CHARTE DES BONNES PRATIQUES

CYBERSECURITE - NORMANDIE

Contact : cybersecurite@normandie.fr

https://www.normandie.fr/cybersecurite

T1-2021

Préambule

La transformation numérique en cours implique de véritables opportunités de croissance, mais également des risques importants pour la protection de l'information comme des infrastructures.

C'est en ce sens, et en lien avec une actualité dense de cyberattaques visant des acteurs multiples et variés, que le Gouvernement a présenté le 18 février 2021 sa stratégie nationale « Cybersécurité, faire face à la menace ». Parmi les objectifs, la consolidation de la filière, l'amélioration d'une culture « d'hygiène informatique » et le renforcement des acteurs, publics et privés sont affichés.

La cybersécurité est un enjeu transversal pour la Région Normandie qui l'a inscrite dans sa stratégie numérique dès 2017, tant dans le volet dédié aux infrastructures numériques, pour accompagner la transformation numérique des acteurs et pour faire émerger un écosystème de confiance de la donnée en Normandie. En lien avec les actions de sensibilisations menées dans le cadre de la dynamique d'intelligence économique territoriale, une première charte, co pilotée avec la CCI Normandie et le soutien de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) a été lancée, en 2018, pour engager les prestataires informatiques et numériques dans de bonnes pratiques en cybersécurité lors de la mise en œuvre de leurs prestations ainsi qu'une sensibilisation à ces bonnes pratiques auprès de leurs clients.

Aussi, la Région Normandie, en qualité de collectivité compétente en matière d'aménagement du territoire et de développement économique, et les services de l'État en région, en qualité de garants de la continuité des activités essentielles de la Nation et de la politique de sécurité économique à destination des entreprises, ont décidé de joindre leurs efforts, avec le soutien de l'ANSSI, dans le cadre de la présente charte, afin de créer et soutenir une dynamique régionale en matière de cybersécurité.

Article 1 – Fondement

Initiée dans une démarche collaborative et volontaire avec des prestataires informatiques et numériques pour l'amélioration des pratiques et la sensibilisation autour des risques numériques, la charte est mise en œuvre par les services de la Région Normandie, dont l'Agence de Développement pour la Normandie (AD Normandie), et les services de l'État en région, dont l'ANSSI à travers son délégué Normandie, en partenariat avec la Chambre de Commerce et d'Industrie de Normandie (CCI Normandie), Cap'Tronic, le CLUSIR Normandie, le Normandigital, Normandy Web Xpert (NWX) et le Pôle TES.

La présente charte ne comporte aucune mesure coercitive, elle invite les structures privées et publiques qui souhaitent rejoindre cette initiative à se conformer aux principes qu'elle édicte, et ne se substitue pas aux dispositions légales et réglementaires existantes.

Tout demandeur doit avoir un établissement en Normandie.

Article 2. DEFINITIONS

Bénéficiaire : usager ou client qui bénéficie de l'intervention ou d'un service mis en œuvre par un signataire.

Bonnes pratiques : ensemble de méthodes et de comportements qui font consensus et qui sont considérés comme indispensables, relevant d'une évidence non formalisée, de normes et de méthodes techniques, de textes réglementaires et figurant notamment dans des guides cités en référence.

Charte : document établissant l'ensemble des principes fondamentaux qui doivent être respectés par les signataires.

Comité de pilotage : groupe formé par les services de la Région Normandie, dont l'AD Normandie, et les services de l'État en région, dont l'ANSSI à travers son délégué Normandie, et leurs partenaires. La constitution

de ce comité de pilotage est définie tel que précisé dans le règlement interne. Le comité de pilotage a la responsabilité de l'écriture et du respect du règlement interne.

Comité d'agrément : groupe formé de partenaires de la Charte choisis pour leur légitimité à apprécier l'adéquation d'une demande d'adhésion avec les principes de la Charte pour le collège « Prestataires engagés ».

Cybersécurité : état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Demandeur : entité, privée ou publique, qui exprime le souhait de devenir signataire de la charte.

Intervenant : employé ou sous-traitant d'un signataire réalisant une mission pour celui-ci, dont la relation contractuelle avec le signataire l'engage par incidence dans la démarche de la présente Charte.

Prestataire : organisme, proposant une offre de service, interne ou externe et relevant du domaine informatique ou numérique, qui s'inscrit pleinement dans la démarche de la charte.

Règlement interne : document écrit par le Comité de pilotage précisant les processus d'entrée et de sortie ainsi que les attendus pour les demandeurs et signataires de la Charte.

Signataire : demandeur qui, après examen de sa candidature tel que présenté en article 4, a signé son engagement et les documents afférents pour formaliser son entrée dans la présente charte.

Usager : entité, privée ou publique (entreprise, collectivité territoriale, association, établissement de santé…) bénéficiant des services proposés par les prestataires et mis en œuvre par les intervenants, dans le cadre d'une relation suivie et récurrente avec ces derniers.

Article 3. OBJET

Cette charte vise à diffuser les bonnes pratiques en cybersécurité auprès de tous les acteurs normands pour élever le niveau global de cybersécurité en Normandie dans l'objectif de réduire les risques numériques des entreprises, des structures de développement ou des collectivités territoriales, tant au niveau des prestataires que des usagers, et à identifier les spécialistes du domaine à même d'accompagner, d'anticiper, de résoudre ou de gérer les crises.

L'adoption d'un comportement vigilant et de bonnes pratiques, en s'appuyant sur la puissance des systèmes d'information et des outils numériques et la connaissance d'acteurs engagés dans cette démarche est un pilier du développement et de la sécurité économiques de la Normandie.

Article 4. MODALITES D'ENGAGEMENT

Trois (3) collèges sont mis en place :

Collège « Prestataires cybersécurité » : prestataires spécialisés en cybersécurité et reconnus par un label ou une certification, dont la liste est présentée en annexe 1 « Cybersécurité : Labels, normes et référentiel de spécialisation ».
Collège « Prestataires engagés » : prestataires, œuvrant dans les domaines informatiques et numériques, qui s'inscrivent dans une démarche volontaire et vertueuse de cybersécurité
Collège « Usagers engagés » : entités privées et publiques, non prestataires informatiques ou numériques, qui s'inscrivent dans une démarche volontaire et vertueuse en cybersécurité.

Chaque entité qui souhaite se prévaloir de la Charte et compter parmi les signataires devra adresser au comité de pilotage une demande motivée et appuyée des éléments nécessaires à l'appréciation du respect de la Charte, dont les attendus seront précisés par le règlement interne établi par le comité de pilotage.

Cette demande est ensuite instruite et validée par le comité de pilotage, à travers les processus précisés par le règlement interne.

Le signataire signifie par courrier avant le 31 janvier de chaque année son engagement à poursuivre le respect des principes de la Charte. Chaque année, des signataires pourront être contactés pour suivre le respect des engagements respectifs tel que décrit dans le règlement interne.

Article 5. ENGAGEMENTS DES SIGNATAIRES

Les signataires de la Charte s'engagent à :

- Respecter les bonnes pratiques professionnelles en termes de cybersécurité (techniques, juridiques, organisationnelles, communication, protection des données personnelles…) selon les recommandations de l'ANSSI et de la CNIL,
- Inciter les intervenants dans un système d'information, informatique ou de production, (sous-traitants, prestataires, clients, salariés…) à respecter les engagements de la Charte,
- Informer et conseiller les bénéficiaires et les inciter à adopter de bonnes pratiques numériques, notamment en s'appuyant sur les outils proposés en annexe 2,
- Participer assidument aux échanges avec la communauté des signataires de la présente Charte,
- Porter à la connaissance des autres adhérents toute information qu'il juge pertinente pour améliorer la connaissance et les moyens de lutte contre les risques numériques,
- Promouvoir la Charte, les guides et les recommandations de l'ANSSI et de la CNIL sur leurs outils de communication,

Plus particulièrement pour les prestataires des collèges « prestataires cybersécurité » et « prestataires engagés » :

- Proposer aux bénéficiaires qui le souhaitent de partager des éléments d'information sur la prestation reçue vers le comité de pilotage de la présente Charte,
- Tenir informés ses bénéficiaires des risques numériques et de leur prévention,
- Respecter les questions liées au secret et à la confidentialité des informations, y compris dans le cadre du secret des affaires,
- Intégrer dans toutes ses propositions techniques et commerciales un volet cybersécurité.
- Informer le comité de pilotage de tous changements de gouvernance et de statuts (labels, certifications, etc.) ayant un impact sur leur activité et leur rattachement à un collège particulier de la présente charte.

Article 6. PREVALENCE DES SIGNATAIRES

Tout signataire de la présente Charte est en droit de s'en prévaloir et de valoriser son engagement au regard de ses bonnes pratiques en cybersécurité.

Il bénéficie des échanges d'informations, dont il peut faire profiter ses relations, et d'outils mis à disposition.

Article 7. CONTROLE ET SANCTIONS EVENTUELLES

Les bénéficiaires ont la possibilité de faire part au comité de pilotage de leur niveau de satisfaction quant au respect des engagements du signataire tels que définis à l'article 6.

Le signataire est informé que tout élément d'information le concernant et remonté vers le comité de pilotage peut faire l'objet d'une instruction par celui-ci. Tout manquement à la présente Charte peut entrainer la radiation temporaire ou définitive de la liste des signataires référencés.

Article 8. REFERENCES ET OUTILS

- Articles 323-1 à 323-7 du Code pénal, issus de la loi n°88-19 du 5 janvier 1988 et complétés par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique « Des atteintes aux systèmes de traitement automatisé de données »
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n°2004-801 du 6 août 2004et par la LOI n°2016-1321 du 7 octobre 2016 et Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD).

- Guide d'élaboration en 8 points-clés d'une Charte d'utilisation des moyens informatiques et des outils numériques
- Guide des bonnes pratiques de l'informatique
- Guide d'hygiène informatique
- Référentiel d'exigences de sécurité pour les prestataires d'intégration et de maintenance de systèmes industriels
- CNIL–Guide LA SÉCURITÉ DES DONNÉES PERSONNELLES

La liste des références et des outils est amendée et actualisée par l'annexe 2.