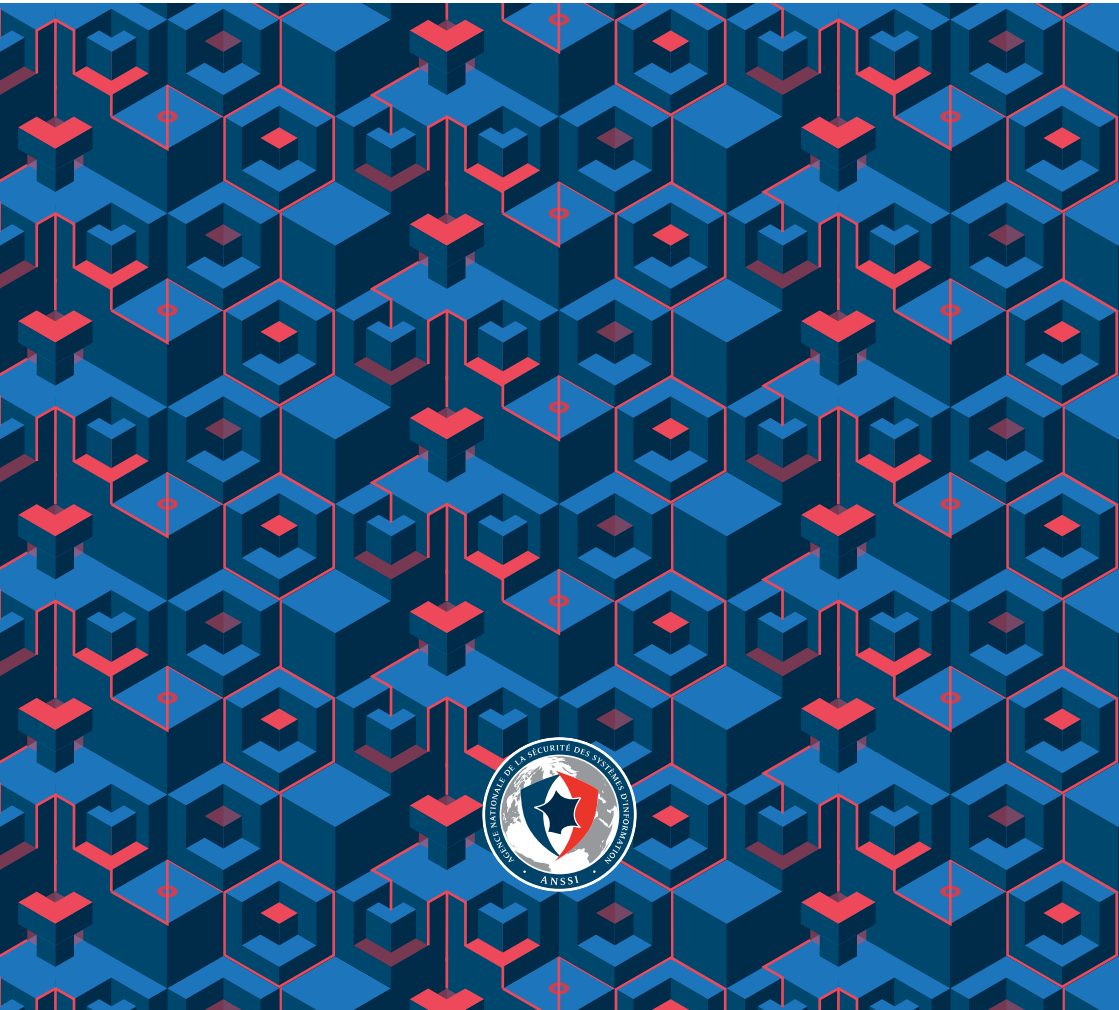
CHARTE D'UTILISATION DES MOYENS INFORMATIQUES ET DES OUTILS NUMÉRIQUES

GUIDE D'ÉLABORATION EN 8 POINTS CLÉS POUR LES PME ET ETI



Les attaques informatiques n'ont de cesse de progresser en nombre, en efficacité et en complexité avec des conséquences parfois dramatiques : atteinte à l'image et à la réputation, indisponibilité des infrastructures ou encore impact financier. Mais la transition numérique est également porteuse de formidables opportunités pour les entreprises qui sauront les saisir à la lumière de leurs besoins en matière de sécurité du numérique.

La mise en œuvre d'un socle de bonnes pratiques informatiques irriguant toute l'entreprise selon un processus vertueux nécessite de passer par certaines étapes fondamentales. L'élaboration d'une charte d'utilisation des moyens informatiques et des outils numériques en fait partie.

Si la prise de conscience du risque numérique progresse, elle reste encore insuffisante au regard des dispositions prises par les entreprises pour sécuriser leurs systèmes d'informations. C'est de ce constat fait par les référents de l'ANSSI en régions qu'est né ce guide à destination des petites et moyennes entreprises (PME) et des entreprises de taille intermédiaire (ETI). Il recense ainsi huit points clés essentiels à l'élaboration d'une telle charte et peut également permettre à l'entreprise qui en est déjà dotée de s'assurer de son adéquation avec les principes développés dans ce guide.

Dirigeants et entrepreneurs, saisissez-vous de l'opportunité que représente ce guide pour faire de la sécurité un enjeu partagé par l'ensemble des utilisateurs de votre entreprise (salariés, partenaires, sous-traitants, etc.). La sécurité du numérique est assurément l'affaire de tous.

Guillaume Poupard
Directeur général de l'ANSSI

SOMMAIRE

AVANT-PROPOS

L'élaboration d'une charte d'utilisation des moyens informatiques et sa mise à disposition auprès des utilisateurs figurent parmi les **bonnes pratiques** à mettre en œuvre dans toute entité dont les informations, données et activités s'appuient sur un système d'information. Il s'agit d'un document à portée juridique dont la rédaction implique de nombreuses compétences transverses. Les recommandations présentées ci-après ne sont pas exhaustives. Il est donc fortement conseillé de solliciter l'avis d'un spécialiste lors de la rédaction de ce document. Une **analyse de risques** doit par ailleurs précéder l'élaboration de cette charte afin de mettre en exergue la façon la plus adéquate de protéger les informations les plus sensibles.

LES HUIT POINTS CLÉS

1
L'OBJECTIF

La charte d'utilisation des moyens informatiques a pour finalité de contribuer à la **préservation de la sécurité du système d'information** de l'entité et fait de l'utilisateur un acteur essentiel à la réalisation de cet objectif.

De façon pragmatique, elle permet d'informer l'utilisateur (bien souvent le salarié) sur :

- les usages permis des moyens informatiques mis à sa disposition ;
- les règles de sécurité en vigueur ;
- les mesures de contrôle prises par l'employeur ;
- et les sanctions encourues par l'utilisateur.

Il est donc primordial que la charte soit aisément lisible et parfaitement compréhensible par chacun des utilisateurs, quel que soit son degré de familiarité avec l'informatique. Au besoin, la charte servira également de support juridique à la collecte de preuves numériques en cas de contentieux.

L'objectif du document peut être abordé dès le préambule en soulignant le rôle de l'utilisateur à qui incombe une utilisation raisonnée et responsable des ressources informatiques et technologiques de l'entité mises à sa disposition.

2
DES DÉFINITIONS CLAIRES ET PRÉCISES

Définir les termes clés du document permet de limiter leur interprétation juridique (administrateur, messagerie électronique, moyens d'authentification, système d'information, utilisateur, etc.). Ces définitions peuvent tenir compte de spécificités propres à l'entité et ne pas se contenter d'une explication générique. À titre d'exemple, les moyens d'authentification peuvent différer d'une entité à une autre.

3
L'OBJET ET SA PORTÉE

La charte doit rappeler ce sur quoi elle porte. Notamment, elle doit exprimer de manière explicite qu'elle a pour objet de préciser les **droits et devoirs de l'utilisateur.** Plusieurs types de charte existent selon l'économie envisagée du document (liste exhaustive ou utilisation raisonnable, grands principes, etc.). Une charte précise sur les droits et devoirs des utilisateurs sera toujours préférable afin d'éviter toute interprétation divergente.

À noter que, **l'administrateur** peut faire l'objet d'une partie de la charte, voire d'une charte spécifique. Ses devoirs seront à la mesure des **droits souvent étendus** qui lui sont confiés. En effet, l'administrateur bénéficie de **privilèges élevés** qui le conduisent, par conséquent, à porter une responsabilité plus grande. En particulier, l'administrateur est tenu par des obligations de loyauté, de transparence et de confidentialité renforcées [1].

[1] ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information,* note technique, juillet 2015 — https://www.ssi.gouv.fr/securisation-admin-si/

4
LES USAGES

De nombreuses questions sont à envisager lorsque l'entité souhaite fixer les règles d'usage de son système d'information. L'entité met-elle à disposition une messagerie professionnelle ? L'utilisateur dispose-t-il d'une connexion Wi-Fi ? Quels sont les moyens d'authentification prévus par l'entité ? L'utilisateur peut-il avoir recours à des supports amovibles ? Si oui, lesquels ? À quelles fins la navigation sur Internet au moyen des ressources informatiques de l'entité est-elle permise ? Autant d'aspects à considérer au travers des étapes suivantes :

- **Recenser l'ensemble des besoins auxquels le système d'information doit répondre.** Par exemple, le système d'information peut permettre aux employés de gérer les besoins RH, de communiquer en interne ou en externe par messagerie sur des sujets sensibles ou non, ou encore de gérer certains besoins métier dont il s'agit de faire l'inventaire. Cette analyse permettra, *in fine*, de déterminer les pratiques autorisées en fonction de la sensibilité du système d'information concerné.

- **Répertorier l'ensemble des moyens informatiques et outils numériques mis à disposition des utilisateurs.** Il peut s'agir d'un poste de travail nomade ou non, d'un ordiphone (smartphone), de supports amovibles (clé USB), d'imprimantes avec ou sans serveur d'impression, de serveurs de partage de fichiers, d'un service de messagerie, d'une application web de gestion RH, ou encore d'une application métier.

- **Définir les pratiques autorisées** afin de permettre à l'utilisateur d'identifier les règles applicables aux systèmes d'information sur lesquels il intervient. Citons par exemple, le transfert de documents entre postes par clé USB, l'envoi de documents en pièce jointe par mail, ou encore la navigation sur Internet à titre privé.

L'ANSSI préconise un certain nombre de bonnes pratiques pour sécuriser son système d'information (*Guide d'hygiène informatique*, *Guide des bonnes pratiques de l'informatique*, etc.), lesquelles peuvent être reprises dans la charte. Les usages doivent définir de façon précise les limites de l'utilisation à titre privé des moyens informatiques, qu'elle soit raisonnable, résiduelle ou interdite.

Il est également fortement déconseillé par l'ANSSI [2] d'utiliser ses outils personnels à des fins professionnelles (et inversement) en raison du manque de contrôle de ces équipements et des risques en matière de sécurité des données. La charte doit impérativement prendre en compte cette pratique largement répandue et définir les mesures que l'entité entend faire appliquer pour préserver la sécurité de son système d'information et protéger les informations personnelles de l'utilisateur.

Le cas échéant, l'entité devra définir les modalités d'exercice du droit à la déconnexion du salarié, conformément à l'article L. 2242-8 du Code du travail.

[2] ANSSI-CGPME, *Guide des bonnes pratiques de l'informatique*, guide, mars 2015, règle n°11.

5
DÉFINIR LES DEVOIRS DE L'UTILISATEUR

Outre les obligations générales qu'il est bon de rappeler, les **devoirs de l'utilisateur** découlent directement des usages autorisés définis en amont.

Ces devoirs vont du simple bon sens au respect d'obligations techniques spécifiques qui sont fonction de l'architecture du système d'information de l'entité et des mesures de sécurité qu'elle applique.

Un certain nombre de **principes essentiels** peuvent être rappelés afin, notamment, de sensibiliser l'utilisateur sur le rôle déterminant qui est le sien dans la protection du système d'information de l'entité. La charte abordera la question du respect par l'utilisateur d'obligations générales telles que la confidentialité, la discrétion, la loyauté ou la vigilance.

Chacun de ces principes essentiels peut, dans un second temps, être décliné par des **mesures concrètes** plus détaillées dont voici quelques exemples :

- l'utilisateur ne pourra communiquer d'informations qu'aux personnes ayant besoin d'en connaître ;
- il devra utiliser les moyens mis à sa disposition pour chiffrer les informations de l'entité ;

- il ne devra en aucun cas transmettre à des tiers les moyens d'authentification qui lui sont fournis par l'entité, lesquels doivent rester personnels et confidentiels ;

- il devra utiliser des mots de passe qui respectent les bonnes pratiques en vigueur [3] ;

- il devra appliquer les mesures de sécurité demandées par l'entreprise avant tout import de données d'origine extérieure ;

- il ne devra jamais mener d'actions engageant la responsabilité juridique ou financière de l'entité en répondant par exemple à un courriel dont l'authenticité n'est pas vérifiée.

L'ensemble des devoirs de l'utilisateur prévu par la charte doit conduire ce dernier à adopter un **comportement responsable** vis-à-vis du système d'information de l'entité.

[3] ANSSI, *Recommandations de sécurité relatives aux mots de passe*, note technique, juin 2012 — https://www.ssi.gouv.fr/mots-de-passe/

6
LES MESURES DE CONTRÔLE

Les mesures de contrôle que l'entité peut mettre en place peuvent être étendues, pourvu qu'elles aient fait l'objet d'une **information préalable des utilisateurs** (via la charte) et qu'elles soient **conformes au droit en vigueur.**

La charte devra donc lister les mesures et les conditions dans lesquelles elles sont mises en œuvre (conservation des données de connexion, chiffrement des données, déchiffrement de flux https, gestion stricte des accès, contrôle des messageries professionnelles, etc.). Ces mesures devront être **proportionnées** à l'objectif poursuivi.

L'ANSSI et la CNIL proposent toutes deux de la documentation permettant d'établir les limites dans lesquelles les mesures de contrôle par l'entité peuvent être mises en place.[4]

[4] CNIL, *Guide pour les employeurs et les salariés*, édition 2010 — https://www.cnil.fr/
ANSSI, *Recommandations de sécurité concernant l'analyse des flux HTTPS,* note technique, octobre 2014 — https://www.ssi.gouv.fr/analyse-https/
ANSSI, *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*, note technique, décembre 2013 — https://www.ssi.gouv.fr/journalisation/

7
LES SANCTIONS

La charte informatique étant un document de portée juridique, elle permettra de fonder les sanctions à l'encontre d'un utilisateur qui ne l'aurait pas respectée. Il est impératif de prévoir une **échelle des sanctions disciplinaires.** La sanction doit être proportionnée à la gravité du manquement, le licenciement pour faute apparaissant comme la sanction ultime pour une faute grave commise par l'utilisateur.

D'autres sanctions, de nature **civile ou pénale**, peuvent être prononcées par les juridictions compétentes.

Si les sanctions disciplinaires découlent directement de la charte informatique, les sanctions pénales peuvent s'appliquer indépendamment de la charte, dès lors qu'une infraction est commise.

Il est utile de rappeler à l'utilisateur que ses actions peuvent avoir des conséquences juridiques lourdes eu égard à des comportements non autorisés. Citons parmi les plus évidents le non-respect de ses obligations, le téléchargement illégal, la consultation de sites à caractère pédopornographique, etc.

8

S'ASSURER DE L'OPPOSABILITÉ DE LA CHARTE

L'opposabilité de la charte nécessite également son acceptation par les utilisateurs (signature de la charte ou annexe au contrat de travail).

Toutefois, afin d'éviter tout refus de l'utilisateur ou renégociation du contrat de travail, la charte peut être annexée au règlement intérieur de l'entité. Dans ce cas, outre la **consultation des instances représentatives du personnel** (comité d'entreprise, comité technique paritaire ou instance équivalente) lorsqu'elles existent et la communication à l'inspection du travail, la charte devra être **portée à la connaissance des utilisateurs.** Cette information peut avoir lieu au travers d'une notification individuelle de la charte (remise en mains propres, message électronique, etc.) ou être affichée ou diffusée sur l'intranet de l'entité par exemple, avec le règlement intérieur.

Les cas supposant l'intervention d'utilisateurs extérieurs (infogérance, sous-traitance, co-traitance, partenariats, etc.) doivent également être pris en compte. L'opposabilité de la charte à ce type d'utilisateur pourra être assurée grâce à son insertion dans les contrats d'entreprise. Dans ce cas, le prestataire devra en informer ses salariés.

En cas de contentieux, des sanctions prises à l'encontre d'utilisateurs n'ayant pas connaissance de la charte pourraient être annulées par les juges.

À noter que ce document lie autant l'employeur que l'utilisateur. Il appartiendra à l'entité de faire respecter la charte de façon effective. En effet, la tolérance antérieure de manquements à la charte risque d'entraîner, en cas de contentieux, l'annulation des sanctions prononcées sur ce fondement.

Enfin, dans tous les cas, l'entité procèdera à la **déclaration, voire à la demande d'autorisation auprès de la CNIL des traitements de données à caractère personnel** que l'entité opère pour la mise en œuvre des mesures de contrôle prévues par la charte. À ce titre, elle devra également informer les utilisateurs de leurs droits tels que le droit d'opposition pour motif légitime ou les droits d'accès et de rectification.

RESSOURCES UTILES

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, note technique, juillet 2015 — https://www.ssi.gouv.fr/securisation-admin-si/

ANSSI-CGPME, *Guide des bonnes pratiques de l'informatique,* guide, mars 2015 – https://www.ssi.gouv.fr/guide-bonnes-pratiques/

ANSSI, *Guide d'hygiène informatique – Renforcer la sécurité de son système d'information en 42 mesures*, guide, janvier 2017 — https://www.ssi.gouv.fr/hygiene-informatique/

ANSSI, *Recommandations de sécurité relatives aux mots de passe*, note technique, juin 2012 — https://www.ssi.gouv.fr/mots-de-passe/

CNIL, *Guide pour les employeurs et les salariés*, édition 2010 – https://www.cnil.fr/

ANSSI, *Recommandations de sécurité concernant l'analyse des flux HTTPS*, note technique, octobre 2014 — https://www.ssi.gouv.fr/analyse-https/

ANSSI, *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*, note technique, décembre 2013 — https://www.ssi.gouv.fr/journalisation/

Version 1.0 - Juin 2017

20170613-1450

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr - communication@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN