Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

DÉLÉGATION INTERMINISTÉRIELLE À L'INTELLIGENCE ÉCONOMIQUE

La sécurité économique au quotidien

en 22 fiches thématiques

Avril 2014

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Entrepreneurs, chercheurs, ingénieurs, financiers, représentants du personnel, fonctionnaires, salariés du secteur public et du secteur privé,

Votre activité économique, votre compétitivité, et même parfois votre emploi reposent - pour partie - sur votre capacité à protéger, au quotidien, votre production, votre savoir-faire, vos informations et votre établissement. Vous en êtes ainsi les meilleurs garants.

Bien entendu, il est indispensable de rester ouvert et de transmettre de l'information à ses partenaires. Bien entendu, il faut soigner sa communication envers ses clients et ses financeurs. Notre économie n'offre aucune perspective à ceux qui se renferment sur eux-mêmes.

Mais pour autant, il est désormais tout aussi indispensable de considérer l'information comme un bien précieux qu'il faut gérer avec rigueur, professionnalisme et surtout bon sens.

La délégation interministérielle à l'intelligence économique (D2IE), que j'ai l'honneur de diriger, a travaillé avec ses partenaires publics et privés à l'élaboration de 22 fiches pratiques, concrètes et simples d'utilisation, pour vous aider à vous impliquer dans la sécurité économique de votre établissement à chaque étape de son quotidien, sans dépenses excessives et inadaptées.

Ces fiches sont faites pour vous et seront réactualisées régulièrement grâce aux retours d'expérience que je vous invite à adresser à la D2IE ou aux services référents mentionnées dans les fiches.

Ensemble nous contribuerons ainsi à améliorer la sécurité de notre économie et sa compétitivité globale. Je sais pouvoir compter sur votre implication personnelle dans cette mission contribuant à l'intérêt général.

Claude REVEL

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

Ont participé à la rédaction de ces fiches :

Par ordre alphabétique

- Agence nationale de la sécurité des systèmes d'information (Premier ministre-ANSSI)
- Chambres de commerce et d'industrie (CCI France)
- Club des directeurs de sécurité des entreprises (CDSE)
- Confédération générale du patronat des petites et moyennes entreprises, Île-de-France (CGPME)
- Conseil national des barreaux (CNB)
- Ministère de l'agriculture, de l'agroalimentaire et de la forêt - Haut fonctionnaire de défense et de sécurité (HFDS)
- Ministère de la défense - Direction de la protection et de la sécurité de la défense (DPSD)
- Ministère de l'écologie, du développement durable et de l'énergie – Haut fonctionnaire de défense et de sécurité (HFDS)
- Ministères économiques et financiers
  Direction générale des douanes et des droits indirects (DGDDI)
  Haut fonctionnaire de défense et de sécurité (HFDS)
- Ministère de l'enseignement supérieur et de la recherche - Haut fonctionnaire de défense et de sécurité (HFDS)
- Ministère de l'intérieur
  Direction centrale du renseignement intérieur (DCRI)
  Direction générale de la Gendarmerie nationale (DGGN)
  Haut fonctionnaire de défense (HFD)
- Mouvement des entreprises de France (MEDEF)
- Ordre des avocats de Paris

La D2IE remercie vivement ses partenaires de leur engagement et de leurs apports précieux dans l'élaboration de ces fiches.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

Mode d'emploi

Comment aborder ce recueil de fiches ?

Ces fiches s'adressent à un public très large. Entreprises de toutes tailles, organismes de recherche et administrations sont regroupés sous le terme générique « d'établissement », même si les rédacteurs sont conscients que cette notion ne recouvre qu'imparfaitement la réalité de nombreuses structures concernées par la sécurité économique.

Chaque thématique est traitée sous différents angles afin de tenir compte de tous les aspects de la vie de « l'établissement ». Ainsi, selon les thèmes, les différentes préconisations sont regroupées autour de trois rubriques principales :

- des recommandations d'ordre **ORGANISATIONNEL** O qui s'adressent, de prime abord, aux managers,
- des recommandations d'ordre **TECHNIQUE** T qui s'adressent principalement aux responsables de la sécurité des systèmes d'information, des locaux ou de la logistique, mais aussi parfois à chaque employé qui peut appliquer lui-même certaines prescriptions très simples,
- et enfin des recommandations d'ordre **COMPORTEMENTAL** C qui s'adressent à tout un chacun, quel que soit son niveau dans la hiérarchie et son poste de travail.

La rubrique « **Mots-clés** » précise des notions abordées dans la fiche ou en relation avec le sujet.

La rubrique « **Pour aller plus loin** » permet d'orienter vers d'autres partenaires et également de proposer un accès rapide, grâce à des liens hypertextes, à des guides plus complets sur des sujets identiques ou complémentaires.

La rubrique « **Référents** » guide l'utilisateur vers les partenaires rédacteurs du présent recueil les plus à même de lui apporter une aide ou de l'orienter. Un annuaire des partenaires facilite, par ailleurs, cette prise de contact.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

O RGANISATIONNEL
C OMPORTEMENTAL

Manager la sécurité économique de l'établissement

fiche **1**

La sécurité économique d'un établissement ne peut se résumer à des mesures techniques ou organisationnelles ponctuelles. Elle suppose une implication comportementale de tout un chacun à son poste de travail.
Pour être pleinement efficace, il est donc indispensable d'accompagner chacune de ces mesures par un management global de la sécurité de l'établissement.

O

- Identifier les risques, les menaces et les vulnérabilités de l'établissement via un diagnostic général.
- Affecter des moyens (humains, financiers, matériels, etc.) adaptés à la mise en œuvre d'une politique de sécurité économique rigoureuse.
- Impliquer l'ensemble des métiers à travers des procédures dédiées et mises à jour.
- Définir et prioriser les objectifs. Suivre régulièrement leurs réalisations au travers d'audits et de tableaux de bord.
- Mettre à disposition de l'ensemble du personnel des supports de communication dédiés à la sensibilisation interne (intranet, plaquettes de communication, notes de service, etc.). Ceux-ci doivent être simples, accessibles à tous et actualisés régulièrement.
- Mettre en place des actions de sensibilisation et de formation adaptées à chaque service de l'entreprise ou corps de métiers.
- Organiser un dialogue régulier sur les problématiques de sécurité, tant horizontalement que verticalement.
- Désigner un ou plusieurs référents ayant un rôle de conseil et d'animation sur les sujets de sécurité.
- Évaluer dans quelle mesure votre établissement peut bénéficier de l'aide proposée par l'État dans le cadre du dispositif de **protection du potentiel scientifique et technique de la nation** (PPST). En effet, la création de **zones à régime restrictif** (ZRR) peut, avec un coût financier limité pour l'établissement :
  - s'avérer une opportunité pour organiser la sécurité d'un site,
  - constituer une base juridique qui permet de demander des avis sur les personnes travaillant dans la zone et qui prévoit un régime de sanctions renforcées en cas d'intrusion,
  - créer un lien privilégié avec l'administration,
  - permettre la reconnaissance du potentiel scientifique et technique du site comme intérêt fondamental de la nation,
  - répondre aux exigences de certains clients et fournisseurs.
- Contacter sans hésiter, les services étatiques de sécurité économique (voir l'annuaire des référents) chaque fois qu'une situation apparait anormale.

C

- Ne jamais à hésiter à signaler, de préférence par écrit, au responsable de la sécurité un fait inhabituel suscitant l'étonnement.
- Se rendre accessible et rester à l'écoute sur toutes les questions de sécurité économique et remarques formulées par ses équipes.
- Ne jamais sous-estimer l'importance d'un incident de sécurité.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

MOTS-CLÉS

Protection du potentiel scientifique et technique (PPST) :
La protection du potentiel scientifique et technique est notamment constituée de l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale appliquée et au développement technologique. Sa protection, fondée sur les articles 410-1 et 413-7-5 du Code pénal, prévoit la mise en place de mesures de protection adaptées permettant, notamment, la création de **Zones à régime restrictif** dont l'accès et la circulation sont réglementés.

ZRR :
Zone à régime restrictif.

RÉFÉRENTS

ANSSI, CCI France, CDSE, CGPME, CNB, DCRI, D2IE, Douane, DPSD, Gendarmerie nationale, HFDS du ministère de tutelle, MEDEF, Ordre des avocats de Paris.

Bien identifier l'information stratégique à protéger

fiche 2

Toutes les informations sensibles ne peuvent être protégées de la même façon, au risque de paralyser l'activité de l'établissement. Une analyse précise des risques est un préalable indispensable pour définir celles qui sont véritablement stratégiques et vitales, et ainsi mieux définir les conditions adéquates de leur protection.

- Appréhender les enjeux liés aux informations détenues par l'établissement en concertation avec l'ensemble des services :
  - en établissant une grille de questions permettant d'apprécier la sensibilité de l'information en fonction de l'activité ;
  - en hiérarchisant la sensibilité des informations en fonction du préjudice qu'engendrerait leur divulgation (impact faible, moyen, fort) pour la vie de l'établissement ;
  - en évaluant les risques de fuite lors de la « vie opérationnelle de l'information », tout en appréciant en particulier s'il s'agit de risques humains et/ou techniques.
- Toujours considérer comme d'une sensibilité stratégique les informations ayant un impact fort sur l'établissement. Elles doivent faire l'objet d'une protection spécifique, quelles que soient la difficulté d'accès et la probabilité de fuite.
- Organiser la gestion des informations stratégiques tout au long de leur vie : qualification/déqualification, diffusion, reproduction, conservation, destruction.
- Définir, en fonction du support et de la "vie opérationnelle de l'information", les moyens les plus adaptés de protection et d'échange : meuble ou pièce sécurisés, conditions de stockage, chiffrement des données, code d'accès, utilisation d'une plateforme d'échange sécurisée, clauses spécifiques dans les contrats de travail, formation, etc.

Exemple d'autodiagnostic

Étape 1 : Analyse du préjudice engendré par la divulgation de l'information

La perte, la destruction ou la divulgation de cette information est-elle de nature à engendrer …	Impact faible	Impact moyen	Impact fort
… un dommage pour l'activité de la structure ou le déroulement d'un projet ?			
… un impact financier ou technique ?			
… un impact sur le personnel ?			
… un impact en matière d'image et de réputation ?			
… une incidence sur la confiance des actionnaires ou des banques ?			
… une perte de confiance d'un client ou d'un partenaire important ?			

Les informations ayant un impact fort sont d'une sensibilité stratégique. Elles doivent toujours faire l'objet d'une protection et d'une traçabilité spécifiques.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Bien identifier l'information stratégique à protéger

Étape 2 : Définir le degré d'exposition des informations au risque de fuite.

La sensibilité des informations à impact moyen s'apprécie en procédant à une phase d'analyse supplémentaire du degré d'exposition de ces informations au risque de fuite. Ici encore, un questionnement précis peut aider à un bon diagnostic.

Exemple de questionnement :

- ***Comment cette information est-elle conservée à l'heure actuelle ?***

Coffre accessible à un petit nombre
Serveur central sécurisé
PC ou support mobile de nombreux collaborateurs et partenaires

- ***Qui, en interne ou en externe, a accès à cette information ?***

Peu de personnes du premier cercle autour du DG
Plusieurs cadres intermédiaires
Une grande partie du personnel

- ***Les droits d'accès à l'information sont-ils ?***

Très limités
Restreints
Libres

- ***L'information doit-elle être transportée sur un support numérique ou autre ?***

Non
Oui, lors de présentation à des partenaires connus, par exemple
Oui, lors de multiples salons à l'étranger, par exemple

- ***Comment les échanges d'information sont-ils contrôlés ?***

Transmission orale de visu ou remise de documents de la main à la main
Transmission par canal numérique sécurisé
Communication par messagerie ou par téléphone

- ***Quelle est la durée de vie de cette information ?***

Quelques heures (avant une conférence de presse, par exemple)
Plusieurs mois avant, par exemple, que le partenariat ne soit conclu ou que le brevet ne soit déposé
Plusieurs années (secret de fabrication, stratégie de sécurité de l'établissement, etc.)

En fonction des réponses accordées aux deux étapes de questionnement, les informations véritablement stratégiques pour l'établissement et, surtout, le moyen le plus adapté pour les protéger pourront être définis.

RÉFÉRENTS

- **CCI France, CDSE, CGPME, D2IE, MEDEF.**

Protéger son savoir et ses idées

fiche 3

Encore trop souvent négligée, la protection du savoir, du savoir-faire et des idées constitue pourtant un investissement souvent déterminant pour le développement et parfois pour la vie de l'entreprise ou de l'organisme de recherche. De nombreux outils juridiques sont pourtant mis à disposition pour protéger le patrimoine intellectuel des personnes physiques et morales.

Comment protéger son savoir et ses idées ?

- Identifier parmi les différents titres de propriété intellectuelle (**brevets, marques, dessins et modèles, droits d'auteur**, etc.) ceux qui sont les mieux adaptés pour protéger et valoriser ses innovations, ses produits ou ses créations immatérielles.
- Avant de déposer une marque, un dessin et modèle ou un brevet, vérifier auprès de l'institut national de la propriété industrielle (INPI) la disponibilité du droit à protéger (recherches d'antériorité) pour s'assurer du caractère nouveau de la création. Examiner la nécessité de se faire assister d'un conseil en propriété intellectuelle.
- Identifier les marchés (national, communautaire, international), présent et futur, sur lesquels protéger ses droits. Si des droits sont présents à l'international, se renseigner auprès du réseau d'experts à l'international (Douanes, **INPI**, Ubifrance, conseiller du commerce extérieur, CCI Innovation, etc.).
- Enregistrer ses droits auprès des offices compétents (**INPI, OHMI, OEB, OMPI**).
- Faire enregistrer les noms de domaine liés aux titres et à l'activité commerciale auprès de l'agence française pour le nommage sur internet en coopération (**AFNIC**).

Quelles démarches adopter pour se prémunir de la contrefaçon ?

- Mettre en place une veille, notamment sur internet, afin de détecter et de se prémunir des **contrefaçons**.
- Déposer une demande d'intervention auprès des Douanes qui permettra de mettre en retenue des marchandises suspectées d'être contrefaisantes et d'alerter le propriétaire du droit. Cette demande gratuite est valable un an renouvelable.
- Protéger ses créations par une confidentialité stricte des documents relatifs aux droits et aux produits : signature de clauses de confidentialité, protection physique et numérique des documents, etc.
- Faire immédiatement opposition auprès de l'INPI ou de tout autre office compétent, dès qu'une personne dépose un droit déjà détenu par l'établissement. Examiner sans délai la nécessité de se faire assister d'un avocat ou d'un conseil en propriété intellectuelle.

Quelle attitude adopter en cas de contrefaçon ?

- Mettre en demeure le contrefacteur de cesser les actes de contrefaçon en lui envoyant un courrier lui rappelant ce qu'il encourt à enfreindre les droits de propriété intellectuelle en question.
- Communiquer aux autorités compétentes, en particulier aux Douanes, les informations dont dispose l'établissement sur la contrefaçon : circuit de fraude, identité des contrefacteurs, caractéristiques des marchandises contrefaisantes, etc.
- Ne pas hésiter à intenter une action en justice, devant les juridictions civiles ou pénales, contre le présumé contrefacteur afin de faire cesser l'infraction et d'obtenir des dommages et intérêts.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

MOTS-CLÉS

Brevet :
Le brevet protège temporairement une innovation technique et industrielle. Pour être brevetable, une invention doit être nouvelle, sa conception doit être inventive et susceptible d'une application industrielle. Attention : il n'est pas possible de protéger une idée par un brevet ! Seuls les moyens techniques mis en œuvre pour la concrétiser le seront.

Marque :
Au sens de la propriété intellectuelle, la marque est un « signe » servant à distinguer précisément vos produits, ou services, de ceux de vos concurrents. Elle peut être notamment sonore, figurative, tridimensionnelle et même olfactive.

Dessins et modèles :
L'apparence des produits peut être protégée au titre des « dessins et modèles », selon qu'elle matérialise un assemblage de lignes et de couleurs en deux dimensions (dessins) ou une forme modélisée en trois dimensions (modèles).

Droit d'auteur :
Le droit d'auteur est un droit de propriété exclusif acquis sans formalité d'enregistrement dès sa création sur toutes les œuvres de l'esprit quels que soient leur genre (littéraire, musical, scientifique et technique) et leur mode d'expression.

Contrefaçon :
La contrefaçon est l'utilisation sans autorisation d'un droit de propriété intellectuelle.

Les droits de propriété intellectuelle couvrent principalement :
- la propriété industrielle : marques, dessins et modèles, brevets ;
- la propriété littéraire et artistique : droit d'auteur et droits voisins du droit d'auteur.

L'institut national de la propriété industrielle, **INPI**, établissement public placé sous la tutelle des ministères économiques et financiers, est l'organisme compétent pour la délivrance des titres de propriété industrielle nationaux (marques, brevets, dessins et modèles).

L'office de l'harmonisation du marché intérieur, **OHMI**, est l'agence de l'Union européenne compétente pour l'enregistrement des marques et des dessins ou modèles valables dans les 28 pays de l'UE.

L'office européen des brevets, **OEB**, offre aux inventeurs une procédure uniforme de demande de brevet, leur permettant d'obtenir une protection par brevet dans un maximum de 40 pays européens.

L'organisation mondiale de la propriété intellectuelle, **OMPI**, permet d'enregistrer ses marques, dessins et modèles à l'échelle internationale.

L'association française pour le nommage internet en coopération, **AFNIC**, est une association loi 1901 en charge de la gestion des extensions françaises d'internet.

POUR ALLER PLUS LOIN

Institut national de la propriété industrielle (INPI)
www.inpi.fr
www.inpi.fr/fileadmin/mediatheque/pdf/brochure_proteger_ses_creations.pdf

Comité national anti-contrefaçon (CNAC)
Ce comité regroupe tous les partenaires publics et privés impliqués dans la lutte anti-contrefaçon.
http://www.contrefacon-danger.com/

Union des fabricants (UNIFAB)
Créée en 1872, l'union des fabricants regroupe plus de 200 entreprises et des fédérations professionnelles. Elle promeut la protection internationale de la propriété intellectuelle et lutte contre la contrefaçon en menant des opérations de lobbying, de formation et de sensibilisation.
http://www.unifab.com/fr

Guide pratique « PME : pensez propriété intellectuelle ! »
Guide pratique de management de la propriété intellectuelle réalisé par la direction générale de la compétitivité, de l'industrie et des services (DGCIS) à l'attention des PME.
http://www.dgcis.gouv.fr/files/files/guides/guide-pme-pensez-pi.pdf

Guide propriété intellectuelle : « Contrefaçon, comment vous protéger »
Guide pratique, élaboré par l'INPI et CCI France dans le cadre de l'action du CNAC, visant à sensibiliser, par des cas concrets, aux enjeux de la protection des innovations et de la défense de la propriété intellectuelle afin de lutter contre la contrefaçon.
http://www.dgcis.gouv.fr/files/files/guides/contrefacon-pme.pdf

Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)
http://www.economie.gouv.fr/dgccrf

RÉFÉRENTS

- **CNB, Douane, Ordre des avocats de Paris.**

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Protéger ses locaux

fiche 4

S'il est évident pour tout un chacun de fermer la porte de son domicile, il est tout aussi indispensable de veiller à ce que seules les personnes dument autorisées entrent et sortent de l'établissement que l'on dirige ou dans lequel on travaille.

O

- Désigner un responsable sûreté, connu de l'ensemble des salariés, chargé de la rédaction des procédures et de leur mise en œuvre.
- Prendre en compte les risques liés à l'environnement immédiat : le voisinage, les bâtiments adjacents, etc.
- Identifier et hiérarchiser des zones à protéger en fonction des risques, des acteurs, du fonctionnement de l'établissement et adapter les mesures de sécurité en conséquence. Eviter de placer les zones les plus sensibles dans des locaux trop vulnérables (emplacement, matériaux utilisés, etc.).
- Réglementer l'accès aux différentes zones en fonction des nécessités réelles de chacun.
- Établir un journal des incidents, des reports et alertes.
- Sensibiliser régulièrement les personnels aux règles de sécurité du site et former les plus concernés.
- Sensibiliser les sociétés prestataires de service et les partenaires aux dispositifs internes de protection des locaux.
- Évaluer périodiquement la performance de son système de contrôle d'accès : audits internes, exercices, tests d'intrusion, vérification des délais d'intervention, etc.

T

La protection mécanique

- Délimiter le périmètre de l'établissement en utilisant une signalétique appropriée.
- Mettre en place une clôture d'enceinte adaptée aux risques identifiées (dimension, double ou non, instrumentée ou non, bas volets ou non, etc.). Utiliser la végétation comme barrière naturelle si le site le permet.
- Équiper le site et ses abords d'un système d'éclairage dissuasif.
- Veiller au niveau de sécurité des ouvertures (portes et fenêtres) afin de limiter tout risque d'intrusion.
- Instaurer un système de contrôle d'accès adapté. Opter pour un système qui prendra en considération la nature des activités menées et préservera la fluidité des flux : humains, marchandises et véhicules.
- Prévoir une gestion rigoureuse des clés et badges d'accès.

La détection et la vidéo-surveillance

- Mettre en place un système de détection des intrusions (barrières infrarouges, détecteurs volumétriques et/ou périmétriques, clôtures de détection, etc.) en fonction des besoins identifiés.
- N'envisager la vidéo-protection que si cela est nécessaire. Dans ce cas, installer un système de vidéo-protection adapté à la configuration de l'établissement (extérieur et intérieur).
- Se renseigner sur la législation en vigueur concernant la vidéo-surveillance et l'appliquer rigoureusement : information du personnel, délai de conservation des images, etc.

C

- Alerter immédiatement le responsable sûreté de tout problème ou événement inattendu survenu sur le site.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

POUR ALLER PLUS LOIN

Le réseau des référents sureté

Les référents sureté sont des gendarmes ou des policiers ayant suivi une formation spécifique. Ils sont en mesure de vous apporter, gratuitement, des conseils sur les plans législatif, matériel ou humain, abordant de la sorte les dispositifs envisagés pour diminuer le passage à l'acte.

http://www.referentsurete.com

RÉFÉRENTS

- **DCRI, Douane, DPSD, Gendarmerie nationale, HFDS du ministère de tutelle.**

TECHNIQUE
COMPORTEMENTAL

Se déplacer au quotidien

fiche
5

Parce qu'ils sont routiniers et prévisibles, les petits déplacements au quotidien exposent les acteurs économiques à d'importantes vulnérabilités facilitant la perte ou la fuite d'informations sensibles.

T

- Installer un **filtre de confidentialité** sur les écrans des ordinateurs portables, des tablettes et des smartphones à usage professionnel.

C

- Éviter de transporter les données sensibles lors des déplacements quotidiens, notamment entre le domicile et le travail. Si cela est indispensable, utiliser une clé USB sécurisée et la conserver en permanence sur soi.
- En cas d'utilisation des fonctions WiFi/Bluetooth des appareils nomades dans les transports en commun, garder à l'esprit que toute liaison peut être interceptée.
- Éviter au maximum de parler de sujets professionnels dans les transports en commun : métro, bus, taxi, train, avion.
- Être attentif à l'environnement lors des échanges dans les espaces publics et partagés : restaurants, cantines, cafés, salles d'attente, etc.
- Rester discret dans ses lectures professionnelles (rapports, notes en cours, courriels, etc.) dans un lieu public.
- Taper discrètement ses identifiants et mots de passe d'accès à l'ordinateur, ou à sa messagerie.
- Ne jamais laisser ses outils de travail (mallette, ordinateurs portables, téléphones, etc.) sans surveillance.
- Lors des déplacements en voiture, déposer discrètement ses affaires dans le coffre verrouillé et non sur la banquette arrière ou le siège passager. Lors des stationnements, ne pas laisser d'ordinateurs portables ou de documents contenant des données sensibles dans la voiture, même dans le coffre.

MOT-CLÉ

Filtre de confidentialité :
Film de protection qui se place sur un écran et qui restreint la vision des données affichées de part et d'autre de l'axe de vision.

RÉFÉRENTS

- **CCI France, DCRI, DPSD, Gendarmerie nationale.**

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Accueillir du personnel temporaire

fiche 6

Un personnel temporaire (stagiaire, intérimaire, prestataire, etc.) concentre ses activités sur un sujet dont les contours sont précisés formellement. N'étant lié à l'établissement que de façon ponctuelle, il représente une vulnérabilité. Il peut être la cible ou l'acteur d'une malveillance. Une attention particulière doit donc être apportée aux conditions d'accès de ces personnels à l'information.

O

- Élaborer et mettre en place un processus visant à bien connaître le parcours du futur personnel temporaire avant qu'il n'arrive. Ce processus doit concerner la personne elle-même mais également son environnement, notamment de travail.
- Avant acceptation du contrat, faire en sorte que les informations relatives à la mission du personnel temporaire soient bien partagées par tous les services concernés (RH, SSI, sécurité, administratif, opérationnel).
- Désigner une personne de l'établissement qui sera responsable de l'encadrement du personnel temporaire tout au long de son séjour dans l'établissement.
- Tenir à jour un répertoire des personnels non permanents. Peuvent notamment y être précisées les données suivantes :
  - nom et prénom, date et lieu de naissance, adresse,
  - références de la CNI pour un ressortissant français, du titre de séjour et du passeport pour un étranger,
  - nom du responsable de l'encadrement,
  - nom de l'accueillant (si différent du responsable de l'encadrement),
  - date de début et de fin de contrat ou de convention,
  - objet de la mission ou thématique(s) abordée(s),
  - autorisations d'accès géographiques et informationnels.
- Prévoir dans le contrat ou la convention :
  - une clause de confidentialité ;
  - une interdiction formelle de toute diffusion d'informations relatives à l'établissement ou à ses activités, sans l'accord express de celui-ci.
- Sensibiliser le personnel temporaire dès son arrivée aux mesures de sécurité exigées par l'établissement.
- Identifier les personnels temporaires par le port obligatoire de badge spécifique ou par tout autre signe distinctif visible de loin.
- Apporter une attention particulière aux informations figurant dans les documents produits par les personnels temporaires (rapport de stage, mémoire, livrable, etc.).
- Saisir rapidement les services de police ou de gendarmerie compétents en cas de malveillance suspectée. Ne pas essayer de gérer la situation uniquement en interne.
- Suivre la carrière des stagiaires durant quelques mois après leur départ.

T

- N'autoriser l'accès aux systèmes d'information qu'à partir d'équipements fournis par l'établissement, et à partir d'un identifiant strictement personnel et tracé.
- Limiter l'accès aux ressources informatiques et aux informations strictement nécessaires et en relation directe avec leur sujet de travail.
- Clôturer les comptes informatiques des personnels temporaires immédiatement après la fin de leur contrat pour l'établissement.

C

- Ne pas évoquer d'informations sensibles en présence du personnel temporaire.
- S'assurer au quotidien que le personnel temporaire a bien compris et pris en compte toutes les instructions de sécurité qu'il s'est engagé à respecter.
- En cas de non-respect des règles encadrant sa présence dans l'établissement, alerter sans délai les responsables de l'encadrement et de la sécurité

RÉFÉRENTS

- **CNB, DCRI, DPSD, Gendarmerie nationale, HFDS du ministère de tutelle, Ordre des avocats de Paris.**

Avril 2014

Premier ministre
Délégation interministérielle à l'intelligence économique

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Recevoir des visiteurs

fiche **7**

Un visiteur ne pénètre dans un établissement que grâce à la volonté expresse de celui qui l'accueille. Il est souvent porteur d'opportunités nouvelles pour l'établissement mais peut également constituer une menace. Il doit donc se conformer strictement aux règles qui lui sont imposées.

O

- Impliquer l'ensemble du personnel lors de visites sensibles. Demander à chacun un regain de vigilance.
- Se faire communiquer avant la visite, l'identité, les coordonnées et la fonction des visiteurs. N'accepter que ceux qui se sont déclarés.
- Élaborer formellement une procédure d'accueil des visiteurs quels qu'ils soient. S'assurer que l'ensemble du personnel en a connaissance et la met en œuvre.
- Enregistrer les horaires d'entrées et de sorties des visiteurs et en conserver la trace plusieurs semaines.
- Remettre un badge d'accès spécifique, ou un autre signe distinctif, et rendre obligatoire son port apparent.
- Prévoir des lieux spécifiquement dédiés à leur accueil (stationnement et réception).
- Notifier, si possible dans la langue des visiteurs, les engagements de confidentialité propres à la visite.
- Définir un parcours de visite (**circuit de notoriété**) excluant les zones les plus confidentielles.
- Définir précisément les informations qui pourront être ou non évoquées au cours de la visite.
- Accompagner les visiteurs, dans la mesure du possible en permanence, de leur arrivée à leur départ.
- Encadrer strictement l'enregistrement du son et la prise de photographie ou de vidéo.

T

- Prévoir un ordinateur dédié, non connecté au réseau, permettant de recevoir les supports amovibles des visiteurs.
- Désactiver tous les supports USB des ordinateurs se trouvant sur le circuit de notoriété.

C

- Ne pas hésiter à questionner un visiteur non accompagné semblant chercher son chemin. Le raccompagner vers son groupe ou son responsable.
- Être vigilant aux questionnements trop intrusifs dont pourraient faire preuve certains visiteurs.
- Rendre compte immédiatement de tout problème ou événement inattendu survenu lors de la visite.

MOT-CLÉ

Circuit de notoriété :
Circuit préétabli permettant de faire visiter un établissement, d'en donner une image concrète et valorisante tout en évitant les locaux sensibles.

RÉFÉRENTS

- **CCI France, DCRI, DPSD, Gendarmerie nationale, HFDS du ministère de tutelle.**

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Protéger son poste de travail

fiche 8

Si les systèmes d'information numériques sont désormais totalement incontournables pour tous les acteurs économiques, l'attention portée à leur sécurité au quotidien par leurs utilisateurs est encore bien insuffisante. Les négligences sur les postes de travail exposent l'établissement à de graves problèmes susceptibles de compromette son activité.

O

- Définir et faire appliquer une politique de choix de **mots de passe robustes**, difficiles à retrouver à l'aide d'outils automatisés ou à deviner par une tierce personne :
  - au minimum 12 caractères de type différent : majuscules, minuscules, chiffres, caractères spéciaux,
  - aucun lien direct avec la personne : éviter les noms, dates de naissance, etc.,
  - absent du dictionnaire.
- Définir un mot de passe unique et personnel pour chaque usage. Les mots de passe protégeant des contenus sensibles (banque, messagerie, etc.) ne doivent en aucun cas être réutilisés.

T

- Désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus systématique afin de vérifier qu'ils ne contiennent aucun virus connu.
- Désactiver les ports USB non utilisés pour la connexion des périphériques.
- Gérer avec une attention particulière les supports amovibles qui sont une extension du poste de travail.
- Tracer l'accès aux informations sensibles à partir des mots de passe ou d'autres systèmes d'authentification sécurisés.
- Mettre à jour régulièrement le **système d'exploitation** et les logiciels. Les logiciels peuvent être configurés pour que les mises à jour de sécurité s'installent automatiquement. Sinon, télécharger les correctifs de sécurité disponibles.

C

- Ne conserver les mots de passe ni sur support papier, ni dans un fichier informatique. Eviter d'utiliser des outils permettant de stocker différents mots de passe. Privilégier la mémorisation de ceux-ci à l'aide de moyens mnémotechniques.
- Face à un courriel suspect :
  - ne jamais ouvrir les pièces jointes provenant de destinataires inconnus, ou dont le sujet ou le format paraissent incohérents avec les fichiers habituellement reçus ;
  - si des liens figurent dans le corps du courriel, passer la souris dessus avant de cliquer. L'adresse complète du site s'affichera ce qui permet une vérification ;
  - ne jamais répondre par courriel à une demande d'informations personnelles, confidentielles ou bancaires ;
  - ne pas ouvrir et ne pas relayer des chaînes de lettre ou des appels à solidarité suspects.
- Télécharger les programmes uniquement sur les sites de leurs éditeurs.
- Se connecter au réseau à partir d'un compte utilisateur limité aux tâches bureautiques d'un ordinateur (navigateur, messagerie, suite logicielle, etc.).
- Ne pas naviguer sur internet à partir d'un compte administrateur, ou d'un compte ayant des droits particuliers.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

MOTS-CLÉS

Anti-virus :
logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants.

Cheval de Troie :
logiciel apparemment inoffensif, installé ou téléchargé et au sein duquel a été dissimulé un programme malveillant qui peut, par exemple, effectuer la collecte frauduleuse, la falsification ou la destruction de données.

Droits administrateur :
faculté d'effectuer des modifications affectant le fonctionnement système et logiciel du poste de travail: modifier des paramètres de sécurité, installer des logiciels, etc.

Mot de passe robuste :
La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres Choisir des mots de passe d'au moins 12 caractères de types différents : majuscules, minuscules, chiffres, caractères spéciaux.

Système d'exploitation :
programme assurant la gestion de l'ordinateur et de ses périphériques.

POUR ALLER PLUS LOIN

Deux méthodes simples pour choisir les mots de passe :

- la **méthode phonétique** : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CD%E7am ;
- la **méthode des premières lettres** : « Un tiens vaut mieux que deux tu l'auras » : 1tvmQ2tl'A.

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Guide d'hygiène informatique – http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Recommandations de sécurité relatives aux mots de passe – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

RÉFÉRENT

- **ANSSI**

O RGANISATIONNEL
T ECHNIQUE

Protéger et gérer l'accès au réseau

fiche 9

Le réseau informatique d'un acteur économique est désormais la principale porte d'entrée pour l'accès à l'information. Sa sécurité peut s'avérer vitale pour l'établissement. Mais celle-ci se mesure à l'aune de son maillon le plus faible. Chacun à son poste doit donc être pleinement mobilisé.

O

- Tenir à jour la liste précise de tous les équipements informatiques de l'établissement qui peuvent se connecter au réseau (ordinateurs personnels, imprimantes, photocopieurs, etc.).
- Identifier nommément chaque utilisateur, supprimer minutieusement les comptes anonymes et génériques.
- Attribuer des droits d'accès (répertoires, calendriers, etc.) de façon graduée et adaptée strictement aux besoins. Actualiser ces droits lors de mouvements internes.
- Limiter drastiquement le nombre d'utilisateurs disposant de **droits administrateurs**.
- S'assurer de la suppression effective des droits d'accès au réseau lors du départ d'un collaborateur ou d'un personnel temporaire.

T

- Privilégier une configuration d'accès à internet par câble plutôt que par WiFi.
- Si le WiFi est le seul moyen d'accéder à internet :
  - sécuriser l'accès en modifiant le nom d'utilisateur et le mot de passe attribué par défaut lors de la configuration initiale ;
  - vérifier que la *box* dispose du protocole de chiffrement **WPA2** et l'activer ;
  - remplacer la clé de connexion par défaut par un **mot de passe robuste** qui ne sera divulgué qu'à des tiers de confiance et changé régulièrement ;
  - activer et configurer les fonctions **pare-feu**/routeur. Ne pas hésiter à contacter l'assistance technique du **fournisseur d'accès**.
- Désactiver le signal WiFi de la borne d'accès lorsqu'il n'est pas utilisé.
- Vérifier qu'aucun équipement connecté au réseau interne (intranet) ne puisse être administré *via* internet. C'est souvent le cas des imprimantes, des serveurs, des routeurs, ainsi que d'équipements industriels ou de supervision. Limiter, si possible, la télémaintenance.
- Ne pas laisser de prises d'accès physique au réseau interne accessibles au public.
- Renouveler régulièrement les identifiants et mots de passe configurés par défaut sur tous les équipements (imprimantes, serveurs,…).

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

MOTS-CLÉS

Droits administrateur :
faculté d'effectuer des modifications affectant tous les utilisateurs (modifier des paramètres de sécurité, installer des logiciels, etc.).

Fournisseur d'accès :
prestataire proposant une connexion à internet.

Mot de passe robuste :
la robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais aussi de divers autres paramètres (Recommandations de sécurité relatives aux mots de passes – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf). Choisir des mots de passe d'au moins 12 caractères de types différents :majuscules, minuscules, chiffres, caractères spéciaux.

Pare-feu (firewall) :
logiciel et/ou matériel protégeant un équipement ou un réseau informatique en contrôlant les entrées et sorties selon des règles définies par son administrateur.

WEP et WPA2 :
protocoles de sécurité permettant de fournir aux utilisateurs de réseaux locaux sans fil une protection contre le piratage. Le WPA2 devrait se substituer au système WEP jugé insuffisant.

POUR ALLER PLUS LOIN

Deux méthodes simples pour choisir les mots de passe :

- la **méthode phonétique** : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CD%E7am ;
- la **méthode des premières lettres** : « Un tiens vaut mieux que deux tu l'auras » : 1tvmQ2tl'A.

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Guide d'hygiène informatique – http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Recommandations de sécurité relatives aux mots de passe – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

RÉFÉRENT

- **ANSSI**

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Utiliser des supports amovibles de façon sécurisée

fiche **10**

Le support amovible, s'il permet de transporter facilement des données, peut être compromis par un logiciel malveillant susceptible d'agir sur la machine ou le réseau auquel il sera connecté. La perte d'un support amovible signifie, par ailleurs, la perte des informations qu'il contient.

O
- Interdire la connexion d'équipements et de supports amovibles personnels (clés USB, disques durs externes, *smartphones*, tablettes, lecteurs MP3, etc.) à des postes reliés au système d'information de l'établissement. Sensibiliser les collaborateurs, notamment au moyen de la charte informatique, à cette règle importante souvent perçue comme une contrainte.

T
- Désactiver l'exécution automatique des périphériques depuis le panneau de configuration de chaque poste.

C
- En cas d'utilisation d'un support amovible, par exemple pour échanger des données, utiliser une clef USB réservée à cet usage.
- Avant de l'utiliser, analyser avec un outil adapté, tout support amovible qui a été connecté à l'extérieur du réseau de l'établissement.

C
- À l'issue de son utilisation, supprimer les données sensibles figurant sur le support amovible avec un logiciel d'effacement sécurisé.
- **Chiffrer** les données les plus sensibles avec un logiciel adéquat.
- Utiliser des supports amovibles pour réaliser des sauvegardes régulières, comme un disque dur externe réservé à ce seul usage, un CD ou un DVD enregistrable. Ranger ce support dans un lieu protégé, éloigné de l'ordinateur, de préférence à l'extérieur de l'établissement, pour éviter, en cas d'événement grave, que la copie de sauvegarde ne soit volée ou détruite en même temps que les données d'origine.
- Ne pas prêter ses supports amovibles. Ne pas les laisser accessibles sans surveillance.

MOT-CLÉ

Chiffrement :
procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

POUR ALLER PLUS LOIN

- L'ANSSI publie sur son site une liste de logiciels de chiffrement et de suppression de données que vous pouvez utiliser en toute confiance.

http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/

RÉFÉRENT

- **ANSSI**

Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

O RGANISATIONNEL
C OMPORTEMENTAL

Utiliser des appareils nomades de façon sécurisée

fiche **11**

Si les appareils nomades sont appréciés et utiles parce qu'ils simplifient souvent les tâches quotidiennes des acteurs économiques, leur usage expose cependant l'établissement et ses partenaires à des risques nouveaux de perte ou de captation d'informations stratégiques qu'il est nécessaire de bien maitriser en prenant certaine précautions élémentaires.

O

- Veiller à ce que personne dans l'établissement n'utilise son appareil nomade personnel (ordinateurs portables, *smartphones*, tablettes, lecteurs MP3, etc.) à des fins professionnelles. Cette règle est souvent perçue comme une contrainte forte, notamment par l'encadrement supérieur ; elle est cependant d'une importance particulière.
- Proscrire toute politique de **BYOD** (*Bring your Own Device*) au sein de l'établissement.

C

- Désactiver la connexion automatique des appareils nomades aux points d'accès WiFi ouverts.
- Désactiver le Bluetooth lorsqu'il n'est pas utilisé.
- En plus du code PIN protégeant la carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l'accès à son *smartphone* ou à sa tablette et les configurer pour qu'ils se verrouillent automatiquement après un court moment d'inactivité.
- Activer le **chiffrement** des supports de stockage, lorsque cela est possible, ou chiffrer les données les plus sensibles à l'aide d'un logiciel dédié.
- N'installer que les applications nécessaires et vérifier à quelles données elles permettent l'accès avant de les télécharger sur l'appareil nomade (informations géographiques, contacts, appels téléphoniques, etc.). Éviter d'installer les applications demandant l'accès à des données qui ne sont pas strictement nécessaires au fonctionnement de l'appareil nomade.
- Effectuer des sauvegardes régulières des contenus sur un support externe pour pouvoir les conserver en cas de restauration de l'appareil dans son état initial.
- Être très attentif à ne pas se séparer des appareils nomades qui peuvent contenir des informations sensibles ou permettre d'accéder au réseau de l'établissement.

MOTS-CLÉS

BYOD ou **AVEC :**
Bring your Own Device ou « Apporter votre équipement personnel de communication ». Politique d'établissement qui admet ou préconise l'utilisation d'équipements de communication personnels à des fins professionnelles.

Chiffrement :
procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

POUR ALLER PLUS LOIN

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Guide d'hygiène informatique – http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Recommandations de sécurité relatives aux mots de passe – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Utiliser des appareils nomades de façon sécurisée

RÉFÉRENT

- ANSSI

Maîtriser l'externalisation informatique

fiche 12

L'externalisation peut parfois permettre de pallier l'absence d'une compétence en interne. L'externalisation informatique (dite aussi « *infogérance* ») présente néanmoins des risques pour les données et les systèmes d'information, qu'il convient de connaitre et de maîtriser.

- Déterminer en fonction de la nature de l'établissement ses besoins précis en externalisation informatique (**infogérance**, *cloud computing*, plateforme logicielle à distance, etc.).
- Hiérarchiser les objectifs de sécurité de l'établissement (disponibilité du site internet, hébergement sur des serveurs dédiés, etc.) et les intégrer lors des appels d'offres par des clauses détaillées dans le cahier des charges.
- Demander explicitement aux prestataires répondant aux appels d'offres un **plan d'assurance sécurité** (PAS).
- Afin de limiter les risques liés à la perte de maîtrise des systèmes d'information, aux interventions à distance et à l'hébergement mutualisé (lorsque les données de plusieurs établissements sont hébergées sur le même serveur physique), faire analyser le contrat par des spécialistes (techniques et juridiques).
- Il existe des risques spécifiques liés au ***cloud computing***, ou **informatique en nuage** : risques pour la confidentialité des données, risques juridiques liés à l'incertitude sur la localisation des données, risques liés à la perte de maîtrise du système d'information, risques liés à l'irréversibilité des contrats. Les contrats proposés dans le cadre des offres génériques ne cadrent généralement ces risques que de façon très insuffisante. Rédiger, en liaison avec des spécialistes (techniques et juridiques), des contrats personnalisés et appropriés aux enjeux de l'entreprise.

MOTS-CLÉS

Infogérance :
externalisation appliquée au domaine des systèmes d'information.

Informatique en nuage *(cloud computing)* **:**
mode de traitement des données d'un client dont l'exploitation s'effectue par internet, sous la forme de services fournis par un prestataire. Dans ce cas de figure, l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients.

Plan d'assurance sécurité (PAS) :
document contractuel garantissant le respect des exigences de sécurité. Le guide édité par l'ANSSI propose un canevas pour la rédaction des objectifs de sécurité devant figurer dans le PAS.

POUR ALLER PLUS LOIN

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- « Maîtriser les risques de l'infogérance » – http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

RÉFÉRENTS

- **ANSSI, CCI France, CNB, Ordre des avocats de Paris.**

Éviter ou gérer la perte d'une compétence-clé

fiche 13

La seule ressource véritablement durable de toute organisation est l'humain. Les compétences-clés ont donc une valeur souvent décisive. Elles sont l'objet de toutes les convoitises exprimées de façon plus ou moins loyale. Leur perte pouvant avoir des conséquences dramatiques, il convient de mettre en place des mesures préventives mais aussi réactives pour limiter l'exposition de l'établissement.

Anticiper et préserver les compétences-clés

- Identifier les compétences-clés par des indicateurs, des grilles de compétences, des entretiens, des courriers de motivation, etc., en tenant compte du secteur dans lequel l'établissement se développe (technologies de pointe, secteurs innovants, secteurs sensibles, etc.).
- Développer une veille sur le recrutement (par exemple : offres d'emploi de la concurrence) et le *turn-over* (par exemple : médias sociaux).
- Garder à l'esprit que le cloisonnement des missions, des activités et des compétences internes accroît sensiblement le niveau de vulnérabilité au changement et donc des risques de départ.
- Favoriser, par la formation interne, le partage des bonnes pratiques et des compétences.
- Établir en amont les schémas d'intervention en cas de vacance d'un poste (personnes-relais, délégations de décision, de signature, etc.).
- Fidéliser les compétences-clés par une politique de gestion des ressources humaines personnalisée (motivation, intéressement, actionnariat, etc.). Profiter notamment des entretiens annuels afin de réévaluer les salaires, les conditions de travail, les projets souhaités, les qualifications, les avantages (fidélisation).

Sur le plan juridique

- Garder à l'esprit que le dépôt d'un brevet peut renseigner sur l'existence d'une compétence-clé. Établir une stratégie interne en matière de propriété intellectuelle et, le cas échéant, se rapprocher d'un cabinet en propriété intellectuelle.
- Formaliser dans les contrats de travail des clauses de confidentialité (durée, champs, etc.), de loyauté (non-concurrence clairement définie dans le temps, l'espace géographique et la contrepartie financière, afin d'éviter son annulation), de dédit-formation (remboursement de la formation par le collaborateur). Veiller à harmoniser ces clauses pour l'ensemble de l'établissement.
- Souscrire, le cas échéant, pour une compétence rare, une police d'assurance « homme-clé » ; penser à son adaptation et à son renouvellement.

Agir face à la perte

Réactions à l'annonce du départ

- Analyser immédiatement l'impact potentiel de la perte subie en termes qualitatifs (image), quantitatifs, financiers et stratégiques.
- Sécuriser le départ pour que le préavis ne soit pas source de problèmes pour l'établissement : procédures informatiques, documents officiels, badges d'accès, clefs, téléphones, etc.
- Rappeler à l'intéressé le cadre contractuel dans lequel il se situe et en particulier, les contraintes le liant par des clauses spécifiques.
- Redistribuer en interne les compétences-clefs perdues (ateliers de travail, séminaires internes, etc.). Transmettre les projets en cours, évaluer les tâches à terminer et celles accomplies.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Éviter ou gérer la perte d'une compétence-clé

Après le départ

- Mettre en place une veille spécifique afin de mesurer l'impact de la perte subie : quel concurrent a bénéficié de la compétence-clé ? Y a-t-il eu des divulgations sur le savoir-faire de l'établissement ? Les clauses ont-elles été respectées par le collaborateur et l'établissement ? etc.
- En interne, identifier précisément le « manque » observé et déterminer rapidement l'organisation interne permettant d'y pallier aux mieux en attendant un éventuel recrutement externe.
- Effectuer un retour d'expérience avec les collègues, les supérieurs et la DRH pour comprendre les raisons de cette perte de compétence-clé et mettre en place les mesures correctives nécessaires.

RÉFÉRENTS

- **CCI France, CGPME, CNB, HFDS, MEDEF, Ordre des avocats de Paris.**

O RGANISATIONNEL
T ECHNIQUE

Gérer ses archives et ses rejets

fiche 14

Les archives et les rejets de l'établissement peuvent renseigner des concurrents, ou des acteurs malveillants à la recherche d'informations technique, commerciale et même privée.
Il convient d'y accorder une attention particulière.

O Archives papiers et numériques

- Mettre en place une solution de suivi, un plan de classement et d'archivage spécifique pour les supports d'informations dont la sensibilité est stratégique.
- Former les collaborateurs à une gestion précise (enregistrement, niveau de sensibilité, durée de vie, etc.) des documents qu'ils créent (notes manuscrites, courriels, fichiers numériques, bordereaux, etc.).
- Mettre en place une procédure de traçabilité de l'accès aux différentes formes d'archives.
- En cas d'externalisation des archives numériques, encadrer strictement le contrat avec le prestataire.
- Insérer dans les contrats de location de matériels informatiques (serveur, unité centrale, imprimante multifonctions, télécopieur, etc.) des clauses spécifiques prévoyant la conservation des disques durs ou leur destruction sécurisée.
- Fournir et gérer les supports d'archivage amovibles vérifiés, notamment dans le cadre du télétravail (clé USB, disque dur externe, etc.). Interdire tout support d'archivage privé.

T

- Conserver les archives papier et numériques dans des locaux sécurisés et adaptés (restriction d'accès, protection contre les sinistres, etc.).
- Archiver les données stratégiques avec des précautions particulières (coffre-fort, cryptage, etc.).
- Tester régulièrement l'intégrité des documents numériques archivés.

O Déchets matériels et numériques

- Définir une politique interne de gestion des déchets professionnels, y compris dans le cadre du télétravail.
- Sensibiliser les collaborateurs au fait qu'une simple suppression des données ne constitue pas une réelle destruction.
- Sélectionner ses prestataires extérieurs en charge de l'évacuation des déchets sur des critères de fiabilité et de sûreté.
- Identifier précisément les personnes physiques en charge de l'évacuation des déchets (ménage, etc.). Faire respecter l'obligation du port du badge apparent.

T

- Mettre à disposition un broyeur à coupe croisée pour détruire de manière sécurisée les documents sensibles (papiers, CD, DVD, etc.).
- Installer sur chaque poste de travail un logiciel d'effacement sécurisé.
- Détruire ou effacer de façon sécurisée les mémoires internes des équipements informatiques en fin de vie ou en fin de contrat (imprimante, fax, photocopieur, etc.).
- Détruire de façon sécurisée les prototypes et résidus de matériaux innovants mis au rebut afin d'empêcher toute récupération à des fins de rétro-ingénierie.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

POUR ALLER PLUS LOIN

- L'ANSSI publie sur son site une liste de logiciels de suppression de données que vous pouvez utiliser en toute confiance.

http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/

- **Norme française NF Z42-013 sur l'archivage électronique** : cette norme AFNOR porte sur les spécifications pour la conception et l'exploitation des systèmes informatiques utilisés pour l'archivage électronique. Cette norme est devenue une norme internationale publiée sous le titre ISO 14641-1.

RÉFÉRENTS

- **ANSSI, DPSD, DRCI, Gendarmerie nationale.**

Maîtriser sa communication au quotidien

fiche 15

Une communication non maitrisée peut entrainer une fuite d'informations stratégiques préjudiciable pour l'établissement. Il est donc toujours nécessaire de bien évaluer la sensibilité des informations qui sont communiquées, que ce soit sur le plan professionnel ou personnel.

O

- Une communication professionnelle doit être centralisée et maîtrisée :
  - demander à tous les employés de l'établissement de faire valider, préalablement et systématiquement, auprès de la direction ou de la personne chargée de la communication, tout contact avec un journaliste, un attaché parlementaire, un analyste financier, le rédacteur d'un rapport ou d'un livre, etc ;
  - toujours se demander si les interlocuteurs et les questions sont légitimes, et s'assurer qu'ils s'inscrivent dans la stratégie de communication. Si possible, demander que soit communiquée à l'avance la liste des questions qui vont être posées et s'assurer de pouvoir relire la publication avant parution ;
  - peser précisément les conséquences, positives mais aussi négatives, de ce qui peut être dit ou écrit sur la base des informations communiquées.
- Préparer précisément ce qui peut être dit lors des événements de communication à l'extérieur (salons professionnels, lancement de produits, colloques, etc.). Identifier les informations sensibles qui doivent rester confidentielles et ne communiquer que ce qui est utile commercialement.
- Sur les supports de communication (cartes de visite, signature électronique, etc.), n'indiquer que les coordonnées strictement nécessaires à la relation professionnelle.
- Sensibiliser les collaborateurs aux risques des sollicitations urgentes, inhabituelles et ne respectant pas les procédures. Cela peut cacher une manœuvre visant à s'approprier indûment une information ou de l'argent (demande de virement en urgence, etc.) :
  - exiger qu'une procédure d'urgence validée par l'établissement pour ce type de situations soit respectée en toutes circonstances.
- S'assurer de la légitimité des démarches d'audits ou de contrôle :
  - vérifier l'identité des intervenants en demandant à voir leur carte professionnelle ;
  - s'assurer auprès des administrations ou organismes auxquels ils prétendent appartenir qu'ils en sont bien mandatés ;
  - exiger une lettre de mission.

C

- Toujours vérifier l'identité et la légitimité de l'émetteur avant de répondre à un questionnaire, notamment par courriel.
- Être mesuré dans ses publications sur les réseaux sociaux, que ce soit sur le plan professionnel ou privé. Toutes les informations personnelles qui sont postées peuvent être exploitées pour gagner la confiance.
- Rester bref et évasif avec des interlocuteurs trop insistants. Ne donner que des réponses générales.
- Rester lucide et sur la réserve lorsqu'un interlocuteur promet des gains exceptionnels ou évoque des risques dramatiques pour l'établissement.
  - Ne pas se laisser dominer par quelqu'un qui se targue d'être un expert et semble connaître beaucoup de monde, en particulier les personnes qui font autorité. Ne jamais se sentir contraint de raconter les détails de l'activité de l'établissement à une personne dont le statut, la fonction ou l'expertise supposée semblent dignes de confiance.
  - Ne pas se laisser impressionner par quelqu'un qui fait des confidences, se montre alarmiste ou pressant.
  - Ne pas sur-réagir aux critiques ou aux mises en cause qui concernent l'établissement : solidité financière, qualité de l'activité, concurrents, etc.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

POUR ALLER PLUS LOIN

Si vous pensez que vous êtes victime d'une action intrusive, récupérez autant d'informations que possible (numéro de téléphone, numéro et type de voiture, adresse mél, description d'un individu, carte de visite, questionnaire, etc.) et alertez les services de l'État. Demandez à vos collaborateurs de vous alerter ou d'alerter le responsable sûreté de l'établissement.

Élicitation/Ingénierie sociale – Technique de communication, intrusive mais pas illégale, qui consiste à manipuler son interlocuteur en usant de ressorts psychologiques (besoin de reconnaissance, séduction, amitié feinte, etc.) afin d'obtenir de sa part des informations qu'il n'aurait pas spontanément délivrées. Elle repose souvent sur une étude préalable de l'environnement personnel et/ou professionnel de la cible.

Name-dropping – Action qui consiste à évoquer avec son interlocuteur des noms de personnes qui font autorité dans leur domaine, en laissant entendre qu'on les connaît parfaitement.

RÉFÉRENTS

- **CCI France, CGPME, CNB, DCRI, DPSD, Gendarmerie nationale, Ordre des avocats de Paris.**

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Les réseaux sociaux et la e-réputation

fiche 16

L'utilisation des réseaux sociaux peut être privée et/ou professionnelle. Il faut néanmoins être bien conscient qu'une utilisation considérée comme privée peut, bien souvent, avoir des répercussions professionnelles.

O Le salarié sur les réseaux sociaux

- Sensibiliser les personnels, en lien avec l'entreprise, grâce à une charte d'utilisation des réseaux sociaux. Leur rappeler les droits et devoirs de tout employé, comme par exemple la loyauté, la discrétion ou le devoir de réserve.
- Prévoir, dans le contrat de travail, une clause spécifique relative à la communication externe.

C

- Ne jamais utiliser le même mot de passe pour accéder à un réseau social et aux ressources informatiques de l'entreprise.
- Prendre conscience qu'une information (texte, photo, etc.) publiée sur internet n'appartient plus à celui qui la met en ligne et peut difficilement être effacée.
- Éviter de communiquer des informations personnelles précises sur les réseaux sociaux (date et lieu de naissance, numéro de téléphone, etc.).
- Etre attentif aux données de géolocalisation ouvertes sur les réseaux sociaux. Elles peuvent apporter des renseignements sur son emploi du temps professionnel : absence, vacances, missions, etc.
- Ne jamais publier de photo, ni y identifier quelqu'un, sans un accord exprès de la personne concernée.
- Veiller à ce que les informations publiées sur les réseaux sociaux ne comportent pas d'information sensible concernant l'entreprise : organigramme précis, systèmes techniques utilisés, mission à l'étranger, contrat en cours de négociation, conflit social frémissant, etc.
- Être vigilant quant aux sollicitations via les réseaux sociaux. Ils sont fréquemment utilisés comme vecteur d'ingérence : virus, usurpation d'identité, ingénierie sociale, etc.
- Toujours se déconnecter du réseau social après l'avoir utilisé, même sur l'ordinateur personnel. S'il n'est pas verrouillé, une utilisation par une tierce personne est possible, avec des conséquences multiples : usurpation d'identité, accès aux données, canular, etc.

O L'entreprise sur les réseaux sociaux

- Identifier correctement le besoin en communication de l'entreprise sur les réseaux sociaux. Une audience faible peut avoir un effet contreproductif.
- Choisir correctement la plateforme de communication. Chacune a ses spécificités en termes de cibles, d'instantanéité, de fréquence d'utilisation, etc.
- Déterminer, après une analyse de risques, qui devra prendre en compte le fait que tous les destinataires ne sont pas forcément bienveillants :

  - quelles informations communiquer ?
  - Qui valide les informations ?
  - Qui les publie ?
  - Quel rythme de publication va être observé ?

- Être très attentif à la cohérence et à l'intégrité des messages de communication externe, eu égard aux réalités de l'établissement.
- Mettre en place une veille rigoureuse sur les noms de la société, de ses dirigeants et des marques afin d'être en capacité de réagir rapidement contre les dénigrements, les « **cybersquats** » ou toute autre action à l'encontre de l'entreprise.
- Privilégier la communication interne. Apprendre une nouvelle sur un réseau social ou par la presse, plutôt que par ses dirigeants peut être déstabilisant pour un employé.
- Désigner un administrateur du compte qui suivra rigoureusement les évolutions techniques du réseau social : sécurité, confidentialité, etc.

T

- Paramétrer les comptes selon les objectifs d'utilisation recherchés (public, semi-public, privé).
- Utiliser un mot de passe robuste afin d'éviter toute utilisation frauduleuse du compte de l'entreprise sur le réseau social. La diffusion de celui-ci sera strictement encadrée.

Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

C

- Signaler tout abus à l'opérateur du réseau social, par l'intermédiaire des pages de contact prévues à cet effet.
- Ne pas hésiter à solliciter la commission nationale de l'informatique et des libertés (CNIL) ou à déposer plainte. L'assistance d'un conseiller juridique doit alors être envisagée.
- Réfléchir, en cas de recours, à l'impact médiatique qui pourra en résulter, souvent démultiplié par la viralité des réseaux.
- Prendre garde à ne pas sur-réagir à chaud en cas de rumeur, de tentative de déstabilisation, de désinformation ou d'intoxication concernant votre entreprise. Faire une analyse rigoureuse des tenants et aboutissants des réactions envisagées avant de les engager.

MOT-CLÉ

Cybersquat :
Acte qui consiste à déposer un nom de domaine en usurpant le nom de l'entreprise ou celui de ses marques (nasa.com était un site pornographique alors que le site officiel est nasa.org, par exemple). Il existe une variante : le "typosquat" qui repose sur une orthographe incorrecte (elyseee.fr pour elysee.fr, par exemple).

POUR ALLER PLUS LOIN

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Guide d'hygiène informatique – http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Recommandations de sécurité relatives aux mots de passe – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

RÉFÉRENTS

- **ANSSI, CCI France, CGPME, CNB, HFDS du ministère de tutelle, MEDEF, Odre des avocats de Paris.**

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Se déplacer à l'étranger

fiche 17

Pour de nombreuses entreprises ou organismes de recherche, voyager est indispensable. Présence, visibilité et démonstration de qualités sur la scène internationale conditionnent, en effet l'accès à de nouvelles opportunités. Lors de ces déplacements à l'étranger, les personnes sont cependant beaucoup plus vulnérables que dans leur environnement habituel, ce qui n'est pas sans risque pour leur sécurité et celle de l'information qu'ils détiennent.

O Préparation du déplacement

- Prendre en compte la situation politico-sécuritaire : consulter le site internet du ministère des affaires étrangères et se rapprocher de son assurance.
- Se renseigner sur les us et coutumes et législations locales.
- En cas de voyage dans les pays à risque :
  - s'inscrire préalablement sur le site *Ariane* (site dédié) du ministère des affaires étrangères ;
  - signaler son déplacement à l'ambassade ou au consulat ;
  - convenir d'un contact à intervalle régulier en France.
- Garder à l'esprit que la menace d'ingérence économique n'est pas limitée aux seuls pays dits "à risque".
- Préparer les numéros de téléphone d'urgence : assistance et services diplomatiques.
- Disposer d'une copie de ses papiers d'identité, rangés dans un endroit distinct des originaux. Ils peuvent être déposés sur le site *mon.service-public.fr*, portail internet gratuit et confidentiel permettant de créer facilement un espace de stockage accessible 24H/24.
- En cas de traitement médical, se munir des copies des ordonnances afin de justifier la possession de produits, parfois interdits dans certains pays.
- Laisser en France les documents qui ne sont pas indispensables à la mission et dont le vol, la consultation ou la confiscation pourrait porter préjudice à ses activités.
- Organiser le transport des échantillons ou des matériels professionnels lors d'un déplacement à l'étranger en se rapprochant de la chambre de commerce et d'industrie.

O
- Se renseigner (douanes, ambassades, conseillers du Commerce extérieur) sur les législations et les pratiques locales, notamment douanières, afin de connaître les modalités d'entrée de marchandises et de matériels sur le territoire tiers : déclaration préalable, normes, sécurité sanitaire, etc.
- Déclarer la marchandise dès l'arrivée dans le pays tiers (hors UE) auprès des autorités douanières compétentes (visa du **carnet ATA** par exemple).

T
- En cas de sensibilité particulière du déplacement, prévoir un ordinateur portable et un téléphone dédiés.
- Désactiver les ports USB des ordinateurs portables depuis le panneau de configuration.

C Pendant le séjour

- Ne pas considérer le coffre-fort de l'hôtel comme un lieu sûr pour stocker des informations sensibles.
- Surveiller en permanence ses documents et ses moyens nomades de communication. Les conserver avec soi.
- Être prudent dans les communications : garder à l'esprit que les conversations au téléphone ou par internet peuvent être interceptées (WiFi des hôtels, etc.).
- Rester vigilant dans ses relations et son comportement :
  - éviter les sollicitations impromptues, demandées à titre amical ;
  - éviter de s'exposer à tout ce qui pourrait relever de la provocation, y compris de ses partenaires, dans le cas d'une demande sortant du cadre officiel ;
  - éviter les excès de toute nature susceptibles d'être utilisés à son encontre.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

C
- Eviter les signes d'appartenance ou d'identification à un établissement ou à une organisation.
- Prendre systématiquement les cartes de visites et coordonnées de ses interlocuteurs.
- Rester discret dans les lieux publics : éviter les conversations sensibles ou confidentielles dans les chambres d'hôtel, chez un particulier, au restaurant.
- Dans les salons et réunions internationaux, maîtriser l'information à diffuser, se méfier des faux clients et des sollicitations multiples.
- Rester vigilant dans ses déplacements.
- Respecter rigoureusement les lois, us et coutumes du pays d'accueil.

O Après le séjour

- Organiser des échanges de bonnes pratiques avec des collègues ou des confrères sur le déplacement dans le pays.
- Conserver les documents prouvant que la marchandise transportée n'a pas été acquise dans un pays tiers (**carnet ATA** ou déclaration d'exportation temporaire sous conditions), afin de ne pas se voir réclamer le paiement de droits de douane éventuels ou de la TVA.

T
- Ne pas utiliser les supports informatiques remis lors de votre voyage (clés USB, etc.) avant de les avoir minutieusement fait analyser.

C
- Rendre compte de tout fait qui aura suscité l'étonnement.

MOT-CLÉ

Carnet ATA :
Du nom de la convention ATA de Bruxelles de 1961, il est délivré par les chambres de commerce et d'industrie, il se substitue aux différents documents douaniers normalement requis pour une opération d'importation ou d'exportation temporaires et permet ainsi de réaliser ces opérations en suspension de droits et taxes.

POUR ALLER PLUS LOIN

Ministère des affaires étrangères (MAE)
- Conseils aux voyageurs – http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs.html
- Plate-forme Ariane (déclarer ses voyages à l'étranger) – https://pastel.diplomatie.gouv.fr/fildariane/dyn/public/login.html

Agence nationale de la sécurité des systèmes d'information (ANSSI)
- Passeport de conseils aux voyageurs
  http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

Club des directeurs de sécurité des entreprises (CDSE)
- Passeport pour la sécurité des voyageurs salariés à l'étranger – https://www.cdse.fr/passeport-securite-des-voyageurs

Douanes
- Les régimes suspensifs douaniers et fiscaux – http://www.douane.gouv.fr/page.asp?id=231

Direction de la coopération internationale (DCI)
La direction de la coopération internationale, direction commune de la police et de la gendarmerie nationales, est en mesure de vous conseiller, aussi bien dans la phase préparatoire de vos déplacements que lors de vos séjours professionnels à l'étranger.

Contact DCI : dci-partenariats@interieur.gouv.fr

RÉFÉRENTS

- **CCI France, CGPME, DCRI, DPSD, Gendarmerie nationale, HFDS du ministère de tutelle, MEDEF.**

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Participer à un salon professionnel

fiche 18

Si les salons professionnels sont souvent porteurs de nouvelles opportunités professionnelles, ils sont également un point d'attention particulier pour les acteurs économiques les moins loyaux. Pour « exposer sans trop s'exposer » il est donc indispensable de préparer rigoureusement ces événements en intégrant de solides paramètres de sécurité.

O Avant le salon

- Définir les informations qui pourront être ou non diffusées sur le salon. Éviter les dossiers de presse trop complets. Préparer par écrit, avec les collaborateurs et/ou une agence de communication, les éléments de langage sur les sujets délicats ou indiscrets (innovation, savoir-faire, etc.).
- Désigner un responsable en charge du matériel sensible lors du montage et du démontage du stand, périodes particulièrement exposées.
- Si possible, choisir l'emplacement de son stand en fonction de la concurrence, ni trop près ni trop loin.
- Ne pas placer les matériels sensibles en bordure du stand. Prévoir, le cas échéant, des vitrines fermant à clé.
- Prévoir une zone permettant des échanges en toute discrétion.
- Sensibiliser les collaborateurs sur les risques de manipulation (flatterie, partage d'un intérêt commun, fausse vérité, information gratuite, etc.).
- Vérifier la couverture assurantielle de l'établissement par rapport aux salons.

T

- Limiter autant que possible le nombre de documents ou matériels sensibles.
- Préparer un ordinateur spécialement dédié aux présentations pour le salon et dénué de toutes données sensibles. Verrouiller les ports USB de tous les autres ordinateurs, une clé USB pouvant contenir un logiciel malveillant.
- Mettre en place une déchiqueteuse permettant de détruire de façon sécurisée les documents de travail (devis, schémas, etc.).
- Développer, si possible, des prototypes ou des répliques anodines pouvant être exposés sans risque de dévoiler une caractéristique majeure du produit ou de permettre un prélèvement, notamment quand l'innovation réside dans les matériaux.

T Pendant le salon

- Désactiver les fonctions Bluetooth et WiFi des appareils nomades de communication.
- Sécuriser le matériel informatique et de démonstration du stand : antivols, vitrines fermées à clé, etc.
- Utiliser un mot de passe personnel dédié au salon composé au minimum de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien personnel et ne figurant pas dans le dictionnaire.
- En cas d'échange de documents lors d'une présentation commerciale, utiliser une clef USB destinée uniquement à cet usage, et effacer ensuite les données avec un logiciel d'effacement sécurisé.

C

- Éviter d'utiliser les moyens de communication mis à disposition (borne WiFi gratuite, etc.).
- Se méfier des rencontres « amicales spontanées ».
- Demander systématiquement une carte de visite à ceux qui témoignent un intérêt aux produits, saisir les informations enregistrées sur leur badge et vérifier l'identité de ses interlocuteurs.
- Éviter de répondre aux sondages, questionnaires et enquêtes multiples. Identifier clairement les demandeurs et s'assurer de la destination des informations transmises.
- Être vigilant en permanence : la fatigue gagne souvent en fin de journée et vers la fin du salon, et avec elle la vulnérabilité augmente.
- Éviter les entretiens et les conversations sensibles dans les lieux publics (transports, restaurants, hôtels, etc.)
- Ne pas aborder de sujets confidentiels au téléphone.
- Être vigilant lors des échanges dans les événements connexes au salon (dîners, cocktails, conférences, pause déjeuner, machine à café, etc.).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

Participer à un salon professionnel

C

- Ne jamais laisser de documents sensibles sans surveillance, les conserver avec soi. Aucune réserve n'est sûre (coffre de la voiture, coffre-fort de la chambre d'hôtel, réserve du stand, etc.).
- Ne jamais laisser sans surveillance les matériels à risque (prototypes, maquettes, ordinateurs personnels, etc.), notamment hors des heures d'exposition.
- Surveiller constamment ses outils de travail (mallettes, ordinateurs, téléphones portables, etc.).

O

Après le salon

- Lors de la clôture, faire place nette sur le stand et vérifier l'ensemble des matériels et documents.

O

- « Débriefing » et rédaction d'un rapport d'étonnement, relatant tout problème ou événement inattendu survenu lors du salon.
- Exploiter les cartes de visites des « démarcheurs » (se demander s'ils sont des clients ou des concurrents potentiels).
- Établir un bilan de l'activité et suivre les commentaires au sein de la profession et des médias (forums internet, presse spécialisée, etc.).
- Aviser les services de l'État de toute tentative d'ingérence et de tout événement ayant suscité l'étonnement durant le salon.

RÉFÉRENTS

- **CCI France, CGPME, DCRI, DPSD, Gendarmerie nationale, MEDEF.**

O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Sécuriser ses flux de marchandises

fiche 19

Maîtriser ses flux de marchandises permet de préserver ses atouts industriels tout en participant à la sécurisation de l'ensemble de la chaîne logistique.

O Comment sécuriser ses flux de marchandises entrants ?

- Identifier tous les acteurs de la chaîne d'approvisionnement, du fournisseur au transporteur final, en passant par l'ensemble des prestataires intermédiaires : acheteur, assureur, affréteur et transitaire, compagnie maritime/aérienne, stockeur, commissionnaire en douane, etc.
- Maîtriser, dans la mesure du possible, cette chaîne en organisant le pré-acheminement (recours à des ***Incoterms*** spécifiques) ou en s'assurant que son fournisseur fasse appel à des prestataires fiables (certifiés opérateurs économiques agréés, par exemple).
- Développer une politique interne exigeante dans le choix des fournisseurs, des prestataires de transport et des autres prestataires : privilégier des partenaires connus et fiables, vérifier leur solvabilité, établir des cahiers des charges stricts, etc.
- Mettre en place des procédures de contrôle du transport entrant, permettant une traçabilité réelle, à chaque étape de l'acheminement des marchandises : calendrier prévisionnel des arrivées, procédure de traitement des arrivées de marchandises imprévues, contrôle de concordance marchandise attendue/réceptionnée, etc.
- Prévoir un filtrage à l'entrée de l'établissement (poste de garde, service de réception, etc.) contrôlant le bien fondé de la livraison et l'identité du transporteur, et orientant vers l'aire de réception du fret.
- Sensibiliser l'ensemble du personnel à tout mouvement inhabituel de marchandise.

Comment garantir la bonne intégrité des unités de fret au sein de l'établissement ?

- Délimiter précisément des aires sécurisées de réception : quais de déchargement et zones de stockage des unités de fret.
- Limiter l'accès à ces zones aux seuls personnels et entreprises externes autorisés et sensibilisés aux enjeux liés à la sécurité/sûreté (notes internes, protocole de transport).
- Vérifier l'intégrité des unités de fret à réception : scellés commerciaux intacts, intégrité physique du moyen de transport.
- Contrôler l'état des marchandises : qualité/quantité.
- Procéder à la vérification systématique des documents de transport (cohérence, lisibilité, etc.).
- Enregistrer précisément tous les problèmes relevés afin de mettre en place des mesures correctives.

Comment sécuriser le stockage des marchandises ?

- Privilégier le stockage en intérieur, surtout si la marchandise est de forte valeur ou susceptible d'attiser la convoitise. En cas de stockage extérieur, désigner une aire de stockage bénéficiant d'un éclairage adapté, si possible sous surveillance vidéo et éloignée des entrées et enceintes de la société. Dissimuler la nature des marchandises, par exemple sous une bâche.
- Limiter strictement l'accès à la zone de stockage aux seules personnes autorisées.
- Mettre en œuvre des contrôles internes : procédures d'inventaire régulier, enquête sur les irrégularités, mesures correctives, etc.
- Mettre en place un système de surveillance proportionné aux risques liés à la nature de la marchandise.

Comment protéger sa zone de production de marchandises ?

- Définir une procédure régissant l'accès afin de garantir la sécurité et la sûreté des processus de production.
- Sensibiliser le personnel de production au respect de cette procédure.

T

- Mettre en place un système de surveillance proportionnel aux risques liés à la préservation du secret industriel.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

Sécuriser ses flux de marchandises

O Comment sécuriser ses flux de marchandises sortants ?

- Formaliser des procédures de contrôle du transport sortant.
- Délimiter précisément des aires de chargement : quais de chargement, zones de stockage des unités de fret.
- Mettre en place une procédure de chargement des marchandises (seul le personnel de la société est autorisé à charger et non le chauffeur du camion, par exemple) avec un contrôle de cohérence des marchandises chargées.
- Vérifier la nécessité ou non d'une licence d'exportation : **biens à double usage**.
- Limiter strictement l'accès à la zone de chargement aux seules personnes autorisées.

T
- Apposer des scellés sur les marchandises sortantes. Stocker ces scellés dans un emplacement sécurisé et tenir un registre de suivi de ce stock.

O Comment sécuriser les acheminements ?

- Sélectionner ses partenaires commerciaux selon des critères de fiabilité : procédure d'identification, encadrement du recours à la sous-traitance, etc.
- Maîtriser, dans la mesure du possible, l'acheminement : soit en choisissant des ***Incoterms*** spécifiques, soit en sensibilisant l'acheteur sur la nécessité de recourir à des prestataires fiables.
- Prévoir un suivi des prestataires en matière de sûreté : choix de prestataires agréés, signature de **déclaration de sûreté**, intégration d'une clause de sûreté dans les contrats avec les prestataires réguliers, audits des prestataires…

MOTS-CLÉS

Biens à double usage (BDU) :
Par biens à double usage on entend, « les produits, y compris les logiciels et les technologies (ainsi que la transmission de logiciels ou de technologies, par voie électronique, par télécopieur ou par téléphone vers une destination située en dehors de l'Union européenne) susceptibles d'avoir une utilisation tant civile que militaire ». Ils sont repris dans une liste annexée au règlement européen qui définit le cadre juridique applicable en la matière. Ce sont des biens sensibles qui, dans la plupart des cas, sont destinés à des applications civiles, mais qui peuvent être utilisés à des fins militaires ou qui pourraient sensiblement renforcer les capacités militaires des pays qui les acquièrent.

Déclaration de sûreté :
Document permettant à une société certifiée OEA d'encadrer juridiquement les prestations réalisées par un prestataire pour son compte.

Incoterms :
« *International Commercial Terms* » ou Conditions internationales de vente. Le but des *Incoterms* est de définir les obligations du vendeur et de l'acheteur lors d'une transaction commerciale, le plus souvent internationale, mais qui peut également s'établir entre des opérateurs nationaux ou communautaires. Ils concernent essentiellement les obligations des parties à un contrat de vente, relatives à la livraison de la marchandise vendue, à la répartition des frais et aux risques liés à cette marchandise, ainsi que la charge des formalités d'export et d'import.

Opérateur économique agréé (OEA) :
La certification OEA atteste le respect de plusieurs critères liés à la gestion de la réglementation douanière et à la prise en compte des risques de sécurité/sûreté. Il existe trois types de certification : OEA Simplifications douanières (OEAC) ; OEA Sécurité/Sûreté (OEAS) ; OEA Simplifications douanières et Sécurité/Sûreté (OEAF). Les entreprises certifiées OEAS et OEAF ont démontré une prise en compte renforcée des risques liés à la sécurité et à la sûreté. Toutes les entreprises européennes intégrant la chaine logistique internationale (fabricants, exportateurs, importateurs, transporteurs, stockeurs, commissionnaires, etc.) sont éligibles à la certification OEA.

POUR ALLER PLUS LOIN

Douane

- En savoir plus sur le statut d'opérateur économique agréé et déposer sa demande – http://www.douane.budget.gouv.fr/page.asp?id=3421
- Guide sur les exportations de biens et technologies à double usage – http://www.douane.gouv.fr/data/file/8039.pdf
- Informations pratiques sur les Incoterms – http://www.douane.gouv.fr/page.asp?id=3625

Direction générale de la compétitivité, de l'industrie et des services (DGCIS)
Service des biens à double usage (SDBU)

www.dgcis.gouv.fr/biens-double-usage/accueil

RÉFÉRENTS

- **CCI France, Douane.**

Protéger juridiquement son établissement

fiche 20

De plus en plus d'acteurs économiques utilisent les failles du droit positif pour acquérir de l'information en toute légalité, même si ce n'est pas en toute loyauté. Protéger juridiquement son établissement permet de repousser les limites des barrières à franchir pour obtenir des informations, sans entrer clairement dans l'illégalité.

- Faire vérifier par un expert que les activités de l'établissement sont suffisamment protégées sur le plan juridique : conditions générales de vente, contrats de travail, droits de propriété intellectuelle.
- Se méfier des modèles de statuts et de contrats en libre accès sur internet. Ils ne protègent l'établissement que de façon imparfaite, soit parce qu'inadaptés à la situation réelle, soit parce que la rupture des liens contractuels n'a pas été valablement envisagée.
- Prévoir des **clauses de confidentialité** dans les contrats de travail des collaborateurs, des intérimaires et dans les conventions de stages.
- Prévoir des **clauses de non-concurrence** dans les contrats de travail des personnes occupant des postes clés.
- Prévoir des **clauses spécifiques pour le partage d'information** et la confidentialité dans les contrats avec les fournisseurs, les sous-traitants et les distributeurs. Prévoir des **clauses de non-débauchage** pour les collaborateurs avec lesquels ils sont en contact.
- Vérifier, dans les contrats avec des tiers les clauses liées au règlement des litiges : veiller à bien choisir le tribunal compétent ; prévoir des clauses de médiation et/ou d'arbitrage adaptées aux enjeux.
- Veiller à protéger efficacement, en liaison avec un expert et dans des conditions adaptée à la réalité de ses besoins, tous les éléments immatériels de l'établissement qui sont susceptibles aujourd'hui de faire l'objet de contrefaçons ou d'usurpation : nom de la société, nom de domaine, marque, modèle, brevet, etc.
- Dénoncer immédiatement auprès de la justice les faux procès, faux appels d'offres, faux brevets, etc. qui paraissent uniquement destinés à recueillir de l'information.
- Prévoir de faire évoluer les contrats et les protections juridiques de l'établissement au fur et à mesure de l'évolution de l'établissement lui-même.
- En cas d'inquiétude ou d'incident avéré, prendre rapidement contact avec son avocat ou son conseil juridique et, si nécessaire, avec les services compétents de l'État.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

Protéger juridiquement son établissement

MOTS-CLÉS

Clauses de confidentialité :
article d'un contrat qui a pour objectif de garantir la non-divulgation à des tiers d'informations dont la ou les personne(s) aurai(en)t connaissance de par ses (leurs) fonctions. Peut s'appliquer à un salarié ou à un partenaire : fournisseur, distributeur, société en joint-venture ou distributeur.

Clause de non-concurrence :
clause permettant à un employeur de se prémunir contre la concurrence que pourrait lui faire un salarié à l'expiration du contrat de travail.

Clause de non-débauchage :
cette clause interdit à la société qui signe le contrat de débaucher l'employé missionné, sous peine de verser un dédit financier plus ou moins important à son client, partenaire etc. Elle est aussi appelée clause de non-sollicitation.

Clauses spécifiques pour le partage d'information :
la clause de partage d'information définit les modalités du partage et établit les règles de coopération entre l'entreprise et les tiers avec lesquels elle est en affaires en matière d'information. Elle vise à s'assurer que les informations nécessaires et suffisantes ont bien été portées à la connaissance du tiers, notamment pour l'exécution de sa mission, ou, à l'inverse, que certaines informations liées à la réalisation d'une mission seront bien intégrées, en toute transparence, aux rapports, au suivi, aux bilans.

POUR ALLER PLUS LOIN

Institut national de la propriété industrielle (INPI)
- www.inpi.fr
- www.inpi.fr/fileadmin/mediatheque/pdf/brochure_proteger_ses_creations.pdf

Direction générale de la compétitivité, de l'industrie et des services (DGCIS)
- www.dgcis.gouv.fr

Autorité de la concurrence
- www.autoritedelaconcurrence.fr

RÉFÉRENTS

- **CNB, Douane, Ordre des avocats de Paris.**

Sécuriser ses relations commerciales

fiche 21

La construction de relations commerciales avec des partenaires extérieurs (financeurs, clients, fournisseurs, prestataires, etc.) fait partie de la vie quotidienne de l'établissement. Ces relations constituent néanmoins des actes dont les conséquences peuvent être gravement préjudiciables s'ils ne sont pas réalisés avec la vigilance et la rigueur nécessaires.

O

- Mettre en place une veille sur ses principaux fournisseurs, distributeurs, et clients (actualités commerciales, évolution du management, difficultés financières, etc.) et l'actualiser régulièrement.
- Porter une attention particulière à ne diffuser que les informations strictement nécessaires, lors des appels d'offres entrants et sortants. Ne pas hésiter à mettre en place des clauses de propriété intellectuelle et de confidentialité sur les informations diffusées à ces occasions. Lire attentivement celles qui sont proposées par les futurs partenaires.
- Adapter ses conditions générales de vente en fonction du type de clientèle (particuliers, professionnels, distributeurs).
- Éviter d'utiliser des modèles de contrats préétablis, souvent mal adaptés à la spécificité de la relation.
- Dans le cas des contrats exports, rédiger le contrat dans une langue parfaitement maîtrisée. Ne pas hésiter à se faire assister par un organisme spécialisé, par un interprète et par un juriste reconnu localement.
- Inclure dans les contrats des clauses de médiation et/ou d'arbitrage. Analyser avec attention les enjeux liés au choix de la juridiction compétente.
- Prévoir dans les contrats avec les fournisseurs, les distributeurs, les partenaires, des clauses expresses relatives :
  - aux échanges d'information et de confidentialité (personnes habilitées, responsabilités respectives, stockage et destruction des informations, etc.) ;
  - au non-débauchage de personnel ;
  - au respect des législations applicables : emploi des mineurs, marchandage, corruption, etc. ;
  - à l'échantillonnage, au prototypage ;
  - à la non-concurrence, à l'obligation de signaler toute relation nouvelle avec un concurrent ;
  - aux pénalités en cas de rupture d'approvisionnement, de non-respect des délais de livraison et de défaut de qualité.
- Ne jamais prendre de décisions importantes pour l'établissement sur la base d'informations ou d'instructions non vérifiées.
- Faire signer les procédures de sécurité par les organismes prestataires (nettoyage, prestataires informatiques, etc.) intervenant sur les sites sensibles. S'assurer au préalable que ces prestataires sont en règle avec la législation en vigueur.

C

- Attendre, pour verser le premier acompte, que le contrat soit validé et signé par les personnes habilitées.
- Respecter rigoureusement la procédure interne de vérification pour toute opération engageant les finances de l'établissement.
- Demander une confirmation écrite pour tout acte engageant l'établissement et ses partenaires. Confirmer chaque échange ou entrevue par un courriel, un reçu ou un fax à l'en-tête de l'établissement.
- Ne jamais traiter avec des subordonnés du partenaire, ou du prestataire, sans avoir vérifié leur mandat.
- Veiller à ce que tous les exemplaires « originaux » des contrats soient numérotés, signés et paraphés. Ne laisser aucune page blanche, aucun blanc, signe ou rature sur les documents. Veiller à ce que chaque partie valide les corrections.
- Limiter le nombre de personnes impliquées dans les nouveaux projets, en externe (fournisseurs, distributeurs, etc.) comme en interne, tant que les clauses de confidentialité ne sont pas signées.
- Utiliser des salles de réunion plutôt que des bureaux pour les échanges ou séances de travail avec les clients, partenaires et/ou fournisseurs.
- Utiliser des équipements informatiques dédiés et « conditionnés » (PC, clef USB, etc.) lors des réunions avec les clients, partenaires et/ou fournisseurs.

Premier ministre
Délégation interministérielle à l'intelligence économique

RÉFÉRENTS

- **CCI France, CNB, CGPME, MEDEF, Ordre des avocats de Paris.**

Sécuriser ses relations avec les investisseurs

fiche 22

La levée de fonds est une étape importante dans la vie d'une entreprise ou d'un organisme de recherche. Outre savoir se protéger pour éviter une perte de contrôle de la gouvernance, la principale difficulté est de limiter les risques de pertes d'informations stratégiques de l'établissement tout en restant attractif.

Anticiper ou rechercher le contact avec un investisseur

- Définir son besoin de financement en précisant la vision stratégique de l'établissement. Les besoins à court terme ne doivent pas dicter les choix fondamentaux.
- Bien cadrer sa communication à destination des possibles investisseurs
- Éviter les fonds potentiellement hostiles ou activistes pouvant déstabiliser l'établissement. S'informer au préalable sur les intentions des partenaires potentiels et privilégier les partenariats financiers ayant démontré leurs qualités dans le passé. En cas de doute, prendre contact avec les pouvoirs publics pour obtenir un avis sur la probité d'un investisseur ou s'informer sur la réglementation en vigueur.

Avant et durant la négociation

- Veiller, dans un premier temps, à ne transmettre aucune information stratégique et confidentielle, dont l'exploitation par l'investisseur pourrait se révéler dangereuse en cas d'échec des négociations.
- Ne pas hésiter à questionner l'investisseur sur ses relations avec la concurrence, ou sur ses besoins spécifiques d'information.
- Demander une lettre d'intention de l'investisseur précisant les investigations qu'il envisage de conduire (aspects financiers, juridiques, due diligence, etc.).
- Rencontrer régulièrement les conseils de l'investisseur afin d'apprécier la crédibilité du projet engagé.
- Désigner un correspondant unique par lequel transiteront toutes les demandes d'information.
- Répertorier les informations stratégiques susceptibles d'être communiquées et anticiper les demandes d'informations afin de garantir la cohérence des réponses.
- Imposer la signature d'un accord-cadre de confidentialité qui pourra être assorti d'engagements de non-sollicitation du personnel et de non-concurrence. Faire signer par l'investisseur un acte par lequel celui-ci, et ses conseils, s'engagent à garder confidentielles, et à ne pas exploiter pour leur propre compte, toutes les informations portées à leur connaissance par l'établissement.
- Bien préparer, avec l'équipe dirigeante, chaque rencontre avec l'investisseur en précisant les conditions de communication des informations à caractère stratégique : objectifs, planification, programmes de recherche-développement, état des différentes négociations avec les prospects, modalités de recrutement du personnel, etc.
- S'assurer que, dans les contrats de travail des collaborateurs impliqués dans la négociation, figurent les clauses de confidentialité adaptées.
- Lors des investigations préalables :
  - regrouper dans un lieu unique (*data room*) l'ensemble des documents communiqués,
  - limiter la période d'investigation afin qu'elle n'empiète pas sur la phase de négociation,
  - avertir le personnel potentiellement concerné par la mission en cours,
  - encadrer les possibilités d'accès des auditeurs au réseau informatique de l'établissement (sécurisation de l'intranet, connexions WiFi, etc.) et aux moyens de copie susceptibles d'être utilisés : téléphone, scanner, micro avec webcam, etc.

Avril 2014

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Délégation interministérielle à l'intelligence économique

- Au cours des échanges avec les auditeurs :
  - éviter de laisser un collaborateur seul lors d'une rencontre afin de connaitre parfaitement la nature et le contenu des échanges,
  - lister précisément les informations transmises.
- En cas de nouveau pacte d'actionnaires :
  - porter une attention particulière aux clauses et dispositions statutaires qui, en cas de différend, pourraient être exploitées : droits de vote, nomination et révocation des dirigeants et administrateurs, minorité de blocage, accès et convocation aux assemblées générales, etc ;
  - définir par convention quels droits particuliers d'information et de communication externe peuvent être accordés aux actionnaires : droit à consultation préalable ou droit particulier d'expertise, par exemple.

POUR ALLER PLUS LOIN

« 10 fiches pratiques : levée de fonds et maîtrise de l'information stratégique », HRIE 2007 – http://www.intelligence-economique.gouv.fr

RÉFÉRENTS

- **CCI France, CGPME, CNB, MEDEF, Ordre des avocats de Paris.**

Annuaire des partenaires

Fiches pratiques de sécurité économique

MOT-CLÉ

Haut fonctionnaire de défense et de sécurité (HFDS) :
Chaque ministre est assisté par un haut fonctionnaire de défense et de sécurité pour toutes les questions relatives à la défense et aux situations d'urgence affectant la défense, la sécurité et la vie de la nation ; dans son domaine il a autorité sur l'ensemble des directions et services de son ministère et dispose, en propre, d'un service spécialisé. S'il veille notamment à la diffusion des plans, des doctrines d'emploi et des directives gouvernementales en matière de défense et de sécurité, ou anime l'application de la politique de sécurité des systèmes d'information, il leur revient également de veiller à la protection du potentiel scientifique et technique et de participer, le cas échéant, à la mise en œuvre de la politique nationale d'intelligence économique.

Agence nationale de la sécurité des systèmes d'information (Premier ministre-ANSSI)

L'agence nationale de sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009, modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au secrétariat général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

http://www.ssi.gouv.fr

communication@ssi.gouv.fr

Chambres de commerce et d'industrie (CCI France)

CCI France est l'établissement national fédérateur et animateur des chambres de commerce et d'industrie (CCI) de France ; constitué d'un réseau de 158 chambres nationales, régionales, locales et des DOM-TOM, son activité est prolongée à l'international par 107 chambres françaises de commerce et d'industrie à l'étranger (CCIFE) réparties dans 77 pays. CCI France représente et défend également les intérêts des 2 000 000 entreprises ressortissantes auprès des pouvoirs publics français et européens, des instances internationales et des grands partenaires publics et privés. Via sa direction internationale, industrie, innovation et intelligence économique (D4I), elle oriente et coordonne l'action en intelligence économique des CCI.

http://www.cci.fr

industrie@ccifrance.fr

Club des directeurs de sécurité des entreprises (CDSE)

Créé il y a plus de 30 ans, et présidé par Alain Juillet, le CDSE dispose d'une solide expérience dans le domaine de la sécurité/sûreté d'entreprise. Il recense plus de 90 entreprises françaises dans 187 pays, qui représentent 700 milliards d'euros de chiffre d'affaires et 2 millions d'emplois.

https://www.cdse.fr et www.securite-strategie.fr

contact@cdse.fr

Confédération générale du patronat des petites et moyennes entreprises Île-de-France (CGPME)

La CGPME Paris Île-de-France est l'organisation représentative des TPE et PME franciliennes. A travers le dialogue direct avec les pouvoirs publics, elle propose des mesures et défend les PME pour développer l'économie et l'emploi. Elle propose à ses adhérents un ensemble de formations, diagnostics, projetspour sécuriser et faciliter la gestion de leur entreprise et accompagner leur croissance. Elle intervient notamment auprès des TPE et PME en difficulté ou en recherche de crédit.

http://www.cgpme-paris-idf.fr

t.sacleux@cgpme-idf.fr

Conseil national des barreaux (CNB)

Le CNB, établissement d'utilité publique doté de la personnalité morale, est l'institution nationale qui représente l'ensemble des avocats exerçant en France. La loi lui confère des missions très spécifiques : unification des règles et usages de la profession d'avocat, formation professionnelle des avocats et organisation de l'accès au barreau français pour les avocats étrangers. Il est l'interlocuteur des pouvoirs publics et des organisations internationales.

http://cnb.avocat.fr

observatoire@cnb.avocat.fr

Délégation interministérielle à l'intelligence économique (D2IE)

Structure légère, la D2IE a pour objectif d'être un centre d'alerte, d'impulsion et d'accompagnement, au service des intérêts économiques de la France et de sa compétitivité.

La délégation, aujourd'hui rattachée directement au Premier ministre, anime un réseau de correspondants dans les services centraux et déconcentrés.

http://www.intelligence-economique.gouv.fr

sec.d2ie@pm.gouv.fr

Ministère de l'agriculture, de l'agroalimentaire et de la forêt

Haut fonctionnaire de défense et de sécurité (HFDS)

intelligence-economique@agriculture.gouv.fr

Ministère de la défense

Direction de la protection et de la sécurité de la défense (DPSD)

La DPSD est, selon les termes du code de la défense, le service de renseignement « dont dispose le ministre de la défense pour assumer ses responsabilités en matière de sécurité du personnel, des informations, du matériel et des installations sensibles. »

La DPSD assure une mission de contre-ingérence au profit des entités du ministère de la défense et des entreprises en lien avec la défense afin de protéger leurs intérêts économiques et financiers et apporter une contribution renforcée en matière de cyber-défense. Sa devise est « renseigner pour protéger ».

http://www.defense.gouv.fr/dpsd

Ministère de l'écologie, du développement durable et de l'énergie

Haut fonctionnaire de défense et de sécurité (HFDS)

ppst.diepi.sdsie.sg@developpement-durable.gouv.fr

Ministères économiques et financiers

Direction générale des douanes et des droits indirects (DGDDI)

Administration de régulation des échanges, la DGDDI est chargée de faciliter et de sécuriser les flux de marchandises. En prise directe avec la chaine logistique des opérateurs, au cœur des flux de marchandises, elle oriente et accompagne les opérateurs vers les solutions douanières les plus adaptées à leurs opérations de commerce international. Le statut d'opérateur économique agréé est l'un des instruments-clés de cette démarche.

http://www.douane.gouv.fr

DGDDI - Bureau E3 - Politique du dédouanement - Cellule OEA :
dg-e3-oea@douane.finances.gouv.fr

Haut fonctionnaire de défense et de sécurité (HFDS)

http://www.economie.gouv.fr/hfds/posez-question-relative-au-guide-securite-economique

Ministère de l'enseignement supérieur et de la recherche

Haut fonctionnaire de défense et de sécurité (HFDS)

http://www.enseignementsup-recherche.gouv.fr/pid24818/haut-fonctionnaire-de-defense-et-de-securite-h.f.d.s.html

hfds@recherche.gouv.fr

Ministère de l'intérieur

Direction centrale du renseignement intérieur (DCRI)

La DCRI est le service référent concernant les menaces économiques étrangères. Elle réalise des actions de sensibilisation individuelles et collectives auprès des entreprises privées et publiques. De plus, elle est inscrite dans une véritable politique publique d'intelligence économique initiée depuis 2003, et peut ainsi faire face à de nouveaux enjeux dans un esprit de partenariat avec les entreprises.

http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-du-Renseignement-Interieur

securite-economique@interieur.gouv.fr

Direction générale de la Gendarmerie nationale (DGGN)

Sur les questions relatives à la sécurité économique, la brigade de gendarmerie du lieu de votre établissement peut vous diriger vers l'un des référents régional « intelligence économique ».

http://www.gendarmerie.interieur.gouv.fr/

Haut fonctionnaire de défense (HFD)

La mission intelligence économique (MIE) du ministère de l'intérieur est rattachée au secrétariat général, service du haut-fonctionnaire de défense. Tête de réseau fonctionnel du ministère, elle anime le dispositif territorial d'intelligence économique en s'appuyant sur le maillage des préfectures. Elle assure notamment l'échange de bonnes pratiques et elle fournit, en tant que de besoin, un soutien méthodologique.

shfd-ie@interieur.gouv.fr

Mouvement des entreprises de France (MEDEF)

Le MEDEF est le premier réseau d'entrepreneurs de France. S'appuyant sur 75 fédérations et 146 MEDEF territoriaux et régionaux, le mouvement défend et promeut 780 000 entreprises de toutes tailles et de tous secteurs d'activité. Dans les régions, les MEDEF territoriaux sont desespaces d'échange et de dialogue entre chefs d'entreprise et constituent le lien de proximité du MEDEF avec ses adhérents. Ils accompagnent les entreprises dans tous les domaines les concernant : droit du travail, fiscalité, formation, environnement, emploi des jeunes, export…

Quinze commissions et sept comités dans lesquels travaillent plus de 4 000 chefs d'entreprise et experts contribuent à bâtir une société française avant-gardiste et favorable à l'entreprise, avec un fil directeur de travail : la compétitivité équitable de la France et des entreprises françaises.

Porte-parole omniprésent des entreprises, le MEDEF est l'interlocuteur privilégié des décideurs et des pouvoirs publics régionaux, nationaux, européens et internationaux.

http://www.medef.fr

sgriselin@medef.fr

Ordre des avocats de Paris

L'ordre des avocats de Paris regroupe les 25 000 avocats parisiens.

http://www.avocatparis.org/

contactIE@avocatparis.org