Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA RÉGION
PROVENCE-ALPES
CÔTE D'AZUR

LA SÉCURITÉ ÉCONOMIQUE,
UN ENJEU-CLÉ POUR LES ENTREPRISES

Au 21e siècle, les chefs d'entreprise ne peuvent plus s'exonérer des problématiques de sécurité économique et de protection de leur système d'information. Ce guide synthétique permet une première approche des sujets à traiter et des procédures à mettre en œuvre.

DGSI · DPSD · ANSSI · Gendarmerie nationale · Douanes & Droits indirects · INPI Institut national de la propriété industrielle

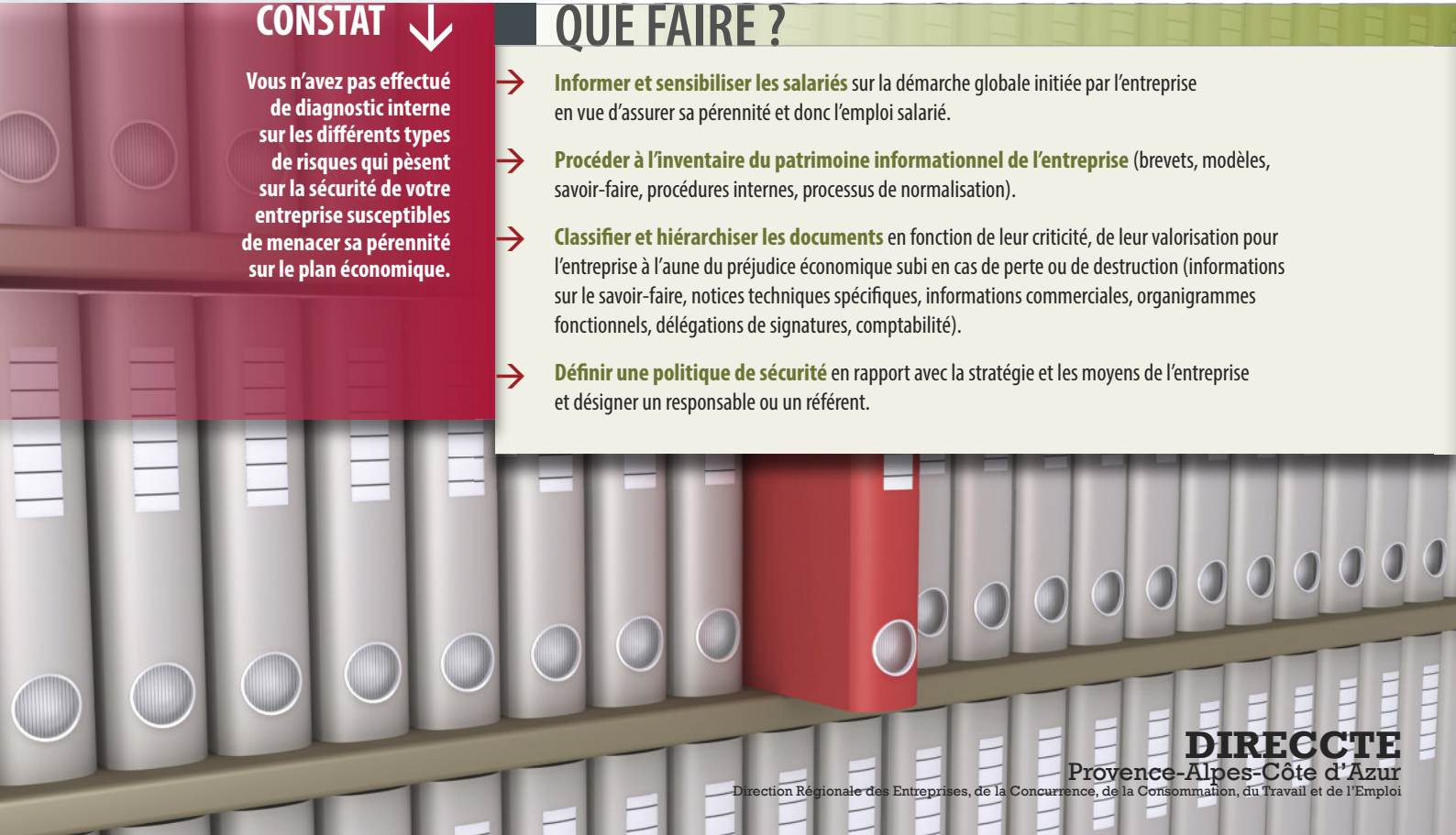
→ DÉFINIR UNE POLITIQUE INTERNE DE SÉCURITÉ RELATIVE À L'INFORMATION STRATÉGIQUE DE VOTRE ENTREPRISE

CONSTAT ↓

Vous n'avez pas effectué de diagnostic interne sur les différents types de risques qui pèsent sur la sécurité de votre entreprise susceptibles de menacer sa pérennité sur le plan économique.

QUE FAIRE ?

- **Informer et sensibiliser les salariés** sur la démarche globale initiée par l'entreprise en vue d'assurer sa pérennité et donc l'emploi salarié.
- **Procéder à l'inventaire du patrimoine informationnel de l'entreprise** (brevets, modèles, savoir-faire, procédures internes, processus de normalisation).
- **Classifier et hiérarchiser les documents** en fonction de leur criticité, de leur valorisation pour l'entreprise à l'aune du préjudice économique subi en cas de perte ou de destruction (informations sur le savoir-faire, notices techniques spécifiques, informations commerciales, organigrammes fonctionnels, délégations de signatures, comptabilité).
- **Définir une politique de sécurité** en rapport avec la stratégie et les moyens de l'entreprise et désigner un responsable ou un référent.



DIRECCTE
Provence-Alpes-Côte d'Azur
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi

→ FAIRE DU FACTEUR HUMAIN UN SUPPORT MAJEUR DE LA RÉSILIENCE ET DE LA SÉCURITÉ DE L'ENTREPRISE

CONSTAT

Une partie importante des informations de l'entreprise est détenue, classée, archivée par les personnels de l'entreprise sur une multitude de supports. Ceux-ci, en quittant l'entreprise, peuvent détourner de manière volontaire ou involontaire des informations sensibles pour l'entreprise, ou être ciblés par des entités extérieures concurrentes.

QUE FAIRE ?

- **Définir un ensemble de procédures et de règles comportementales** se rapportant à la sécurisation de l'information reprises dans les divers documents contractuels (contrat de travail, accords de confidentialité, clause de non-concurrence, règlement intérieur, charte informatique...).
- **Configurer les droits d'accès des salariés au système d'information** à proportion de leurs besoins fonctionnels et opérationnels. Habilitations logiciels, ERP, CRM, SCM.
  Dès la connaissance du départ de la société d'une personne, mener une action sur ses droits d'accès et rester vigilant sur ses agissements.
- **Impliquer le personnel de l'entreprise dans la mise en œuvre des procédures d'accueil** concernant les visiteurs, les stagiaires, les personnels de maintenance, les clients et fournisseurs.
- **À l'extérieur de l'entreprise, recommander une attitude discrète**, y compris lors des déplacements professionnels (colloques, foires, transports en commun, restaurants).

DIRECCTE
Provence-Alpes-Côte d'Azur
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi

➔ DÉFINIR UNE POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PSSI) AFIN DE PRÉSERVER LA CONFIDENTIALITÉ DE VOS DONNÉES

CONSTAT

Vous n'avez pas encore réellement défini une politique de sécurité de vos systèmes d'information (PSSI) ni organisé une protection globale du système au travers de ses différents supports (ex : *BYOD). S'il s'avère que la protection mise en œuvre au fil du temps comporte des failles du fait de sa non cohérence d'ensemble, dès lors, en dépit des mesures prises, vos fichiers sensibles, fichiers clients, modèles non protégés, fichiers comptabilité, stratégie commerciale) pourront être captés de manière illicite par des personnes à l'intérieur ou à l'extérieur de l'entreprise.**

* *Bring your own devices*
Apportez vos appareils personnels

QUE FAIRE ?

- **Faire réaliser un audit de votre architecture informatique** et des risques relatifs à la configuration générale de votre système d'information (infrastructures informatiques propres, infrastructures *cloud*, supports d'information nomades : portables, tablettes, téléphones, clefs USB).
- **Contrôler l'accès au Système d'Information** (comptes à privilège) afin d'assurer la traçabilité des connexions et l'authentification des auteurs (identification, mot de passe).
  Ne pas relier directement le réseau informatique de l'entreprise à Internet.
- **Veiller à la mise à jour du système de protection** (antivirus, *firewall*) et à l'intégrité des sauvegardes informatiques.
- **Privilégier l'accès par VPN** (Réseau Privé Virtuel) lors de connexion au SI de l'entreprise à partir de l'étranger.
- **Mettre en place un monitoring des systèmes** afin de détecter des niveaux d'activité anormaux, à des horaires fortement décalés des phases de travail de l'entreprise.
- **Privilégier des systèmes d'échanges sécurisés** concernant les échanges de données sensibles (cryptage des systèmes de messagerie ou des pièces jointes, plateformes d'échanges sécurisées).
- **Limiter et sécuriser les accès wifi dans l'entreprise.**
  Ne pas garder les mots de passe et codes d'identification constructeur.
- **Prévoir un plan de reprise d'activité** après un sinistre éventuel.

DIRECCTE
Provence-Alpes-Côte d'Azur
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi

→ ASSURER LA PROTECTION PHYSIQUE DU SITE ET DES LOCAUX DE L'ENTREPRISE

CONSTAT

Même si, au 21e siècle, dans un environnement de plus en plus numérique, le périmètre de l'entreprise ne se limite plus à son emprise physique, la protection des locaux et des accès reste essentielle pour la préservation de ses données sensibles, ainsi que pour l'intégrité physique de ses salariés.

QUE FAIRE ?

- **Protéger le site par des barrières physiques adaptées**, respecter l'équation de sûreté : détection + freinage > temps d'intervention (enceinte, grilles, alarmes, codes d'accès, éclairages adaptés).
- **Créer des ZRR (Zones à Régime Restrictif) au sein des entreprises,** dans le cadre de la mise en œuvre de la PPST (Protection du Potentiel Scientifique et Technique de la nation).
  La ZRR permet :
  - de s'appuyer sur le Code Pénal pour défendre les actifs de l'entreprise ; la pénétration dans la ZRR est un délit.
  - de mobiliser légalement les services de sécurité de l'Etat (DGSI ou DPSD) sur les accès à la ZRR.
- **Établir un plan de sécurité interne** avec un accès restrictif aux zones les plus sensibles de l'entreprise (« parcours de notoriété »).
- **Utiliser des systèmes d'alarmes et systèmes anti-intrusion.**
- **Utiliser des mobiliers de sécurité** (coffres-forts, armoires fortes)
- **Contrôler les déplacements à l'intérieur du site et des locaux** (port du badge obligatoire, tenue d'un registre des visites).
- **Signaler systématiquement aux services spécialisés** (police, gendarmerie) toute intrusion, vol, ou tentative d'effraction.

DIRECCTE
Provence-Alpes-Côte d'Azur
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi

→ STRUCTURER, ORGANISER LA COMMUNICATION SUR INTERNET ET PRÉVENIR LES RISQUES LIÉS À UN USAGE MAL MAÎTRISÉ DES RÉSEAUX SOCIAUX

CONSTAT

La communication, les données mises en ligne, les messages émis par l'entreprise destinés à son écosystème véhiculés sur les réseaux sociaux, construisent l'empreinte numérique de la société. Dès lors, la maîtrise, par l'entreprise, de sa communication, de son image(e-réputation), dans un monde numérique, requiert une véritable stratégie organisée à l'interne et à l'externe.

QUE FAIRE ?

- **Contrôler et valider les publications internes** (bulletins), **ou externes** (brochures, plaquettes, documentations techniques) **de l'entreprise**, afin de ne pas laisser filtrer des informations sensibles (innovations brevetables, signature du dirigeant et du responsable de la comptabilité, personnes-clés de la R&D).
- **Sur le site Web, ne pas donner d'informations trop précises** concernant les organigrammes fonctionnels (l'identité – nom, téléphone, mel – des collaborateurs), pour ne pas faciliter des attaques par ingénierie sociale (prévoir des formulaires de contact dédiés pour organiser l'interface entre l'entreprise et l'extérieur).
- **Définir en interne des règles contractuelles précises avec les salariés**, se rapportant à la protection à l'extérieur, de l'image de l'entreprise, de ses projets industriels, ou de ses données sur les réseaux sociaux.
- **Procéder régulièrement à une vérification des informations publiées sur Internet** et les réseaux sociaux concernant le nom de l'entreprise, afin d'identifier des commentaires ou informations préjudiciables à son image et/ou son activité.

DIRECCTE
Provence-Alpes-Côte d'Azur
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi

→ PRÉVENIR L'IMPACT DE CERTAINES PHASES CRITIQUES DU DÉVELOPPEMENT ÉCONOMIQUE DE L'ENTREPRISE ET INTÉGRER L'EXPLOSION DES PHÉNOMÈNES FRAUDULEUX AFIN DE PRÉSERVER SES ACTIFS IMMATÉRIELS ET FINANCIERS

CONSTAT ↓

La recherche de financements, la transmission de l'entreprise par le dirigeant, apparaissent comme des moments-clés dans la vie de la société à un moment où celle-ci peut devenir vulnérable. L'explosion du nombre de faux virements, la diversité des rançongiciels (*cryptolockers*) qui ciblent directement la trésorerie des entreprises sont des menaces qui requièrent la mise en œuvre de procédures particulières.

QUE FAIRE ?

→ **Privilégier l'appui d'entités financières bien identifiées** respectant le code monétaire et financier et les règles bancaires applicables au niveau européen.

→ **Éviter l'adossement en garantie des prêts au portefeuille brevets de l'entreprise,** la rédaction de la clause se rapportant au fait générateur de la mobilisation de la propriété intellectuelle(PI) devant faire l'objet d'une vigilance particulière.

→ **Prévenir les attaques frauduleuses** (faux virements, fraude au président) mises en œuvre par des assaillants mobilisant des techniques d'ingénierie sociale, qui doivent conduire le dirigeant à définir des procédures sécurisées (double signature) pour les virements excédant un seuil prédéfini.

→ **Anticiper les attaques virales** ciblées à partir de logiciels crypto-bloqueurs (cryptolockers) qui cryptent les données vitales de l'entreprise soumise au paiement d'une rançon.
L'entreprise doit donc pouvoir compter sur des sauvegardes complètes, régulièrement vérifiées, pour redémarrer rapidement son activité.

DIRECCTE
Provence-Alpes-Côte d'Azur
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi

LES PARTENAIRES INSTITUTIONNELS EN RÉGION PROVENCE-ALPES-CÔTE D'AZUR

ANIMATION ET COORDINATION DE LA POLITIQUE PUBLIQUE D'INTELLIGENCE ÉCONOMIQUE

PREFECTURE DE REGION PACA – Service Général aux Affaires Régionales (SGAR)
Tél. : **04 84 35 45 88** *vanessa.perles@paca.pref.gouv.fr*

INNOVATION, COMPÉTITIVITÉ, SÉCURITÉ, DÉFENSE ÉCONOMIQUE

DIRECCTE PACA – Déléguée à l'information stratégique et à la sécurité économiques
Tél. : **04 86 67 33 09** *claire.de-guisa@direccte.gouv.fr*

RENSEIGNEMENT ÉCONOMIQUE ET FINANCIER LIÉ À LA PROTECTION DU PATRIMOINE SCIENTIFIQUE ET TECHNIQUE DES ÉTABLISSEMENTS INDUSTRIELS NON CONTRÔLÉS PAR LE MINISTÈRE DE LA DÉFENSE

DIRECTION GENERALE DE LA SECURITE INTERIEURE - DGSI
Tél. : **04 91 00 06 00** *inteleco-ri13@interieur.gouv.fr* (Marseille)
Tél. : **04 92 17 20 81** *inteleco-ri06@interieur.gouv.fr* (Nice)
Tél. : **04 98 03 55 96** *inteleco-ri83@interieur.gouv.fr* (Toulon)
Tél. : **04 32 44 82 41** *inteleco-ri84@interieur.gouv.fr* (Avignon)

PROTECTION DU PATRIMOINE INDUSTRIEL, SCIENTIFIQUE ET TECHNOLOGIQUE DES ÉTABLISSEMENTS INDUSTRIELS CIVILS SOUS CONTRÔLE DU MINISTÈRE DE LA DÉFENSE

DIRECTION DE LA PROTECTION DE LA PROTECTION ET DE LA SÉCURITÉ DE LA DÉFENSE - DPSD
Tél. : **04 42 43 67 86** *bsi.tln@dapesid.net*

PROTECTION ET CONSEILS EN SÉCURITÉ ÉCONOMIQUE, SUIVI DU RENSEIGNEMENT ÉCONOMIQUE ET SOCIAL

GENDARMERIE NATIONALE - Cellule régionale Sécurité Économique
Tél. : **04 91 85 70 52** *LCL sebastien.rigault@gendarmerie.interieur.gouv.fr*
LCL christophe.clarinard@gendarmerie.interieur.gouv.fr

CONSEILS SUR LES RÈGLES DE SÉCURITÉ DE L'ANSSI SERVICES DE L'ÉTAT ET STRUCTURES POUVANT VOUS ORIENTER SUR LA SSI

OBSERVATOIRE NATIONAL DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION – OZSSI-SUD
Tél. : **04 84 35 31 19** *joel.macaruella@interieur.gouv.fr*

PROBLÉMATIQUES CONCERNANT LE FLUX DE MARCHANDISES TRANSITANT À L'IMPORT OU À L'EXPORT, LE SIGNALEMENT DE CONTREFAÇONS, LES CONSEILS SUR L'OPTIMISATION DE TRÉSORERIE DES FORMALITÉS DOUANIÈRES

DIRECTION RÉGIONALE DES DOUANES DE MARSEILLE
Tél. : **09 70 27 84 25** *pae-marseille@douane.finances.gouv.fr*
DIRECTION RÉGIONALE DES DOUANES DE PROVENCE
Tél. : **09 70 27 91 02** *pae-provence@douane.finances.gouv.fr*
DIRECTION RÉGIONALE DES DOUANES DE NICE
Tél. : **09 70 27 87 02** *pae-nice@douane.finances.gouv.fr*

PROTECTION, OPTIMISATION DE LA PROPRIÉTÉ INDUSTRIELLE, DES MARQUES, BREVETS, DESSINS ET MODÈLES

Diagnostics de propriété industrielle et orientation sur les dispositifs d'aide sur la propriété industrielle
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE (INPI)
Tél. : **0 820 210 211 choix 4** *pacaouest@inpi.fr* (Marseille)
pacaest@inpi.fr (Nice)

SENSIBILISATION DES ENTREPRISES SUR LA PROPRIÉTÉ INDUSTRIELLE, L'INTELLIGENCE ÉCONOMIQUE, L'INNOVATION, LA SÉCURITÉ

CHAMBRES DE COMMERCE ET D'INDUSTRIE DE PROVENCE-ALPES-CÔTE D'AZUR
Tél. : **04 91 14 42 51** *xavier.grimaldi@paca.cci.fr*

Coordination éditoriale : **Unité Communication de la DIRECCTE Provence-Alpes-Côte d'Azur**
Design graphique : François Nagot - **www.alliage-design.fr**
Crédits photo / illustrations : **Fotolia**

DIRECCTE
Provence-Alpes-Côte d'Azur
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi