Guide de l'intelligence économique

chefs d'entreprises, la pérennité et le développement de votre entreprise passent par la maîtrise et la protection de vos informations stratégiques

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA RÉGION BOURGOGNE

LA SECURITE ÉCONOMIQUE de votre entreprise, c'est VOTRE AVENIR !

Chefs d'entreprises,

Entrepreneurs,

Dans un monde où la concurrence est exacerbée, la compétitivité conditionne la survie de l'entreprise. La protection des savoir-faire et des informations devient alors un enjeu vital pour sa pérennité. Du chef d'entreprise à l'ouvrier, du cadre supérieur au contre-maître, chacun est concerné par ce qu'on appelle communément « l'intelligence économique ».

Il s'agit de porter un regard nouveau sur l'entreprise, ses informations stratégiques et son environnement pour anticiper les défis et adapter en conséquence sa conduite.

Plus qu'une politique publique, l'intelligence économique est une démarche pour vous aider à identifier les opportunités et les déterminants du succès, à anticiper les menaces, à prévenir les risques, à sécuriser les informations, à agir et influer sur le monde extérieur pour préserver la compétitivité de votre entreprise. C'est cette méthodologie que nous vous proposons de mettre en œuvre au travers de ce guide.

Vous y trouverez une aide au diagnostic des vulnérabilités de votre entreprise ainsi que les réflexes essentiels pour la protéger et défendre ses intérêts et, au-delà, assurer son développement futur.

Pour vous aider, les services de l'État restent à votre disposition.

Mais en attendant, n'oubliez pas que

LA SECURITÉ ÉCONOMIQUE de votre entreprise, c'est VOTRE AVENIR !

2 Ça peut vous arriver !

Stagiaire indélicat

ILLUSTRATION D'INGERENCE ECONOMIQUE DETECTEE PAR LA DGSI

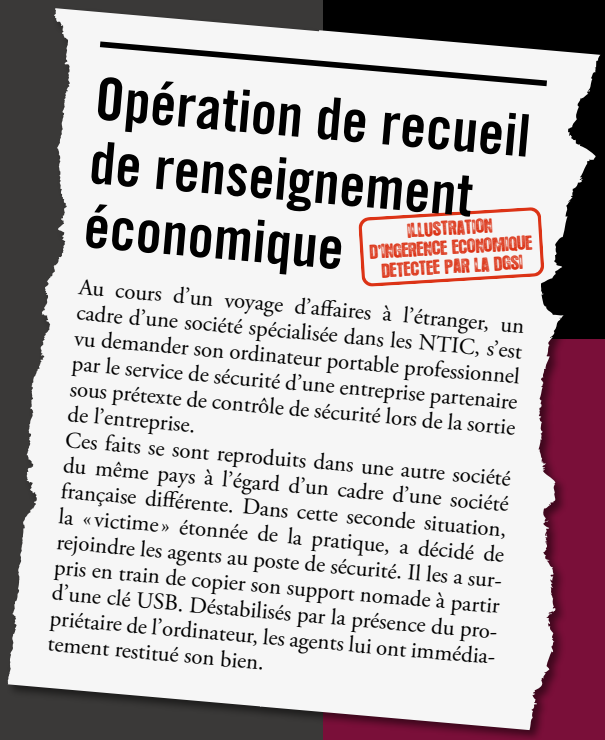
Un ressortissant étranger, qui réalise un doctorat au sein d'un laboratoire spécialisé dans les nanomatériaux, a transmis par le biais d'Internet des données relatives aux travaux de recherche menés par l'organisme d'accueil à destination de son université d'origine. Ce transfert d'informations a été entrepris de manière officieuse, en dehors de tout cadre de collaboration et sans que sa hiérarchie en soit avisée.

Informé de cette situation, le laboratoire français a décidé de ne pas déposer plainte mais a sommé l'intéressé de quitter l'établissement. Une veille documentaire est en cours afin de revendiquer la paternité de travaux qui seraient amenés à être déposés par l'université avec laquelle il interagissait.

Les actions d'ingérence économique sont très fréquemment commises par des personnes autorisées à pénétrer au sein des structures de recherche ou des entreprises. Il est en effet courant d'observer des stagiaires dévoués, revenir sur le lieu de travail en dehors des horaires habituels. Ces comportements sont des signaux d'alerte de nature à attirer l'attention des responsables de l'établissement. Ils doivent être signalés au service.

➜ Que faire en cas d'incident ?

Si le comportement du stagiaire contrevient aux règles de droit, notamment an cas de tentative d'intrusion informatique, ou de vol d'échantillons, un dépôt de plainte auprès des services compétents doit être envisagé.



Opération de recueil de renseignement économique

ILLUSTRATION D'INGERENCE ECONOMIQUE DETECTEE PAR LA DGSI

Au cours d'un voyage d'affaires à l'étranger, un cadre d'une société spécialisée dans les NTIC, s'est vu demander son ordinateur portable professionnel par le service de sécurité d'une entreprise partenaire sous prétexte de contrôle de sécurité lors de la sortie de l'entreprise.

Ces faits se sont reproduits dans une autre société du même pays à l'égard d'un cadre d'une société française différente. Dans cette seconde situation, la «victime» étonnée de la pratique, a décidé de rejoindre les agents au poste de sécurité. Il les a surpris en train de copier son support nomade à partir d'une clé USB. Déstabilisés par la présence du propriétaire de l'ordinateur, les agents lui ont immédiatement restitué son bien.

Un périphérique externe (disque dur ou clé USB), doté de son propre système d'exploitation, est connecté à l'ordinateur avant son allumage. Cette technique permet à l'attaquant d'avoir accès à l'ensemble du disque dur de l'ordinateur cible sans laisser de trace.

Elle est généralement mise en œuvre par les services de renseignements étrangers s'abritant derrière les contrôles de sécurité aéroportuaires ou lors de « visites » plus discrètes dans les chambres d'hôtel.

➜ Que faire ?

Dédier un ordinateur pour les déplacements contenant uniquement les informations en lien avec le motif du déplacement.

Conserver les informations sensibles sur une clé USB chiffrée et la garder sur soi lors du séjour.

Utiliser une solution de chiffrement du disque dur et appliquer des règles élémentaires de sécurité informatique (mot de passe à l'allumage de l'ordinateur - au boot -, désactivation de la possibilité de « booter » sur un disque externe, etc...).

2 Ça peut vous arriver !

TENTATIVE D'ESPIONNAGE INDUSTRIEL

Lors d'une visite chez un industriel du secteur de l'aéronautique, un membre d'une délégation d'un pays d'Extrême-Orient demande à imprimer un support de présentation à partir de sa clé USB. Le représentant de l'industriel visité demande à son service informatique de réaliser l'impression. Le responsable informatique teste la clé avant d'autoriser la connexion à un ordinateur de l'entreprise.

Lors de l'analyse de la clé USB, un programme malveillant permettant la récupération automatique de données a été détecté.

Le responsable informatique informe le délégué étranger que l'impression n'a pas pu être réalisée du fait de la présence de virus sur la clé. En parallèle, l'industriel prévient de l'incident les autres sociétés devant être visitées par cette délégation étrangère.

ILLUSTRATION D'INGERENCE ECONOMIQUE DETECTEE PAR LA DGSI

L'insertion de cette clé dans un ordinateur de la société aurait permis d'en pirater les données, y compris les mots de passe d'administrateurs et d'utilisateurs.

➜ Que faire ?

Contrôler strictement tout accès à un ordinateur d'une société par un personnel extérieur à celle-ci, a fortiori de nationalité étrangère.

Utiliser uniquement des supports (CD, clés USB...) préalablement vérifiés par le service informatique, surtout si ces supports ont été fournis à l'entreprise par des visiteurs.

ILLUSTRATION D'INGERENCE ECONOMIQUE DETECTEE PAR LA DGSI

SOUS-PROTECTION DES DONNÉES SENSIBLES

Une PME, spécialisée dans la création de logiciels d'aide à la décision pour la gestion des risques industriels, a dépêché un ingénieur en géophysique pour la représenter lors d'un séminaire international.

Il a présenté les activités de son entreprise, dont il a notamment évoqué l'expertise dans le domaine très sensible de la gestion des risques industrio-environnementaux.

Oubliant toute règle élémentaire de sécurité lors de la pause déjeuner, il a laissé dans la salle de conférence son ordinateur portable. Alors que la salle contenait de multiples supports informatiques nomades, seul celui du géophysicien a été dérobé.

L'appareil contenait des informations stratégiques pour l'entreprise : fichier clients, contrats commerciaux confidentiels, bilans carbone et rapports d'audits de plusieurs sociétés clientes, informations confidentielles concernant la gestion des risques industriels dans le domaine énergétique et des transports.

Un vol qui peut paraître « crapuleux » peut avoir un objet économique.

Plus de la moitié des cas d'ingérence économique par atteintes aux systèmes d'information est constituée de vols d'ordinateurs à contenus très sensibles.

➜ Que faire ?

Ne pas se séparer de son matériel.

3

Mettez en place une organisation

Protection de vos informations sensibles et stratégiques : **ORGANISEZ-VOUS**

Nommez un responsable sûreté :

- rattaché à un membre de la direction ou du comité exécutif afin de favoriser l'efficacité de son action.
- qui définit et garantit la bonne application des politiques de sécurité de l'entreprise.
- qui assure un rôle :
  - préventif - il doit donc être consulté en amont des grands projets,
  - de conseil - il concourt au développement de l'activité en aidant à la décision les dirigeants et en sécurisant les opérations,
  - d'information,
  - de formation,
- qui est l'interlocuteur privilégié des services de sécurité de l'Etat.

Les fuites intentionnelles ou non d'informations sensibles conduisent souvent à des pertes de marché où à des atteintes à l'image de l'entreprise.
IL EN VA DE LA PÉRENNITÉ DE L'ENTREPRISE.

Identifiez les éléments à protéger afin d'éviter les fuites intentionnelles ou non :

- données sensibles,
- données stratégiques,
- lieux sensibles.

Sensibilisez périodiquement le personnel :

- par le responsable sûreté,
- en faisant appel aux services de l'Etat (DGSI, DPSD, Gendarmerie, DIRECCTE)

Accès : **SÉCURISEZ-LES**

Le site, les locaux sensibles :

- sécurisez le site par des moyens passifs (murs, grillages...) et actifs (code d'accès, éclairage dissuasif...),
- installez un système de surveillance adapté (alarmes, télésurveillance, gardiennage, équipes de sécurité).
- signalez systématiquement aux services spécialisés (police, gendarmerie) toute intrusion, vol ou tentative d'effraction,

Les déplacements à l'intérieur du site :

- mettez en place un système de contrôle d'accès restrictif aux bureaux et locaux, détenant des informations et matériels sensibles,
- différenciez aux moyens de badges les employés des visiteurs extérieurs (stagiaires, intérimaires, prestataires, visiteurs...)

4

Sécurisez votre système informatique

RISQUE : vol, perte d'informations sensibles, contamination par virus informatique, indisponibilité du système d'information

Organisation informatique : **DÉTAILLEZ**

- Désignez un administrateur réseau, responsable de la sécurité informatique.
- Instaurez une charte informatique à laquelle souscrit tout le personnel. Sensibilisez annuellement les utilisateurs aux règles d'hygiène informatique (respect de la politique de sécurité, verrouillage systématique de la session lorsqu'elle est inutilisée...).
- Définissez une politique de mise à jour des logiciels.
- Rédigez des procédures d'arrivée et de départ des utilisateurs (personnel, stagiaire...).

Réseau interne : **PROTÉGEZ-LE D'INTERNET**

- Utilisez un anti-virus régulièrement actualisé et un pare-feu (firewall).
- Dans la mesure du possible, isolez du réseau commun les ordinateurs dédiés à l'accès internet.
- Evitez l'usage de technologies sans fil (Wifi). Si cette utilisation est indispensable, cloisonnez le réseau d'accès Wifi du reste du système d'information et utilisez un système de cryptage.
- Interdisez l'utilisation d'un même mot de passe pour les applications professionnelles et celles personnelles.

4

Sécurisez votre système informatique

Risques liés au TIC : **MAÎTRISEZ**

- Protégez les comptes utilisateurs par un mot de passe (10 caractères minimum de types différents) individuel, secret et régulièrement changé. Supprimez les éléments d'authentification par défaut.
- Imposez une méthode phonique ou des premières lettres pour les mots de passe. (ex : « J'ai acheté huit cd pour cent euros cet après midi » deviendra « ght8CD%E7am » ; la citation « un tiens vaut mieux que deux tu l'auras » donnera « 1tvmQ2tl'A »).
- Utilisez uniquement des supports (CD, clé USB...) préalablement vérifiés par le service informatique, surtout si ces supports ont été fournis par des visiteurs à l'entreprise.
- Méfiez-vous des courriers électroniques douteux ou d'expéditeur inconnu. Ne les ouvrez pas et placez-les dans la corbeille.
- Limitez le nombre de sauvegardes. Placez-les dans des pièces sécurisées à accès contrôlé.
- N'implantez aucun logiciel sans réaliser au préalable une analyse de ses caractéristiques.
- Interdisez la connexion d'équipements personnels (smartphone, tablette...) au système d'information de l'entreprise (ou BYOD : « Bring Your Own Device », « apportez votre propre appareil » en français). Si le travail à distance est nécessaire, fournissez des moyens professionnels nécessaires.
- Extrayez et conservez le disque dur de la photocopieuse en cas de révision à l'extérieur de l'entreprise ou de renouvellement de l'appareil.
- Disposez judicieusement les écrans afin d'assurer une confidentialité lors d'intrusion consentie (visite, stage, livraison, nettoyage...).

5

Maîtrisez le facteur humain

RISQUE : diffusion d'informations, débauchage, corruption, séduction…

Informations sensibles : **AGISSEZ**

- Incluez une clause de confidentialité dans les contrats d'embauche.
- Répertoriez les locaux contenant des éléments stratégiques, limitez-en l'accès aux personnes qui ont besoin d'en connaître.
- Portez une attention particulière aux prestataires de services extérieurs (nettoyage, maintenance, entreprises partenaires, fournisseurs...).
- Sensibilisez vos salariés à la protection de l'information stratégique.
- Instaurez des bonnes pratiques : rangement des documents sensibles sous clé (pause déjeuner, soir, nettoyage du bureau), utilisation de la déchiqueteuse...
- Sensibilisez vos salariés au bon usage des réseaux sociaux (Facebook, Twitter, Dailymotion, Youtube...)

5

Maîtrisez le facteur humain

Stagiaires et intérimaires : **ENCADREZ-LES**

Avant le stage ou la période d'intérim

- Étudiez le CV. Renseignez-vous auprès de l'organisme de formation ou du dernier employeur.
- Délimitez le contenu du stage ou de la mission d'intérim en identifiant les points critiques du travail prévu vis-à-vis de vos informations, documents, locaux ou matériels stratégiques.
- Désignez un responsable chargé d'encadrer le stagiaire ou l'intérimaire.
- Établissez un contrat ad hoc entre l'entreprise, le stagiaire/intérimaire et son organisme d'origine. Il précisera les restrictions informatiques, les mesures de sécurité, la clause de confidentialité, les limites de diffusion du rapport de stage et des documents en dehors de l'entreprise,
- Informez préalablement l'encadrement et le stagiaire/intérimaire lui-même du champ des informations autorisées, des locaux accessibles, des conditions d'utilisation de la photocopieuse, des outils informatiques, de son matériel personnel (smartphone, clé USB...)

Pendant le stage ou la période d'intérim

- Ne laissez pas les stagiaires et les intérimaires accéder seuls aux équipements et matériels sensibles ainsi qu'aux documents et informations à caractère stratégique, notamment par un accès non contrôlé aux systèmes informatiques.
- Soyez attentif aux liens pouvant se tisser entre le stagiaire ou l'intérimaire et les membres du personnel.

Après le stage ou la période d'intérim

- Récupérez les badges à l'issue de la mission. Changez les codes d'accès.
- Étudiez les travaux du stagiaire. Vérifiez la non divulgation de données jugées sensibles. Transmettez le rapport de stage au responsable sécurité.

Visiteurs : **ACCOMPAGNEZ-LES**

Avant la visite

- Renseignez-vous sur l'identité et la fonction des visiteurs.
- Assurez-vous de l'adéquation entre le motif de visite et les fonctions annoncées.

Pendant la visite

- Tenez un registre des visites. Remettez un badge spécifique.
- Faites déposer les téléphones portables et tous les autres appareils de prises de vue à l'accueil.
- Accompagnez les visiteurs en permanence dans l'entreprise, même jusque dans les endroits les plus incongrus !
- Établissez un programme de visite avec le contenu des exposés, l'identification des informations à ne pas divulguer. Définissez le circuit de la visite en évitant les points sensibles de l'entreprise.
- Interdisez le contact avec des salariés non préalablement pressentis pour être leurs interlocuteurs.
- Évitez que les mêmes questions soient posées successivement à différents employés.
- Réfutez toute question dépassant le cadre initialement prévu de la visite.
- Proscrivez toute prise de vue, enregistrement sonore et prélèvement d'échantillon sauf autorisation.

Collaboration avec des partenaires : **SOYEZ VIGILANT**

De nombreux développements de nouveaux procédés, de nouveaux produits sont issus de travaux collaboratifs entre plusieurs entreprises complémentaires (co-conception) ou entre entreprises et établissements de recherche ou centres techniques.

Les développements les plus innovants nécessitent en effet souvent l'intervention de compétences issues de fournisseurs, d'entreprises complémentaires, de clients, de laboratoires publics et privés français ou étrangers, de centres techniques, de pôles de compétitivité.

Si ce type d'organisation est nécessaire à l'émergence de nouvelles solutions, il est particulièrement difficile d'assurer une bonne protection des intérêts de l'entreprise qui y est associée.

Avant le projet :

- Analysez précisément les objectifs, les enjeux et les risques liés au projet collaboratif pour l'entreprise.
- Identifiez clairement le positionnement de chacun des partenaires dans le projet :
  - Qui fait quoi ?
  - Qui accède à quel type d'informations, qui est responsable de quoi ?
  - Quels sont l'objectif et le retour attendu de chacun des partenaires ?
  - Y a-t-il des concurrents potentiels ?
  - Y a-t-il des partenaires qui ont déjà des liens privilégiés avec certains concurrents ?
- Identifiez nominativement les personnes qui seront impliquées au sein des différentes structures dans le projet. Informez-vous sur leurs parcours, leurs travaux et leurs liens passés ou présents avec d'éventuels concurrents.
- Construisez un accord de partenariat ou de consortium précisant clairement le rôle et les limites d'intervention de chacune des structures intervenant dans le projet et la manière dont sera répartie la propriété intellectuelle des résultats (brevets, licences, publications scientifiques...).
- Exigez des accords de confidentialité (de la part des personnes impliquées) et d'exclusivité (de la part des structures) sur les technologies développées. Le recours à un juriste spécialisé est vivement recommandé.

Pendant le projet :

- Utilisez une plate-forme collaborative sécurisée prévoyant, pour chaque personne préalablement identifiée, un accès limité aux seules informations auxquelles elle peut avoir accès.
- Réalisez périodiquement des rencontres chez les partenaires associés. Examinez les outils et moyens visant à assurer la sécurité des connaissances ou informations qu'ils détiennent.
- Réalisez une veille approfondie des informations publiées par les partenaires sur le projet en question et/ou sur les projets qui s'en approchent (campagnes de communication, articles de presse, publications scientifiques...).
- Organisez, réévaluez, sécurisez la répartition des droits de propriété intellectuelle et industrielle de chacune des innovations.
- Dotez-vous d'outils de traçabilité des travaux réalisés (type cahier de laboratoire tenu individuellement par chaque partenaire). Chacun pourra ainsi apporter la preuve de sa qualité d'auteur ou d'inventeur sur les éléments nouveaux qu'il a apportés au projet.

6

Protégez l'information à l'extérieur de l'entreprise

RISQUE : diffusion d'informations par négligence

Lieux publics : **ÉTABLISSEZ DES CONSIGNES**

- Évitez d'aborder des sujets professionnels de vive voix ou au téléphone (train, avion, restaurant...)
- Surveillez vos outils de travail (mallette, documents, ordinateur, téléphone).
- Évitez d'utiliser les moyens de communication mis à disposition dans les hôtels.
- Ne laissez pas des supports contenant des données sensibles dans la chambre d'hôtel (même dans le coffre-fort de l'hôtel) encore plus à l'étranger.
- Si vous devez travailler dans les lieux publics, désactivez le Wifi et posez un filtre sur votre écran d'ordinateur.

Séjours à l'étranger : **RESPECTEZ CERTAINES RÈGLES COMPORTEMENTALES**

Vie quotidienne

- Respectez strictement la législation locale.
- Soyez discret dans les transports et lieux publics.
- Évitez les déplacements seul dans les lieux sensibles.
- Soyez réservé sur les sujets politiques locaux.
- Refusez les cadeaux de valeur.
- Soyez prudent en matière de relations extraprofessionnelles.
- Évitez les habitudes trop facilement identifiables.

Vie professionnelle

- Sélectionnez les informations transportées.
- Signalez votre présence aux autorités officielles françaises.
- Évitez de lire ou travailler dans les transports.
- Ne laissez jamais un ordinateur, un téléphone portable ou de la documentation confidentielle dans une chambre.
- Proscrivez les échanges téléphoniques sensibles.
- Soyez prudent en matière de photocopie sur place.
- Restez discret sur vos déplacements.
- Au retour, rédigez un rapport d'étonnement.

6 Protégez l'information à l'extérieur de l'entreprise

SALON PROFESSIONNEL

Avant le salon : anticipez

- Définissez les objectifs de votre participation (prospecter, trouver des partenaires, lancer un produit...)
- Ciblez les stands. Préparez un plan de visite.
- Répertoriez les renseignements que vous souhaitez collecter avec le degré de précision et la façon de les obtenir (plaquette, échantillon...)
- Définissez les informations qui pourront ou non être diffusées sur le salon.
- Préparez des axes de réponse sur les sujets délicats (savoir-faire, innovation...)

Pendant le salon : collectez

- Informez-vous. Collectez des informations (attente des clients, mécontentement sur un produit...).
- Présentez vos produits techniques par des professionnels et non par des hôtesses.
- Privilégiez l'écoute et le dialogue avant de vous lancer dans vos démonstrations. Restez vigilant dans vos conversations.
- Soyez vigilant. Surveillez les matériels à risque. Limitez au strict minimum le nombre de documents ou matériels sensibles.

Après le salon : exploitez

- Lors de la clôture, videz le stand et vérifiez l'ensemble des matériels et documents.
- Étudiez les réactions dans la presse et sur internet.
- Analysez la documentation collectée.
- Organisez une réunion de débriefing.
- Rédigez un document de synthèse avec les contacts nouveaux, les faits surprenants et les actions à accomplir.

7

Protégez votre patrimoine, vos savoir-faire

RISQUE : copie, contrefaçon

Propriété industrielle : **ORGANISEZ-LA**

- Protégez vos créations techniques ou esthétiques par le dépôt de titres de propriété industrielle (brevets, marques, dessins, modèles...). Ils vous permettront d'exercer un monopole d'exploitation sur ces créations.
- Dans le cas de partenariat, établissez des contrats de confidentialité. Instaurez des moyens de preuve de la date à laquelle les dispositifs innovants ont été mis en place.
- Conservez le secret absolu avant le dépôt de la demande de brevet. Toute divulgation est susceptible de détruire la condition de nouveauté et ainsi être un obstacle au dépôt de brevet ou un motif d'annulation.
- Assurez une sensibilisation maximale au sein de l'entreprise sur l'intérêt de l'utilisation des outils de la propriété industrielle et sur l'importance de la confidentialité.
- Considérez l'activité d'invention dans les contrats de travail des salariés qui participent à la mise au point de vos innovations. Sinon le salarié pourrait revendiquer la propriété de l'invention.

Brevet, marque, logo : **SURVEILLEZ LES VÔTRES ET CEUX DE VOS CONCURRENTS**

- Observez ses brevets et ses marques par une veille technologique et concurrentielle pour vous assurer que personne n'utilise son invention sans autorisation.
- Utilisez en particulier les sources d'information brevet en accès libre sur Internet (fr.espacenet.com) afin, par exemple, d'étudier les dépôts de vos concurrents : déposent-ils des demandes de brevet sur des techniques que vous avez vous-même protégées ?
- Cherchez à repérer le plus en amont les signaux de la contrefaçon (baisse d'activité par la perte de marchés, dégradation inexpliquée de la notoriété...).

7

Protégez votre patrimoine, vos savoir-faire

Vous avez identifié un contrefacteur ?

Commencez par négocier à l'amiable. La présentation de votre titre peut mettre un terme à toute velléité de contrefaçon ou déboucher sur un accord entre les parties (par un contrat de licence par exemple). Si le contrefacteur persiste, demandez l'intervention des services spécialisés (douane, conseils en propriété industrielle, avocats spécialisés...) qui vous aideront à faire respecter vos droits.

➔ Pour toute question, contactez l'Institut National de la Propriété Industrielle (INPI).

L'INPI délivre les brevets, marques, dessins et modèles et donne accès à toute l'information sur la propriété industrielle et les entreprises. Il participe activement à l'élaboration et à la mise en œuvre des politiques publiques dans le domaine de la propriété industrielle et de la lutte anti-contrefaçon.

La délégation régionale INPI Bourgogne :

- aide les PME-PMI en leur proposant des outils d'évaluation personnalisés, comme le « pré-diagnostic propriété industrielle »,
- soutient les actions permettant la sensibilisation, la formation et l'accompagnement des entreprises dans leur démarche d'innovation et de mise en pratique de la propriété industrielle,
- mène des opérations de sensibilisation et de formation dans les écoles, les universités, les laboratoires et les centres de recherche,
- accompagne les démarches de propriété industrielle des pôles de compétitivité.

➔ Contact délégation régionale de Dijon : 03 80 71 29 32- bourgogne@inpi.fr

Savoir-faire spécifique lié à un collaborateur : **ANTICIPEZ**

➔ Organisez le départ de tout agent affecté à un poste stratégique de l'entreprise (départ en retraite, débauchage, maladie...) par la préservation de son savoir-faire (formation d'un autre agent) et par des mesures de précaution en vue d'en empêcher la divulgation (signature préalable d'une clause de non concurrence).

8 Surveillez votre environnement

RISQUE : dénigrement, diffamation,
atteinte à la marque, perte de marchés

E-RÉPUTATION :
savez-vous ce qu'Internet dit de vous ?

- Surveillez votre image sur Internet. Étudiez les informations, concernant votre société, vos produits, trouvées par vos clients (site, forum, blog, réseaux sociaux...)
- Répondez aux avis (positifs et négatifs). Montrez votre intérêt pour les questions et remarques des clients. Maîtrisez l'information diffusée sur vos produits.
- Protégez votre réputation en ligne. Instaurez une communication de crise en cas d'atteinte à l'image de votre entreprise.

VEILLE STRATÉGIQUE :
connaissez-vous vos concurrents
aussi bien qu'ils vous connaissent ?

- Définissez les enjeux stratégiques de votre société. Surveillez uniquement ceux qui sont véritablement importants pour l'entreprise.
  - Est-il plus judicieux de connaître vos clients, vos concurrents ou vos fournisseurs ?
  - Est-il plus pertinent de détecter de nouvelles technologies ou les tendances du marché ?
- Analysez vos forces et vos faiblesses.
- Détectez les opportunités de développement ou les menaces pour votre entreprise.
- Développez une culture de la collecte d'information chez vos salariés (retours d'expérience, rapports d'étonnement, capacité à s'interroger...).
- N'hésitez pas à contacter le réseau consulaire (CCI, ARIST, Réseau Entreprise Europe, Guichet Unique Export...), les structures professionnelles (UIMM, Allizé Plasturgie Bourgogne, ARIA, Agence NTIC...), les centres techniques (CETIM, FCBA...).
  - Ils organisent des veilles technologiques, matériaux, marchés, réglementaires...
  - Ils vous accompagneront pour développer votre innovation et votre compétitivité.

9 Vos partenaires en Bourgogne

La Direction Régionale des Entreprises de la Concurrence, de la Consommation et de l'Emploi (Direccte) est placée auprès du Préfet de la région Bourgogne.

Elle assure le pilotage coordonné des politiques de l'Etat en matière de développement économique, d'emploi, de travail et de protection des consommateurs.

La DIRECCTE est le relais en région de la politique publique d'intelligence économique définie au niveau interministériel qui a pour finalité de contribuer à la croissance de l'économie ainsi qu'à la préservation et à la création d'emplois.

Elle met également en œuvre des politiques locales complémentaires spécifiques au tissu économique régional.

Ses missions :

- le montage et le pilotage d'actions individuelles et collectives d'intelligence économique qui visent à sensibiliser, conseiller et informer les entreprises,
- le soutien technique et financier aux pôles de compétitivité, aux filières, aux réseaux consulaires, aux structures et syndicats professionnels et autres collectifs d'entreprises, en particulier dans l'élaboration de leurs stratégies de développement (analyse de positionnement, des marchés, de la concurrence...).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA RÉGION BOURGOGNE
DIRECCTE

03 80 76 29 44
bourg.intel-eco@direccte.gouv.fr

Spécialisée dans la contre ingérence économique, la **Direction Générale de la Sécurité Intérieure (DGSI)** est le service opérationnel et d'analyse de référence en matière de sécurité économique (circulaire du Ministre de l'Intérieur du 13.08.2008).

Elle a notamment pour mission de prévenir, détecter, analyser et neutraliser les comportements ou situations destinés ou susceptibles de nuire à une entreprise française ou à un établissement de recherche, au profit d'intérêts étrangers.

Elle apporte, aux entreprises et laboratoires, conseils et audits en termes de sécurité comportementale, bâtimentaire et des systèmes d'information.

La DGSI est associée aux groupes de travail mis en place dans le cadre du schéma régional de l'intelligence économique et participe aux réunions du Comité Régional d'Intelligence Economique Territoriale (CRIET).

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE
DGSI

03 80 44 57 10
contact-eco21@interieur.gouv.fr

9

Vos partenaires en Bourgogne

Votre entreprise est-elle bien protegée ?

Nous vous proposons un diagnostic complet et gratuit des vulnérabilités économiques susceptibles de nuire à votre entreprise

La Gendarmerie Nationale peut vous aider à défendre votre savoir-faire :

- Elle propose aux chefs d'entreprises sa capacité en matière de sécurité économique sur l'ensemble du territoire national.
- Elle peut vous aider à vous protéger contre les atteintes à votre patrimoine.

La gendarmerie, acteur de la sécurité économique, peut vous apporter ses compétences en matière de :

- conseils et formation : sensibilisation à la sécurité, délinquance informatique...
- information : nouvelles technologies, coopération policière internationale...
- police judiciaire : vols de données, contrefaçon...

03 80 70 65 64

intel-eco.rgbourg@gendarmerie.interieur.gouv.fr

La Direction de la Protection et de la Sécurité de la Défense (DPSD) est le service de renseignement du ministère de la défense dont la mission est de « RENSEIGNER POUR PROTEGER ».

La Défense doit protéger ses personnels, ses matériels, ses informations et installations sensibles, d'actes hostiles, qualifiés d'ingérence (le terrorisme, l'espionnage, les actions de subversion comme celles de sabotage ou encore le crime organisé) qui peuvent émaner d'organisations ou d'individus qui chercheraient ainsi à porter atteinte aux capacités opérationnelles de la défense.

La DPSD doit s'assurer de la protection du secret confié aux entreprises.

Elle contribue aussi à la préservation du patrimoine scientifique et technique de défense.

La DPSD travaille ainsi avec environ 2 000 sociétés liées avec le ministère de la défense.

Par son action dans le domaine de la sécurité économique (sécurité industrielle et contre ingérence) la DPSD est un acteur reconnu de la politique publique d'intelligence économique.

03 80 11 23 27

bur.etude@wanadoo.fr

LA SECURITE ÉCONOMIQUE de votre entreprise, c'est VOTRE AVENIR !

PRÉFET DE LA RÉGION BOURGOGNE

dpso

DGSE

Gendarmerie nationale

PRÉFET DE LA RÉGION BOURGOGNE

DÉLÉGATION RÉGIONALE À LA RECHERCHE ET À LA TECHNOLOGIE