborateurs des moyens de protéger l'information ;
- valider et contrôler régulièrement les droits d'accès ouverts à toute personne, interne ou externe à l'entreprise, qui accède à des informations Renault dans son périmètre de responsabilité ;
- maîtriser l'information dans les projets menés en partenariat, en faisant préciser les limites des informations à partager avec le partenaire, et en veillant au respect des droits de propriété du partenaire ;
- s'assurer de la conformité vis-à-vis des lois et des règlements ;
- donner l'exemple et contrôler l'application.

## 4.5 – La Politique de Sécurité des Systèmes d'Information

La Politique de Sécurité des Systèmes d'Information (PSSI), établie par le Département Sécurité de la DSIR, définit l'ensemble des règles et outils mis en œuvre pour la sécurité des systèmes d'information.

ANNEXE A

## PRINCIPALES REFERENCES

| | |
|---|---|
| Code de déontologie du Groupe Renault | Armoire Electronique Renault – 02361-02-01 |
| Charte du bon usage des outils informatiques | Déclic / Mes services / Vie pratique / Informations : Protection et sécurité |
| Règle de classification des informations | Armoire Electronique Renault – RPIF-INFOR-2009-0002 |
| Protection de l'information – tableau de synthèse des solutions techniques | Déclic / Mes services / Vie pratique / Informations : Protection et sécurité |
| Guide de maîtrise de l'information | Déclic / Mes services / Vie pratique / Informations : Protection et sécurité |
| Maîtrise de l'information : Aide-mémoire du manager | Déclic / Mes services / Vie pratique / Informations : Protection et sécurité |
| Politique de Sécurité des Systèmes d'Information | Déclic / Mes espaces métier / Espace Métier Fonction Informatique |