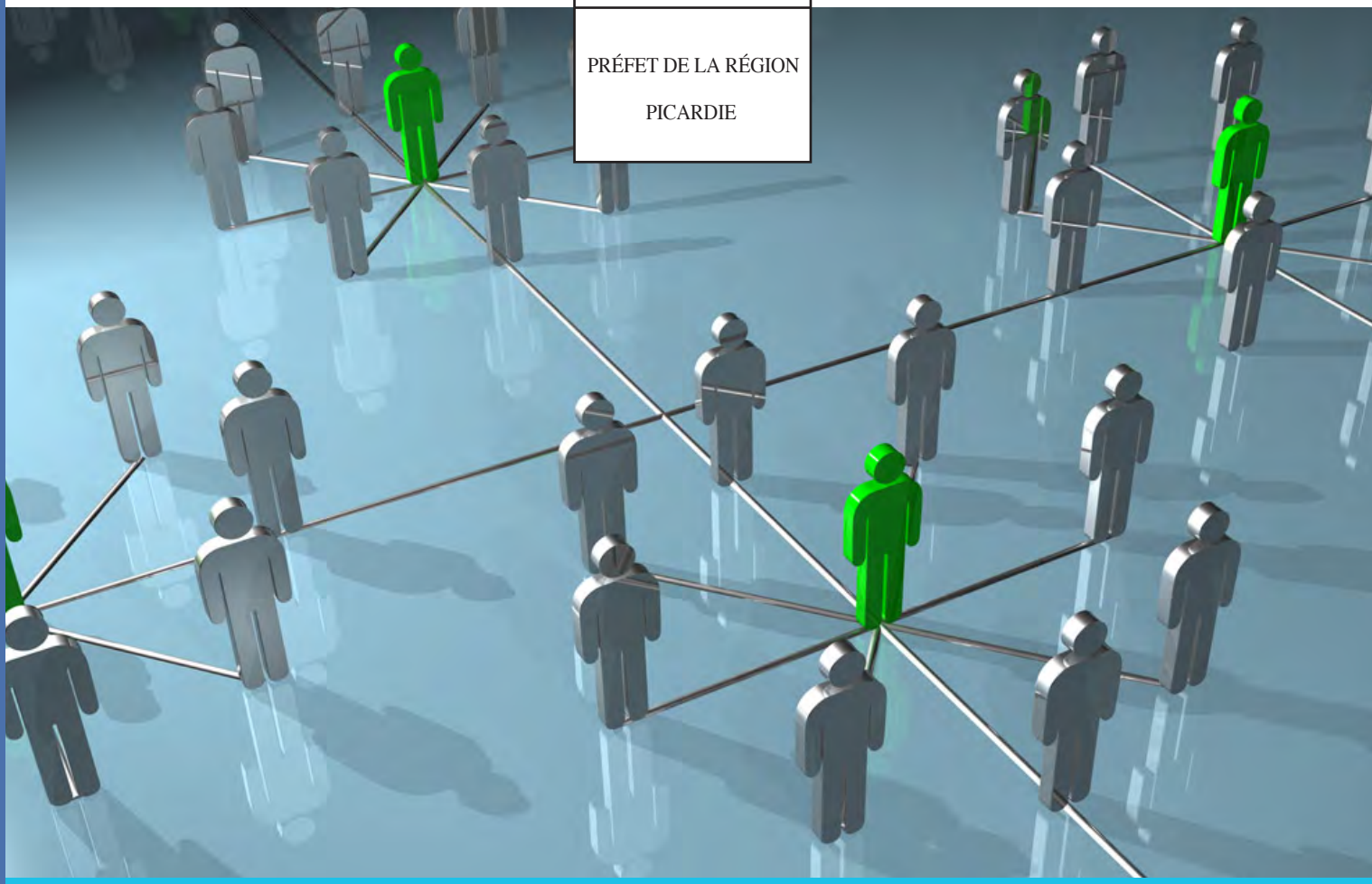
Sécurité économique

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA RÉGION
PICARDIE



INTELLIGENCE ÉCONOMIQUE

ENTREPRISES : Guide de bonnes pratiques pour assurer la protection de vos informations stratégiques

9 fiches pratiques

Fiche 1 : Assurer la sécurité physique de l'entreprise
Fiche 2 : Assurer la sécurité informatique de l'entreprise
Fiche 3 : Protéger les appareils nomades
Fiche 4 : Les stagiaires, les intérimaires
Fiche 5 : Les risques liés aux facteurs humains internes
Fiche 6 : Les visites d'entreprises, les délégations étrangères
Fiche 7 : Les salons professionnels
Fiche 8 : Les déplacements professionnels à l'étranger
Fiche 9 : La sécurité de l'entreprise à l'épreuve des réseaux sociaux

Le mot du préfet de région

Dans une économie mondialisée marquée par une radicalisation de la concurrence internationale, la bonne santé des entreprises repose sur leur compétitivité. Dans ce contexte hostile, la protection des savoir-faire et des informations devient un enjeu crucial pour assurer la pérennité de son activité. Engager une démarche de sécurité économique devient indispensable, car aujourd'hui n'importe quelle entreprise, quelle que soit sa taille, quel que soit son secteur d'activité, peut être la cible d'une atteinte destinée à s'approprier ses avantages concurrentiels, à la déstabiliser et à l'affaiblir.

Devant être une préoccupation quotidienne du chef d'entreprise, la protection des informations stratégiques doit impliquer l'ensemble du personnel, quel que soit son niveau de responsabilité. La sécurité économique est l'affaire de tous puisqu'il s'agit de protéger son entreprise, son activité, et donc, par voie de conséquence, les emplois qu'elle génère.

Jean-François CORDET,
Préfet de la région Picardie

L'intelligence économique en 4 axes

L'intelligence économique (IE) vise à collecter, analyser, diffuser et protéger l'information économique stratégique. Outil d'aide à la décision, au profit de l'ensemble des acteurs économiques (entreprises, établissements de recherche, ministères, régions), elle se décline en 4 axes :

1- **un volet pédagogique**, permettant de sensibiliser les acteurs concernés sur les objectifs et les méthodes de l'intelligence économique ;

2- **un volet anticipation** et accompagnement des évolutions, notamment par la veille stratégique, afin de permettre à ces acteurs de prendre les meilleures décisions ;

3- **un volet sécurité économique**, à travers la prévention des risques, notamment immatériels (savoir-faire, réputation, etc.) ;

4- **un volet travail d'influence** de long terme sur l'environnement économique, comme par exemple les régulations internationales de toutes natures, techniques ou de gouvernance, afin de créer un environnement favorable aux orientations choisies.

Le dispositif territorial d'intelligence économique

L'Etat engage une démarche partenariale afin d'accompagner les acteurs économiques dans leur mise en œuvre de l'intelligence économique. Elle se traduit par le dispositif territorial d'intelligence économique.

Sous l'autorité du Préfet de région, un comité régional fédère et coordonne les actions mises en oeuvre par les partenaires pour promouvoir et développer l'intelligence économique auprès des acteurs économiques : entreprises, universités, institutionnels.

Conjointement, un groupe dédié à la sécurité économique, composé des services de sécurité de l'Etat, est constitué pour favoriser la sécurité économique et mener des actions de protection des entreprises sensibles.

FICHE N°1

Assurer la sécurité physique de l'entreprise : protection du site et des locaux

La sécurité physique du site et des locaux constitue le premier niveau de protection de l'entreprise.

Les moyens et mesures mises en place viseront à empêcher toute intrusion, à contrôler les déplacements dans l'enceinte de l'entreprise, et à éviter ainsi tout recueil indu d'informations.

Quelques recommandations :

- Sécuriser le site par des moyens passifs (murs, grillages...) et actifs (code d'accès, éclairage dissuasif...).
- Installer un système de surveillance adapté (alarmes, télésurveillance, gardiennage, équipes de sécurité).
- Mettre en place un système de contrôle d'accès restrictif aux bureaux et locaux détenant des informations et matériels sensibles.
- Mettre en œuvre le port du badge permettant de différencier les employés des visiteurs extérieurs (stagiaires, intérimaires, prestataires, visiteurs...).
- Prévoir la procédure de prise en charge des visiteurs (registre des visites, port d'un badge spécifique, circuit de notoriété...).
- Signaler systématiquement aux services spécialisés (police, gendarmerie) toute intrusion, vol ou tentative d'effraction.

FICHE N°2

Assurer la sécurité informatique de l'entreprise

L'organisation de la sécurité informatique

- Désigner un administrateur réseau chargé de la sécurité informatique.
- Élaborer une charte informatique que l'ensemble des salariés devront signer (bonnes pratiques en matière d'utilisation des outils informatiques).
- Mettre en place une politique de gestion des mots de passe (distinction comptes utilisateur/administrateur, codes alphanumériques de 10 caractères minimum, individuels, secrets, régulièrement changés, suppression des comptes obsolètes...).
- Sensibiliser régulièrement les utilisateurs aux règles d'hygiène informatique.

Le serveur réseau de l'entreprise :

- Veiller à disposer d'une cartographie précise et actualisée du réseau informatique.
- Protéger son système d'information à l'aide d'outils régulièrement mis à jour (antivirus, pare-feu, anti-spam, anti-rootkit...).
- Veiller à réaliser des sauvegardes régulières des données sur un serveur placé dans une pièce sécurisée dont l'accès est contrôlé ainsi que sur des supports externes stockés dans des lieux sécurisés autres que la pièce du serveur.
- Dans la mesure du possible, isoler les postes dédiés à l'internet du réseau intranet.
- Mesurer les risques quant à l'utilisation des technologies sans fil (Wifi) par rapport à l'environnement de l'entreprise.
- Utiliser des solutions de chiffrement pour la transmission d'informations confidentielles.
- Vigilance quant aux opérations de télémaintenance informatique.

Le poste de travail individuel :

- Configuration des postes (installation et modification des logiciels et périphériques) contrôlé par l'administrateur SSI.
- Désactivation totale ou partielle des périphériques sur les postes de travail (lecteurs disquette, CD, port USB).
- Protéger les comptes utilisateurs par un mot de passe robuste et prohiber l'utilisation d'un même mot de passe pour les applications professionnelles et pour les applications personnelles.

Des règles comportementales à respecter

- Ne pas laisser visibles ses mots de passe (post-it sur l'écran, sous le clavier ...).
- Verrouiller sa session dès que l'on s'éloigne de son ordinateur.
- Ne pas connecter d'équipements personnels sur son poste de travail (tablette, smartphone ...).
- N'utiliser que des supports externes autorisés par le responsable de la sécurité informatique, et vérifier, avant toute utilisation sur le réseau de l'entreprise, leur intégrité sur une station de décontamination.
- Ne pas ouvrir les courriers électroniques douteux ou d'expéditeurs inconnus.
- Rendre compte sans délai de tout incident et faire appel au responsable de la sécurité des systèmes d'information.

Quelques précautions quant à l'utilisation des ordinateurs portables et autres équipements TIC :

- A l'intérieur de l'entreprise, ranger systématiquement en lieu sûr l'ordinateur portable.
- De retour d'un déplacement professionnel, avant de connecter l'ordinateur portable au réseau de l'entreprise, le confier à une personne qualifiée qui s'assurera de son intégrité.
- A l'extérieur de l'entreprise, surveiller de manière constante son ordinateur portable. Ne jamais le laisser dans le coffre de sa voiture, dans une chambre d'hôtel, ou dans la salle de travail durant les pauses.
- Conserver sur soi, à l'aide d'un support amovible (clé USB...), les informations les plus sensibles.
- Les photocopieurs numériques disposent d'un disque dur gardant en mémoire les documents traités. Si le photocopieur est en location, veiller à l'effacement sécurisé des données ou prévoir une clause de propriété dans le contrat de location.
- Surveiller les opérations de maintenance sur le photocopieur.

FICHE N°3

Protéger les appareils nomades

Le nomadisme permet aux collaborateurs de travailler en dehors de l'entreprise et d'accéder à des ressources professionnelles.

Ce phénomène en pleine expansion constitue un enjeu en terme de sécurité des systèmes d'information compte tenu de la plus grande vulnérabilité de ces « bureaux mobiles ».

Les principaux risques liés au nomadisme sont le vol ou la perte de l'équipement (téléphone portable, clés USB, PC portable, assistant personnel) et des données contenues, ou l'infection par un virus informatique lors d'une connexion à un réseau peu sûr (réseau internet domestique ou dans les lieux publics).

Quelques recommandations pour accroître la sécurité des terminaux nomades :

- Imposer un mot de passe au démarrage de la machine (mot de passe de « boot »).
- S'assurer de la mise à jour régulière des antivirus.
- Dissocier le compte administrateur du compte utilisateur dont les droits seront restreints afin de limiter les risques d'installation de logiciels non autorisés.
- Restreindre l'usage des périphériques (lecteurs de disques, ports USB...). Désactiver la fonction autorun afin d'éviter l'exécution automatique d'un programme sans vérification préalable.
- Passer systématiquement à l'antivirus tout support numérique extérieur et refuser la connexion d'un équipement dont on ne connaît pas la provenance.
- Instaurer un verrouillage automatique de la session après un certain délai d'inactivité, et prévoir un mot de passe alphanumérique complexe (chiffres + lettres + caractères spéciaux) pour le déverrouillage.
- Désactiver les fonctions de communication wifi et Bluetooth de vos appareils nomades.
- Mettre en œuvre une solution de chiffrement des données.
- Utiliser un filtre de confidentialité dans les lieux publics.
- Éviter les connexions sur des réseaux extérieurs et bornes wifi publiques.
- Ne pas consulter les sites internet réputés dangereux (jeux en lignes, sexe, streaming...).
- Mettre en œuvre une solution de communication sécurisée entre l'utilisateur nomade et le réseau de l'entreprise (VPN – réseau privé virtuel).
- Désactiver la fonction géolocalisation des applications embarquées sur le smartphone.

FICHE N°4

Les stagiaires, les intérimaires

Disposant d'un droit d'accès dans l'entreprise (intrusion consentie), le stagiaire et l'intérimaire peuvent avoir accès à des données essentielles pour l'entreprise. Afin de limiter le risque de fuite d'information, ce type de mission doit être encadré et contrôlé.

Avant le stage ou la période d'intérim :

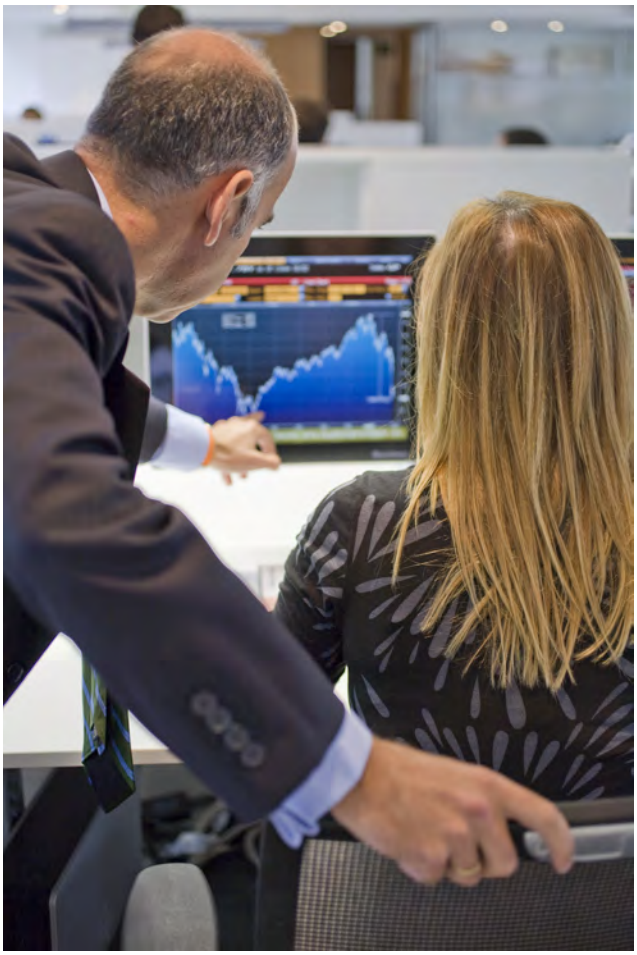
- Étudier le CV. Renseignez-vous auprès de l'établissement de formation ou du dernier employeur.
- Délimiter le contenu du stage ou de la mission d'intérim en identifiant les points critiques du travail prévu vis à vis de vos informations, documents, locaux ou matériels stratégiques.
- Désigner le responsable qui sera chargé d'exercer l'encadrement du stagiaire ou de l'intérimaire.
- Établir un contrat spécifique entre l'entreprise d'accueil, le stagiaire ou l'intérimaire et son organisme de formation. Ce document 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.
- Informer 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 pas laisser les stagiaires et 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.
- Être 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 :

- Récupérer les badges à l'issue de la mission.
- Changer les codes d'accès et fermer les sessions qui ont pu être activées sur le réseau lors du départ du stagiaire ou de l'intérimaire.
- Étudier les travaux du stagiaire. Vérifier la non divulgation de données jugées sensibles. Transmettre le rapport de stage au responsable sécurité.



FICHE N°5

Les risques liés aux facteurs humains internes

Les facteurs humains au sein de l'entreprise sont déterminants.

Les collaborateurs ne peuvent se tenir à l'écart de réseaux de relations qui peuvent donner accès à de nombreuses informations utiles si elles sont correctement exploitées.

L'image de l'entreprise est liée pour partie au savoir-faire et au comportement de ses salariés, sans parler des indiscrétions, le plus souvent involontaires, qui peuvent devenir des handicaps lourds.

Afin de limiter le risque de fuite d'information, il est utile de mettre en œuvre des mesures adaptées.

Quelques mesures à prendre en interne de l'entreprise :

- Désigner un responsable sécurité.
- Formaliser les consignes de sécurité.
- Informer régulièrement le personnel sur ces consignes.
- Contrôler l'application de ces mesures.
- Sensibiliser les cadres occupant un poste stratégique.
- Inclure des clauses de confidentialité dans les contrats de travail.

FICHE N°6

Les visites d'entreprise, les délégations étrangères

Si les visites d'entreprises sont d'abord source d'opportunités, la présence de personnes extérieures au sein de l'entreprise constitue un risque, notamment en terme de recueil indu d'informations sensibles. Afin d'en limiter la portée il est nécessaire d'identifier les menaces pour mettre en œuvre des mesures adaptées.

Identifier les menaces :

- Le renseignement économique, financier, commercial : connaissance de la politique marketing, recherche du catalogue des prix, du fichier clients, identification des fournisseurs, sous-traitants...
- Le vol : informations stratégiques, procédés, matériels...
- Le sabotage : dégradation de l'outil de production.
- Les risques liés au système d'information (site Internet, messagerie, réseau...) : piratage, vols de données, interruption de service, corruption des données...

Gérer les menaces :

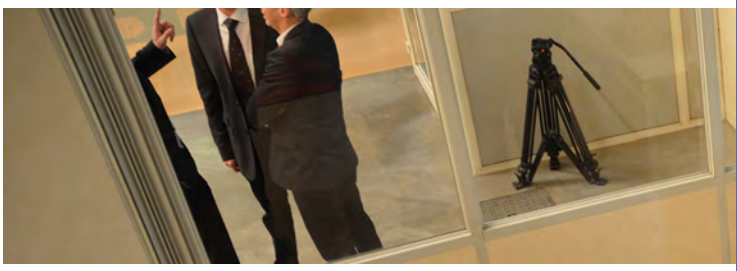
- Informer le personnel et lui rappeler les enjeux économiques pour l'entreprise.
- Définir les informations communicables et les savoirs à protéger en identifiant leur localisation dans l'entreprise.
- Élaborer une stratégie de communication de l'intervenant ou du guide.
- Établir un parcours de notoriété : circuit de visite accompagnée dans l'entreprise qui évite les zones sensibles.
- Interdire les appareils photo, caméscopes, usage des téléphones portables. A cet effet, une consigne sera ouverte à l'accueil.
- Prendre des mesures contre le vol.
- Sensibilisation de l'ensemble des collaborateurs : discrétion, réserve, vigilance, protection adaptée des données sensibles.

Préparer la visite :

- Se renseigner sur l'identité et la fonction des visiteurs et s'assurer de l'adéquation entre le motif de la visite et les fonctions annoncées.
- L'entreprise doit identifier ce qu'il ne faut pas montrer : mode d'implantation des machines, techniques de fabrication, données stratégiques, chiffres cruciaux...
- L'entreprise doit construire le discours à tenir et désigner la personne qui sera chargée de l'exposé oral. Seul le guide, préalablement préparé, répondra aux questions au cours de la visite.
- Méfiance à l'égard des questions trop indiscrètes.
- Sur des sujets dont on mesure difficilement l'intérêt stratégique, il convient de ne pas trop donner d'éléments.
- Suivant la même logique, il conviendra d'évaluer la pertinence d'évoquer les futurs produits ou projets.

Le déroulement de la visite :

- Tenir un registre des visites. Remettre un badge spécifique.
- Principe de l'inscription préalable : Dans les délégations, la liste des visiteurs doit être connue à l'avance. Il ne faut jamais accepter de changement de dernière minute. Si les noms de visiteurs ne correspondent pas, il faut refuser l'accès.
- Faire déposer à l'accueil les téléphones portables et tous les autres appareils permettant des enregistrements photo, vidéo ou audio.
- Le circuit de notoriété tel qu'il a été défini doit rester immuable. Il ne faut pas s'écarter du passage balisé.
- Accompagner les visiteurs en permanence dans l'entreprise dès leur arrivée sur le site jusqu'à la fin de la visite.
- Interdire le contact avec des salariés non préalablement pressentis pour être leurs interlocuteurs.
- Ne pas permettre l'accès au réseau de l'entreprise et gare aux faux prétextes (lecture ou impression d'un document sur une clé USB, consultation de courriers électroniques...).
- La visite se termine lorsqu'on s'est assuré que tous les visiteurs ont quitté le site.



FICHE N°7

Les salons professionnels

Participer à un salon professionnel contribue à renforcer la notoriété de l'entreprise et à offrir des opportunités d'affaires. Ce type de manifestation permet également de se tenir informé sur son environnement (concurrents, état de l'art, marchés...). Toutefois, loin de votre entreprise, les risques d'être victime de manœuvres malveillantes sont accrus. Voici quelques conseils pour les déjouer.

Avant le salon :
la préparation de l'événement :

Préalable nécessaire : définir le cadre précis de la mission et circonscrire les informations qui doivent demeurer confidentielles pour des raisons technologiques, pour des raisons commerciales ou encore pour des raisons liées à la stratégie de l'entreprise.

- Sensibiliser en amont les collaborateurs chargés de représenter les sociétés sur le salon et leur préciser les sujets qui pourront être abordés et ceux qui devront être évités.

- Préparer des axes de réponses sur les sujets sensibles (savoir-faire, innovations...).

- Définir les documents et matériels qui seront emmenés en limitant au strict minimum ceux présentant une sensibilité particulière.

- Étudier la disposition du salon, votre emplacement par apport aux autres exposants (concurrents...).

- Prévoir la location de mobilier de sécurité : vitrine fermant à clé pour les modèles d'exposition, coffre-fort, déchiqueteuse...

- Prévoir un ordinateur portable spécifiquement dédié à ce type de manifestation et expurgé de toutes données sensibles non nécessaires à la mission.

Pendant le salon :

Attention aux vols de documents et outils professionnels : ordinateurs, mallettes, prototypes, maquettes, téléphones, registres contenant les fiches de contact, cartes de visite prospects...

- Assurer la sécurité physique de son ordinateur portable en l'équipant d'un système antivol.

- Garder sous surveillance constante ses outils professionnels pour éviter la perte, le vol, ou la consultation non autorisée.

- Utiliser le mobilier de sécurité.

- Éviter les entretiens sensibles dans les lieux publics.

- Ne pas divulguer d'informations sur vos partenaires, donneurs d'ordre, clients, fournisseurs...

- Méfiez-vous du comportement de certains visiteurs (personnes qui filment ou photographient votre stand).

- Face à un visiteur, s'assurer de son identité et demander systématiquement une carte de visite.

- Formaliser le contact à l'aide d'une « fiche de contact ».

- Prendre garde aux techniques d'ingénierie sociale consistant à amener une personne à livrer des informations sur son entreprise, sur lui-même ou sur ses collègues : faux questionnaires de toutes sorte, flatterie, partage d'intérêt commun...

- Se méfier des rencontres amicales spontanées

- Vigilance à l'égard des prestataires de service qui, par hypothèse, n'appartiennent pas à votre société : agents de sécurité, hôtesses, femmes de ménage...

- Maintenir son degré de vigilance durant toute la durée du salon : lors de festivités, en fin de manifestation alors que la fatigue vous gagne...

A l'extérieur du salon :

- Faire preuve de discrétion dans les transports en commun, dans les taxis, au restaurant et à l'hôtel où séjournent peut être des concurrents.

- Ne jamais laisser sans surveillance dans sa chambre d'hôtel de la documentation sensible et/ou son ordinateur portable.

- Les coffres-forts mis à disposition dans les hôtels n'offrent pas de garanties suffisantes (le personnel de l'hôtel peut disposer du code maître).

Après le salon :

- Faire place nette sur le stand en veillant à ne rien oublier dans le mobilier loué pour l'occasion.

- Procéder à un débriefing et rédaction d'un compte rendu relatant tous les problèmes ou incidents rencontrés.

FICHE N°8

Les déplacements professionnels à l'étranger

Loin des locaux de l'entreprise, le voyageur ne dispose pas de l'ensemble des dispositifs et mesures de protection mises en œuvre au sein de sa structure. Il se déplace dans un environnement hostile.

Face à l'augmentation des risques, et à son isolement, le niveau de vigilance doit être accru. Des règles comportementales spécifiques de sécurité doivent être respectées.

Préparer son voyage :

- Relire attentivement et respecter les règles de sécurité édictées par l'établissement.
- Prendre connaissance de la législation locale.
- Utiliser de préférence du matériel dédié aux missions (ordinateurs, téléphones, supports amovibles, etc.). Ces appareils ne doivent contenir aucune information autre que celles utiles pour la mission.
- Sauvegarder les données emportées. Cette mesure permet de récupérer les informations à son retour en cas de perte, de vol ou de saisie des équipements.
- Éviter de partir avec des données sensibles. Le cas échéant, prévoir avec le RSSI la mise en place d'une protection des données sensibles. (Privilégier, si possible, la récupération de fichiers chiffrés par VPN).
- Emporter un filtre de protection écran pour l'ordinateur en cas d'utilisation dans les transports collectifs et lieux publics.

Pendant le séjour :

- Garder avec soi, ses appareils, supports et fichiers. Ne pas les laisser dans un bureau ou dans la chambre d'hôtel (même dans un coffre).
- Protéger son téléphone portable en retirant la carte SIM et la batterie lors d'un dépôt en consigne.
- Utiliser un logiciel de chiffrement pour toute transmission d'informations sensibles (mail), et vérifier la compatibilité du logiciel avec la réglementation locale.
- Ne pas communiquer d'information confidentielle via le téléphone mobile.
- Effacer les fichiers mémoire des appareils nomades.
- Informer systématiquement son entreprise d'une inspection réalisée par les autorités locales sur ses appareils nomades.
- Signaler toute perte ou vol d'un équipement professionnel à l'entreprise.
- Méfiance à l'égard des pratiques de déstabilisation (risque sexuel, cadeau de grande valeur semant le doute sur votre loyauté ou votre probité lors du passage frontière, ne pas s'exprimer sur la politique du pays visité...).
- Méfiance à l'égard des cadeaux technologiques : ils peuvent contenir des logiciels malveillants.
- Ne pas connecter ses équipements à des postes ou à des périphériques informatiques qui ne sont pas de confiance.

Avant votre retour de voyage :

- Transférer vos données sur le réseau de votre organisme à l'aide de la connexion sécurisée de votre entreprise.
- Effacer l'historique des appels et des navigations.

Lors du retour :

- Changer les mots de passe utilisés pendant le déplacement.
- Avant toute connexion au réseau de l'entreprise, faire analyser les équipements par le responsable de la sécurité informatique.
- Rendre compte systématiquement de tout incident à sa hiérarchie et au responsable de sécurité.

FICHE N°9

La sécurité de l'entreprise à l'épreuve des réseaux sociaux

Espace de socialisation pour les individus, espace de communication pour les entreprises, les réseaux sociaux représentent un média permettant d'accroître sa visibilité. Toutefois, il convient d'en faire une utilisation raisonnée pour ne pas sacrifier sa vie privée ni impacter son entreprise.

Face aux risques (attaques informatiques sur les réseaux sociaux, divulgation d'information confidentielle, perte de contrôle de son image ou de sa réputation) quelques règles élémentaires doivent être respectées.

- A la création du compte, ne renseigner que les informations réellement utiles.
- Créer un mot de passe robuste (10 caractères de type différent).
- Utiliser un mot de passe différent de ceux utilisés pour les applications professionnelles.
- De même, utiliser un mot de passe différent pour chaque compte créé afin d'éviter le piratage de l'ensemble de ses profils.
- Ne pas utiliser l'adresse mail professionnelle. Créer une adresse électronique spécifique pour éviter un accès directe à sa messagerie professionnelle.
- Configurer les paramètres de confidentialité pour circonscrire l'accessibilité à son profil.
- Activer la fonction d'alerte en cas de taggage par une personne malveillante.
- Ne pas mettre d'informations trop personnelles (date de naissance, adresse, numéro de téléphone, photos de soi et de ses proches...).
- Être discret sur ses activités et relations professionnelles.
- Afin de préserver l'entreprise, veiller, avant toute publication, à ne dévoiler aucune information interne et confidentielle.
- Respecter la loi : éviter les commentaires injurieux, diffamatoires et racistes susceptibles d'engager sa responsabilité.
- Désactiver, quand c'est possible les options de géolocalisation de votre appareil nomade, lors de la navigation sur les réseaux sociaux.
- Ne pas mentionner sur son profil une éventuelle habilitation à traiter des informations classifiées.

Contacts

L'intelligence économique en Picardie :
www.iepicardie.org
contact@iepicardie.org

Sécurité économique :
secueco-amiens@interieur.gouv.fr

Ressources

Délégation interministérielle à l'intelligence économique :
www.intelligence-economique.gouv.fr

Service de coordination à l'intelligence économique - Bercy :
www.economie.gouv.fr/scie

Face à la surabondance de l'information, l'entreprise doit pouvoir disposer de l'information stratégique pour lui assurer un avantage concurrentiel.

- Trouver la bonne information, au bon moment, au meilleur coût, afin de prendre la bonne décision.
- Diffuser l'information par des actions d'influence : réseautage, lobbying, communication de crise...

Face au risque de captation de sa propre information, l'entreprise doit protéger son patrimoine immatériel et informationnel.

- La sécurité économique consiste en la protection des informations stratégiques pour l'entreprise (identification des risques et menaces).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA RÉGION
PICARDIE

Préfecture de la région Picardie
51 rue de la République 80020 AMIENS Cedex 9
www.picardie.pref.gouv.fr

Edition : décembre 2013 - Conception : DRRI / Région de Gendarmerie de Picardie & DIRECCTE Picardie - Réalisation maquette : préfecture de la région Picardie / SRCI. Crédits photo : préfecture / PHOVOIR.