



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET
DE LA RÉGION
BASSE-NORMANDIE

Réseau Intelligence Économique
de Basse-Normandie

Sécurisez
votre système
d'information

Réseau Basse-Normandie
IE Intelligence
Economique



Introduction

Pourquoi sécuriser mon système d'information ?

Mon système d'information (SI) est l'ensemble des ressources (matériels, logiciels, personnels, données et procédures) qui permettent à mon entreprise de collecter, traiter et diffuser de l'information de manière maîtrisée.

L'entreprise doit donc concilier les nécessités de communiquer des informations et de préserver et sécuriser certaines d'entre-elles, en mettant en place une démarche de sécurité de son système d'information.

La mise en œuvre de cette démarche est de la seule responsabilité du chef d'entreprise, elle implique cependant l'ensemble des salariés.

Sécuriser mon système d'information est un facteur de pérennité et de compétitivité de mon entreprise.

Pour compléter ce document, des fiches réflexes sont consultables sur le site : www.basse-normandie.net

Je me pose des questions...

- ▶ Quel est l'intérêt de disposer d'une charte informatique ?
- ▶ Comment éviter de se faire pirater son système informatique ?
- ▶ Quelles règles d'hygiène informatique doivent appliquer mes salariés ?
- ▶ Si j'externalise la gestion de mon SI, est-ce que j'accrois les risques liés à la sécurité des données ?

J'ai des réponses sur...

Ma responsabilité.....	page 4
Que protéger.....	page 5
Quels sont les risques.....	page 6
Quelles procédures.....	page 7
Quelques bonnes pratiques.....	page 8
Mes contacts.....	page 10
Liens utiles.....	page 11

Ma responsabilité ?

En tant que dirigeant

Je respecte la loi car

- je suis responsable de l'utilisation qui est faite des systèmes d'information⁽¹⁾
- je mets en œuvre tout moyen nécessaire pour éviter les comportements à risques⁽²⁾
- je suis responsable des données collectées ou stockées⁽³⁾

J'ai des bonnes pratiques

- je désigne un responsable sécurité des systèmes d'information
- je rédige la charte informatique de mon entreprise et la notifie à chaque salarié
Sans charte informatique, je suis seul responsable de mon SI, avec une charte informatique la responsabilité de mes salariés peut être engagée,
- je m'assure de la sensibilisation et/ou de la formation de mon personnel

En tant qu'utilisateur

- je suis responsable de l'utilisation des outils et systèmes mis à ma disposition
- je respecte la charte informatique

Se référer aux articles :

⁽¹⁾ 121-1, 121-2 du code pénal, 1384 du code civil

⁽²⁾ 1383 du code civil

⁽³⁾ 226-17 du code pénal, 34 de la loi n°78-17 CNIL du 06/01/1978

Que protéger ?

Ce qui est nécessaire au fonctionnement de l'entreprise

Les données sensibles :

- fichiers fournisseurs, clients, salariés
- comptabilité, tarifs, marges, données financières
- procédures : qualité, process
- brevets, secrets, savoir-faire, bureau d'étude
- données d'accès : digicode, mot de passe

Les process sensibles :

- décisionnels : actionnariat, communication
- production, achats (fournisseurs, sous-traitance)
- commerciaux : prospection, négociation
- financiers : paye, règlements
- ressources humaines : recrutement, stagiaire

Où sont mes données ?

- sur quels supports : papier, clés USB, CD, Cloud (serveurs sur réseau internet)
- dans quelles machines : ordinateurs, téléphones portables, machines-outils, photocopieurs
- dans quels réseaux : interne à l'entreprise, réseau des partenaires, messagerie, Internet
- sont-elles détenues de façon informelle par les dirigeants, cadres, assistants, personnels extérieurs ?

Quels sont les risques ?

J'identifie les risques propres à mon entreprise

Divulgarion :

je ne veux pas que mes concurrents accèdent à mes données confidentielles

- fichier client à la concurrence
- données critiques circulant sur des réseaux que je ne maîtrise pas

Altération :

je ne veux pas que mes données ou process soient dégradés

- falsification de virements de paye
- fichier de paramétrage d'une machine outil

Indisponibilité :

je ne peux pas attendre pour utiliser mes données

- informations indispensables disponibles sur une seule machine
- panne de réseaux téléphonique, informatique

J'identifie les incohérences de mon système d'information pour connaître tous les risques et limiter les impacts sur mon image, mes finances, mes relations, ...

Quelles procédures ?

- J'identifie les ressources matérielles, logicielles, humaines de mon entreprise
- Je contrôle les accès physiques
- Je sécurise, j'enregistre et je surveille les accès aux systèmes d'information de l'entreprise
- Je contrôle les accès aux applications et aux données : mot de passe individuel, verrouillage automatique de l'ordinateur, des smartphones
- Je définis les droits afin que chacun n'accède qu'aux informations dont il a besoin
- Je précise les règles d'utilisation des matériels personnels pour des usages professionnels et inversement
- Je rédige mon Plan de Continuité de l'Activité
- Je connais mes droits et mes obligations juridiques
 - envers mes salariés et partenaires de l'entreprise
 - par rapport aux recommandations de la CNIL
- Je veille à la bonne rédaction des clauses de mes contrats de sous-traitance et d'assurance, ainsi qu'à leur révision périodique

Quelques bonnes pratiques...

- Je responsabilise mes salariés sur les dangers liés à l'utilisation des moyens informatiques de l'entreprise en dehors de celle-ci, mais aussi à l'utilisation de supports externes, disques durs, clés USB, téléphones, sur le parc informatique de l'entreprise
- Je vérifie que mes informations sensibles (écrans d'ordinateur, paperboard, documents papier...) ne sont pas visibles de l'extérieur des bâtiments
- En déplacement, j'applique un filtre anti-regard sur mes écrans (ordinateurs, tablettes), je suis prudent dans mes conversations et je ne laisse pas mon matériel sans surveillance
- Lors de rendez-vous ou d'intervention de prestataires, je ne laisse pas mes visiteurs sans surveillance
- Je gère la destruction de mes documents, je broie les documents papier et supports amovibles, je détruis mes disques durs, y compris ceux des photocopieurs et imprimantes après l'avoir contractualisé
- J'utilise toujours des mots de passe personnels que je n'affiche pas à la vue de tous !
- Je sauvegarde mes données régulièrement et les stocke à l'abri du feu ou d'autres dangers

... pragmatiques

- Je porte une attention particulière aux informations qui peuvent sortir de l'entreprise : rapport de stage, organigramme sur Internet, projets stratégiques échangés par messagerie...
- Je sensibilise régulièrement mes salariés
- En tant que dirigeant, je suis une cible privilégiée, je suis d'autant plus prudent. Je ne stocke pas l'intégralité de la vie de l'entreprise sur mon ordinateur portable
- Je suis peut-être déjà piraté, sans le savoir. Je n'attends pas l'accident pour mettre en place des moyens de détection
- J'adapte mes investissements en sécurité aux risques encourus
- Je veille à l'homogénéité de mon niveau de sécurité : inutile de blinder la porte si je laisse la fenêtre ouverte
- J'engage une démarche continue, pas à pas : j'identifie, j'améliore, je vérifie, et je recommence

La sécurité est une affaire de dosage, entre l'inconscience et la paranoïa, je choisis la prudence et la sagesse

Mes contacts...

Pour signaler des intrusions ou demander conseil :

Comité opérationnel de sécurité économique

Animatrice : Corinne Marbach

Tél. : 06 07 26 17 05

Mel : corinne.marbach@direccte.gouv.fr

Direction régionale du renseignement intérieur de Basse-Normandie

Tél. : 02 31 30 94 60

Mel : ie.basse-normandie@interieur.gouv.fr

Gendarmerie, référent régional

Tél. : 02 31 35 92 31

Mel : alain.gloannec@gendarmerie.interieur.gouv.fr

DPSD Détachement de Cherbourg

Tél. : 02 33 92 60 52

Chargé de mission numérique au SGAR

Tél. : 02 31 30 63 06

Mel : pierre.touzeau@basse-normandie.pref.gouv.fr

Pour vous faire accompagner par des spécialistes juridiques, informatiques... consultez l'annuaire de compétence du site : www.basse-normandie.net

Liens utiles

www.ssi.gouv.fr

www.certa.ssi.gouv.fr

Agence Nationale pour la Sécurité
des Systèmes d'Information

www.securite-informatique.gouv.fr

Portail grand public de l'ANSSI

www.cnil.fr

Commission Nationale Informatique et Libertés

www.afnor.fr

Agence Française de Normalisation

www.internet-signalement.gouv.fr

Portail officiel de signalement
des contenus illicites de l'Internet

www.clusif.asso.fr

Club de la Sécurité de l'Information Français

www.cdse.fr

Club des Directeurs de Sécurité des Entreprises

www.cases.lu

Portail luxembourgeois de la sécurité
de l'information pour tous

Le Comité opérationnel de sécurité économique
remercie les sociétés

ELITT, MEDOLISE et CYRIL PATRIGEON

d'avoir apporté leur expertise
à la rédaction de ce document



Edition : janvier 2014

Réseau Basse-Normandie
IE Intelligence
Economique

