



Publication

Charte d'utilisation d'un système de veille

Rapport réalisé en 2015,

Référence : GF/FC/090101 – R5 – V1



TABLE DES MATIERES

1. PREAMBULE.....	3
2. DEFINITIONS	3
2.1. Acteurs d'un système de veille.....	3
2.2. Termes appartenant au domaine de la veille	4
3. REGLES D'UTILISATION	7
3.1. UTILISATION STRICTEMENT PROFESSIONNELLE.....	7
3.2. PARTAGE ET MUTUALISATION DES INFORMATIONS.....	8
3.2.1. Traçabilité des activités	8
3.2.2. Identification du contenu.....	8
3.2.3. Coopération	8
3.2.4. Responsabilité au titre de l'information	9
3.3. RESPECT DES DROITS DE PROPRIETE INTELLECTUELLE	9
3.4. ACCES ET SECURITE	9
3.5. CONFIDENTIALITE ET CRYPTOLOGIE.....	10
3.6. ACCES PAR LES TIERS AU SYSTEME DE VEILLE.....	11
4. OBLIGATIONS D'UNE ENTREPRISE OU D'UNE ADMINISTRATION	11
5. LOIS EN VIGUEUR ET REGLEMENTATION	11
6. IMPLEMENTATION DE LA CHARTE	12



1. PREAMBULE

La charte d'utilisation d'un système de veille dans une entreprise par ses agents a pour objet de préciser les comportements attendus en termes d'échange, d'accès et de diffusion de l'information qui est contenu dans la base d'information d'un système de veille.

Elle permet de formaliser les règles de déontologie et de sécurité relatives à l'utilisation d'un système de veille d'une entreprise ou d'une administration, constitué des éléments matériels et logiciels constituant la partie informatique de la solution, mais aussi d'éléments immatériels représentés par les abonnements à des banques de données nationales et internationales.

La présente charte décrit le comportement loyal, respectueux et responsable que chaque agent doit observer à l'occasion de l'utilisation d'un système de veille quel qu'en soient les motifs et les objectifs.

L'utilisation de ce système suppose le respect de règles dont le rôle est d'assurer, notamment, la valorisation et la préservation du capital intellectuel créé et stocké dans la base de données d'un système de veille et de ses sauvegardes, fondement de la compétitivité d'une entreprise ou d'une administration.

2. DEFINITIONS

La bonne compréhension de cette charte s'appuie sur les définitions présentées ci-dessous.

2.1. Acteurs d'un système de veille

Administrateur des données¹ : personne qui a en charge la gestion du contenu des bases de données et qui gère les droits d'accès aux informations, aux documents et aux dossiers.

Administrateur d'un système : personnes qui est un informaticien et qui garantit au système de veille sa pérennité technique et qui assure le bon fonctionnement de l'ensemble des modules et met en place les règles de gestion de la DSI (sauvegardes, restauration, lancement de script, etc.).

Documentaliste : personnes qui a en charge les mises à jour des éléments associés à la recherche de l'information dans les dossiers : thésaurus, dictionnaires des mots vides (un par langue), dictionnaires de traduction, etc.

¹ Administrateur de données et administrateur d'un système sont deux fonctions qui peuvent être assurée par une même personne, sous réserve que l'agent ait un suppléant en cas d'absence.



Coordinateur :	personne qui gère les cellules de veilles pour des thématiques transverses et qui coordonne les sujets reçus du responsable. Cette personne appartient à une direction pôle.
Expert (contributeur):	expert d'un domaine qui apporte sa connaissance pour valider les synthèses et les conclusions des veilleurs. Cette personne appartient à un service ou à une direction.
Responsable :	personne qui a pour rôle de définir la politique de veille d'une entreprise ou d'une administration et de déterminer les thèmes à veiller. Il coordonne l'activité de veille d'une entreprise ou d'une administration aussi bien pour la direction générale que pour les directions opérationnelles et fonctionnelles et les filiales. Cette personne appartient à la direction générale et la représente lors des réunions et est décisionnaire face à toute demande, y compris les périodes de crise.
Veilleur :	utilisateur qui crée des sujets et scénarios de collecte, qui télécharge des documents collectés vers l'espace de diffusion.
Visiteur :	personne qui est destinatrice des synthèses et qui est habilitée à accéder ou à recevoir des informations et des documents confidentiels qui sont élaborés par les cellules de veille

2.2. Termes appartenant au domaine de la veille

Affectation :	action d'associer un sujet du plan de collecte à une rubrique du plan de classement.
Asymétrie d'information :	situation dans laquelle deux acteurs ne sont pas informés au même niveau sur l'environnement qu'ils partagent. L'objectif de la veille stratégique est de repérer les asymétries auxquelles il faut remédier pour que l'entreprise puisse mettre au point sa stratégie globale, sa communication et son lobbying.
Axe de surveillance :	description ou caractérisation de thèmes d'information.
Cellule de veille :	ensemble des personnes regroupées dans un service chargées de rechercher, collecter, analyser l'information sur l'environnement pour une organisation. Cette cellule doit ensuite diffuser l'information auprès des personnes concernées. Pour être efficace, elle doit être suffisamment proche de la direction afin de focaliser son action sur les axes stratégiques de l'organisation.
Centrage :	dans le module d'analyse, vous pouvez voir le graphe représentatif du nombre de documents (ordonnée) faisant mention [ou dont le sujet ou le titre est celui] du concept en question par date (abscisse).



Collecte :	action de collecter les informations sur les sources externes et internes.
Compétences :	capacité que possède une personne de porter un jugement de valeur dans un domaine dont elle a une connaissance approfondie (dictionnaire de l'Académie). G. de Tressac [1995] définit la compétence comme « une notion intermédiaire qui permet de penser les relations entre le travail et les savoirs détenus par les individus ».
Connaissance :	idée, notion que l'on a d'une personne ou d'une chose, représentation que l'on s'en fait (dictionnaire de l'Académie). Sur un support matériel on peut stocker de la connaissance explicite alors que la connaissance implicite se trouve dans la tête des individus. Une partie de celle-ci (tacite) ne peut être explicitée.
Densité :	dans le module d'analyse, vous pouvez voir le graphe représentatif de la densité des documents, intitulé "analyse par cooccurrence". La densité est associée à la centralité, entre l'indication de signaux forts ou faibles concernant la pertinence des documents.
Désinformation :	utilisation de techniques de l'information, notamment de l'information de masse, pour induire en erreur, cacher ou travestir les faits.
Donnée :	quantité connue dans l'énoncé d'un problème et qui sert à trouver la solution : <i>les données d'un problème</i> . Par extension : ce qui est connu et admis, et qui sert de base à un raisonnement, à un examen ou à une recherche (dictionnaire de l'Académie).
Entité nommée :	unité d'information de types Nominal (personne, lieu ou organisation), Temporel (date, heure) ou Numérique (pourcentages, valeurs) extraite d'un texte. Les grands types d'informations sont eux-mêmes subdivisés ensuite en sous-types.
Gestion des compétences :	la gestion des compétences vérifie l'adéquation entre les savoirs, savoir-faire et savoir-être du collaborateur et la définition de son poste, présent et futur. Elle relève du domaine de la Direction des ressources humaines [Laurent, 2005].
Information :	élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué (dictionnaire de l'Académie). Dans le domaine de la veille : Donnée(s) acquise(s) d'une source
Information blanche :	information aisément et licitement accessible
Information grise :	information licitement accessible, mais caractérisée par des difficultés dans la connaissance de son existence ou de son accès
Information noire :	information à diffusion restreinte et dont l'accès ou l'usage est explicitement protégé
Information critique :	information susceptible d'infléchir la stratégie de l'organisme



- Information stratégique :** information contenant des éléments susceptibles de contribuer à la définition, l'infléchissement ou la remise en cause de la stratégie de l'organisation
- Information utile :** information directement exploitable par son destinataire
- Intelligence économique :** "L'intelligence économique peut être définie comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques. L'information utile est celle dont ont besoin les différents niveaux d'une entreprise ou d'une administration, pour élaborer et mettre en œuvre de façon cohérente la stratégie et les tactiques nécessaires à l'atteinte des objectifs définis par l'entreprise dans le but d'améliorer sa position dans son environnement concurrentiel". Henri MARTRE
- Lot de documents :** un lot de documents est un ensemble de documents réunis par le veilleur, en principe à destination d'un expert, en vue de leur validation. Chaque document dispose d'une métadonnée représentative de la rubrique dans laquelle il est classé. Cette donnée modifiable est choisie par le veilleur. Les propriétés d'un lot sont automatiquement affectées aux documents de ce lot (ex : date de livraison, nom de l'expert...).
- Observatoire :** centre de regroupement et d'analyse de données qualitatives et quantitatives relatives à une problématique particulière pour en suivre les évolutions.
- Plan de classement :** structure d'accueil arborescente des documents.
- Plan de Collecte :** organisation de la collecte, à partir du produit AMI Enterprise Intelligence. Cette structure arborescente est composée de "services, veilleurs, sujets et scénarios".
- Rubrique :** un élément du plan de classement.
- Savoir :** ensemble de connaissances acquises, d'expériences vécues dans un domaine, dans une discipline, dans une science, dans une profession (dictionnaire de l'Académie)
- Savoir-faire :** qualité d'une personne qui manifeste de l'habileté à réussir ce qu'elle entreprend, dans divers domaines, surtout pratiques : affaires, relations, vie sociale (dictionnaire de l'Académie).
- Signal d'alerte :** information critique qui génère le déclenchement d'une analyse stratégique.
- Signal faible :** information qui annonce le changement d'une tendance et doit déclencher un travail de recherche d'informations complémentaires pour la confirmer et permettre le déclenchement d'une analyse stratégique.



Signal fort :	information qui confirme une tendance actuelle et qui permet de bâtir une stratégie de réponse adéquate.
Sujet/scénario :	les principaux éléments du Plan de Collecte. Le sujet permet de définir le thème de recherche et la fréquence de collecte. Le scénario permet de définir la requête à envoyer et la ou les sources à explorer.
Système de veille :	ensemble structuré réunissant les compétences répondant à des besoins de veille
Utilisateur :	personne ou chose (application informatique) qui utilise les services d'une organisation.
Veille :	activité continue et en grande partie itérative visant à une surveillance active de l'environnement technologique, commercial, etc., pour en anticiper les évolutions.
Veille passive :	écoute de tous les signaux de l'environnement sans axe précis
Volumétrie :	information d'analyse des documents collectés qui permet de visualiser la présence du sujet étudié dans les documents.

3. REGLES D'UTILISATION

Il est dans l'intérêt de l'entreprise de veiller à ce que la confidentialité des documents soit assurée par le système de veille en interoparabilité et en parfaite synchronisation avec le système d'annuaire électronique, et donc qu'il comporte des dispositifs efficaces de contrôle d'accès par :

- ✓ Le niveau de fiabilité des logiciels ;
- ✓ Le respect des procédures de demandes de modification des droits d'accès ;
- ✓ La réalisation des mises à jour dans les outils de sécurité.

Il est également de l'intérêt du concept de faire évoluer les droits d'accès aux documents et aux données en fonction du niveau de risque associé à leur contenu : renforcement de la limitation des accès pour toute raison décidées par la hiérarchie que en les diminuant, le temps diminuant, dans certains cas, les aspects de risque.

3.1.UTILISATION STRICTEMENT PROFESSIONNELLE

Le système de veille mis à disposition des agents d'une entreprise ou d'une administration est réservé à l'usage exclusif de leurs activités professionnelles au profit d'une entreprise ou d'une administration. Toute utilisation à des fins personnelles est strictement interdite.

Toutefois, les utilisateurs qui pourraient être amenés à titre personnel à réaliser des travaux liés à l'activité d'une entreprise ou d'une administration et souhaiteraient utiliser l'outil de veille devront



préalablement en obtenir l'autorisation auprès de la hiérarchie suivant la procédure qui gère ce type d'évènements.

L'entreprise ou l'administration est en droit de réaliser tous les traitements automatisés d'analyse et de renseignement qu'elle jugera utiles sur la base de données d'un système de veille.

Les agents d'une entreprise ou d'une administration doivent enrichir le système de veille de toute information ou donnée rentrant dans le cadre de leur activité professionnelle et quelque soit le support contenant l'information.

3.2.PARTAGE ET MUTUALISATION DES INFORMATIONS

3.2.1. Traçabilité des activités

Toute information susceptible d'apporter à l'entreprise ou à l'administration une plus value sur l'enrichissement immatérielle d'une entreprise ou d'une administration devra être mis à disposition de l'administrateur d'un système pour qu'il soit intégré et mis à disposition de la communauté de veilleurs.

3.2.2. Identification du contenu

Tout contenu sous forme numérique (écrits, enregistrements audio ou vidéo) diffusé dans le système de veille doit être assorti de métadonnées qui précisent notamment son réalisateur, son origine et les droits d'usage.

Le réalisateur est responsable du contenu de ces métadonnées et accepte de les renseigner au mieux, dans le respect des règles d'identification en vigueur dans la direction ou le service auquel appartient la cellule de veille.

3.2.3. Coopération

L'administrateur du contenu accessible par le système de veille d'une entreprise ou d'une administration peut être amené à répondre aux questions des utilisateurs portant sur les règles de gestion de ce contenu.

Dans ce cadre, il est tenu d'apporter toutes les précisions requises tout en respectant les règles de confidentialité et de diffusion de l'information en interne et en externe à l'entrepriseSA.



3.2.4. Responsabilité au titre de l'information

L'administrateur des données est responsable de l'information qu'il délivre et diffuse dans le système de veille d'une entreprise ou d'une administration et notamment en ce qui concerne sa complétude et sa pertinence.

L'exploitation des documents accessibles par le système de veille est faite sous la pleine et entière responsabilité de l'utilisateur.

3.3.RESPECT DES DROITS DE PROPRIETE INTELLECTUELLE

L'utilisation d'un système de veille implique le respect des droits de propriété intellectuelle d'une entreprise ou d'une administration, de ses partenaires et plus généralement de tout tiers titulaire de tels droits.

Chacun doit donc :

- ne pas reproduire au sein d'un système veille les créations de tiers protégées par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas diffuser au sein d'un système de veille de textes, des images, des photographies, des oeuvres musicales ou audiovisuelles et, plus généralement, toute création copiée sur le réseau Internet et tout autre réseau sauf si les droits d'usage associés en sont clairement définis.

La contrefaçon est un délit qui fait l'objet de sanctions civiles mais qui peut également faire l'objet de sanctions pénales.

3.4.ACCES ET SECURITE

Les personnes responsables de l'établissement et du maintien des droits d'accès doivent être identifiées et leur identité communiquée au sein d'une entreprise ou d'une administration.

Les niveaux d'accès des utilisateurs sont définis selon les critères propres à leur statut, leurs missions, la nature de leur poste, leurs besoins professionnels. Ces critères doivent être communiqués au sein d'une entreprise ou d'une administration pour chaque base de connaissances.

La sécurité d'un système de veille mis à la disposition des utilisateurs leur impose :

- de respecter les consignes de sécurité et, notamment, les règles relatives à la définition et au changement des modalités d'accès et d'authentification ;



- de respecter la gestion des accès, en particulier, ne pas utiliser les modalités d'accès et d'authentification d'un autre utilisateur, ni chercher à connaître ces informations ;
- de garder confidentiel ses modalités d'accès et d'authentification et ne pas les dévoiler à des tiers ;
- de s'interdire d'accéder ou tenter d'accéder à des ressources diffusées au sein d'un système de veille pour lesquelles l'utilisateur ne bénéficie pas d'une habilitation ; l'utilisateur doit limiter ses accès aux seules ressources pour lesquelles il est expressément habilité à l'exclusion de toute autre, même si cet accès est techniquement possible ;
- de signaler au référent toute possibilité technique d'accès à une ressource informatique qui ne correspond pas à son habilitation ; l'utilisateur s'interdit toute divulgation de cette possibilité d'accès ;
- d'avertir le référent de tout dysfonctionnement technique constaté et de toutes anomalies découvertes, telles que les intrusions dans le système de veille.

Si, pour une raison exceptionnelle, l'utilisateur est dans l'obligation de communiquer ses modalités d'accès et d'authentification, il doit alors procéder dans les plus brefs délais au changement de celles-ci. La personne qui détient les modalités d'accès et d'authentification d'un autre utilisateur ne peut en aucun cas les communiquer à un tiers, ni les utiliser à d'autres fins que celles pour lesquelles il lui a été spécifiquement donné.

3.5.CONFIDENTIALITE ET CRYPTOLOGIE

La sauvegarde des intérêts d'une entreprise ou d'une administration nécessite le respect par tous d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des informations et documents électroniques disponibles au sein d'un système de veille.

Le respect de cette confidentialité implique notamment de :

- veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein d'une entreprise ou d'une administration.

Cependant, l'utilisation de procédés de cryptage est une fonction qui ne peut être mise en oeuvre que dans certains cas autorisés. Il est interdit d'utiliser des moyens de cryptologie ou de protection d'accès autres que ceux expressément autorisés.

Les consignes de sécurité de chaque base de stockage des informations acquises et produites sont définies par la personne responsable de la base de et portées à la connaissance des utilisateurs et de l'administrateur du contenu.



3.6. ACCES PAR LES TIERS AU SYSTEME DE VEILLE

Tout utilisateur qui ferait intervenir des tiers amenés à avoir accès au système de veille de l'entreprise a l'obligation de leur communiquer et de leur faire accepter la présente charte dont une version spécifique est disponible.

4. OBLIGATIONS D'UNE ENTREPRISE OU D'UNE ADMINISTRATION

L'entreprise ou l'administration s'engage à mettre à disposition des utilisateurs un système de veille ergonomique et moderne qui leur facilite le travail de capitalisation, de stockage et de partage des informations en l'intégrant dans les processus des directions opérationnelle et fonctionnelles.

Elle s'engage à le maintenir à l'état de l'art par des améliorations et des mises à jour régulières.

5. LOIS EN VIGUEUR ET REGLEMENTATION

Les utilisateurs sont informés que l'ensemble des règles légales et réglementaires en vigueur au Maroc s'applique au système de veille d'une entreprise ou d'une administration.

En conséquence, il est rappelé que les utilisateurs devront notamment respecter, sans que cette liste ait un caractère exhaustif, les réglementations précisées ci-dessous dont le non respect peut être sanctionné pénalement :

- le droit d'auteur qu'il s'agisse de créations multimédias, de logiciels, de textes, de photos, d'images de toute nature, étant rappelé que toute mention relative aux droits de l'auteur ne peut faire l'objet d'une suppression et que toute reproduction, adaptation ou modification de l'oeuvre de celui-ci sans son consentement constitue une contrefaçon ;
- les dispositions relatives à la fraude informatique, qu'il s'agisse de l'intrusion dans un système de traitement automatisé de données ou de l'altération des éléments d'un système concerné ;
- les règles en matière de traitements automatisés de données à caractère personnel ;
- les règles d'ordre public, les informations portant atteinte à l'intégrité ou à la sensibilité des autres utilisateurs par accès à des messages, images ou textes provoquant et incitant à la haine, à la guerre ou couvrant des thématiques prohibées par les autorités et l'entreprise.



6. IMPLEMENTATION DE LA CHARTE

Les conditions d'implémentation de la charte au sein d'une entreprise ou d'une administration seront définies dans un livret des procédures.

Article optionnel dans l'hypothèse où l'entreprise ou l'administration souhaite que la charte ait valeur de règlement intérieur :

« Le non respect des règles définies dans la présente charte pourra entraîner la suppression immédiate du droit d'accès de l'utilisateur à l'outil de veille ainsi que des sanctions disciplinaires et/ou des poursuites judiciaires. Toute utilisation non conforme aux conditions et limites définies par la charte est constitutive d'une faute et pourra faire l'objet, à ce titre, de l'une des sanctions visées au règlement intérieur d'une entreprise ou d'une administration. En cas de présomption basée sur des indices d'une violation des dispositions de la charte ou d'une disposition légale ou réglementaire impérative, des contrôles portant sur l'utilisation de l'outil de veille pourront être effectués.

La présente charte sera annexée au règlement intérieur en vigueur dans l'entreprise. Conformément au Code du travail, cette charte a été soumise aux membres du comité d'entreprise. L'avis émis par le comité d'entreprise a été adressé à l'inspecteur du travail en même temps que deux exemplaires de la présente charte.