

Charte d'utilisation des ressources des systèmes d'information et de communication

Mise à jour avril 2026

1.	Définitions	4
2.	Champ d'application de la charte	4
3.	L'accès aux ressources du SIC.....	5
4.	Règles de sécurité – protection des ressources et du SIC.....	6
5.	Modalités d'utilisation des moyens informatiques et de télécommunications	8
6.	Protection des ressources par l'utilisateur.....	12
7.	Accès aux dossiers, fichiers et courriels des utilisateurs et récupération du matériel mis à disposition.....	13
8.	Contrôle des activités.....	15
9.	Données à caractère personnel au sens de la loi.....	16
10.	Conservation et archivage	17
11.	Responsabilités et sanctions encourues en cas de non-respect de la charte.....	17
12.	Adoption de la charte et information des collaborateurs	18

Préambule

Les CCI de la région Auvergne-Rhône-Alpes mettent en œuvre un système d'information et de communication (SIC) nécessaire à leurs activités, comprenant notamment un réseau informatique et téléphonique.

Dans un but de transparence à l'égard des utilisateurs du SIC, d'incitation à un usage loyal, responsable et sécurisé du système d'information, la présente charte définit les règles relatives à l'utilisation de ces ressources, les droits et obligations de chacun en la matière. Elle constitue une règle de référence interne en cas de conflit.

Elle peut être complétée par des documents s'appliquant à des catégories particulières d'utilisateurs, telles les Administrateurs réseau et systèmes du personnel de la DSI, les étudiants ou les personnes suivant des formations dans les établissements gérés...

L'ensemble des données accessibles, fournies et exploitées via les outils et applications régionales et locales telles que la Gestion de la relation client (VITAE), les ERP Formation (Ammon et Ypareo), l'entrepôt de données régional (Datawarehouse), le FCU (Fichier consulaire unique), ERP Finance (XRP Ultimate SIFI), Gestion de notes de frais (Notilus), Gestion des temps (Kelio) constitue le patrimoine immatériel des CCI de la région Auvergne-Rhône-Alpes.

Chaque utilisateur doit veiller au respect de ce patrimoine et à la stricte confidentialité des données.

Les outils et applications régionales et locales dont il est question actuellement sont, et de façon non exhaustive :

- Les outils et portail web dont la webfactory,
- l'outil régional de gestion de la relation client (GRC) dénommé VITAE, et les outils associés (emailing, gestion des enquêtes, marketing digital ...),
- Les outils régionaux de gestion des centres de formations continues, qualifiantes et par apprentissage dénommés ERP Formation,
- l'outil de gestion des contrats d'apprentissage dénommé APPRENTIWEB utilisé par certaines CCI,
- l'outil régional de gestion des formalités et Fichier Consulaire Unique dénommé PIXI,
- les outils locaux de gestion des équipements gérés,
- l'outil régional de gestion des achats, de gestion comptable et de gestion budgétaire dénommé SIFI,
- L'ensemble d'outils nationaux RH : SIRH, Talentsoft
- L'entrepôt de données régional, et les outils d'analyse et de reporting associé,
- la plateforme régionale de gestion électronique de documents,
- les outils d'infrastructures techniques (communication unifiée, centre de contacts clients, ...).
- Les outils bureautiques et collaboratifs, et de visio (Teams...)
- Les applications d'Intelligence Artificielle ou outils utilisant l'IA

Cette liste non exhaustive, sera sujette à évolution en fonction de la mise en place des projets régionaux ou locaux.

1. Définitions

Sont désignés ci-après sous le terme :

- **CCI** : l'ensemble des CCI rattachées à la CCI de région Auvergne Rhône-Alpes et la CCI de région elle-même.
- **Utilisateur** : toutes personnes (élus, collaborateurs, stagiaires, alternants, intérimaires, apprenants des centres de formation, prestataires, visiteurs occasionnels...) ayant accès ou utilisant les ressources du système d'information mis à disposition par les CCI sur site ou à distance (cf. art. 2.A de la présente charte).
- **Administrateurs DSI** : les membres de la DSI, stagiaires y compris le cas échéant, chargés de la gestion du réseau, de l'enregistrement des utilisateurs, de l'affectation des droits d'accès ainsi que de la sécurisation des données.
- **Administrateurs d'application** : les utilisateurs ayant des droits avancés autres que ceux strictement nécessaires à l'utilisation basique d'un logiciel (exemple : gestion des droits des utilisateurs).
- **Données** : toutes informations gérées par une application informatique ou par un système d'infrastructures informatiques (ex : Téléphonie).
- **Données personnelles** : toutes informations relatives à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un ou plusieurs éléments qui lui sont propres.
- **DPO** : Data Protection Officer (délégué à la protection des données)
- **EDR** : Endpoint Detection and Response (logiciel de détection et de réponse à des cyber-attaques).
- **ERP** : Enterprise Ressource Planning (progiciel de gestion)
- **SIC** : Système d'Information et de Communication
- **MFA** : Multi Facteurs Authentification

2. Champ d'application de la charte

A. Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication des CCI de la région Auvergne-Rhône-Alpes, quel que soit leur statut :

- Le personnel, quelles que soient la durée et la nature de l'engagement (collaborateurs, stagiaires, alternants, intérimaires),
- Les élus,
- Les apprenants et stagiaires des centres de formation
- Les collaborateurs des associations hébergées, associations devant adhérer à la charte dans le cadre de leur convention d'occupation,
- Les clients des CCI qui sont locataires des locaux consulaires, qui dans le cadre de leur contrat souscrivent à un service DSI,
- Les employés de société prestataires, les visiteurs, qui auront été autorisés à utiliser le système d'information des CCI et qui auront été dûment informés du contenu de cette charte,
- Toute entité filialisée fera l'objet d'un protocole d'adhésion à cette charte dans le cadre de la mise en place d'une filialisation.

B. Système d'information et de communication

Il regroupe tous les moyens informatiques et de communications (logiciels, matériels, réseaux) utilisables depuis les locaux des CCI ou accessibles à distance, ainsi que les « services internet », c'est-à-dire la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses, notamment les outils de la gestion de la relation client, de la gestion de la formation, sites web, espaces collaboratifs, messageries classiques ou instantanées, forums de discussion, réseaux sociaux, etc.

Par extension, il comprend l'intégralité des données numériques stockées, traitées et échangées par ces installations.

Pour des raisons de sécurité, sera considéré comme faisant partie du SIC le matériel personnel des utilisateurs connecté au réseau de la CCI.

3. L'accès aux ressources du SIC

Le système d'information et de communication des CCI est et reste la propriété des CCI, hormis le matériel personnel de l'utilisateur dont ce dernier ferait usage sous réserve de l'accord de la DSI.

Ce système est mis à disposition des utilisateurs par la DSI pour l'exercice de leurs missions, conformément aux instructions de la hiérarchie, et son usage doit respecter les modalités définies par la présente charte.

A. Compte utilisateur et paramètres de connexion

L'accès aux ressources du SIC est subordonné à la création d'un compte utilisateur par la DSI. Ce compte est clôturé par la DSI dès :

- la date de sortie des effectifs du collaborateur,
- la date de fin de mission d'un prestataire,
- la date de fin de formation pour les apprenants,
- la fin de journée pour les visiteurs connectés au wifi...

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant et mot de passe) qui doivent obéir à certains critères de sécurité fixés par la DSI.

Ces paramètres sont strictement personnels à l'utilisateur. Ils doivent rester confidentiels et mémorisés par l'utilisateur. Ils ne doivent pas être transmis à des tiers ou stockés de façon non sécurisée dans ou hors du système d'information. Ils ne doivent pas reprendre des mots de passe de messagerie ou comptes web personnels.

Lorsqu'ils sont choisis par l'utilisateur, ces paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par la DSI afin d'appliquer les bonnes pratiques en la matière.

Ces recommandations sont également valables pour les paramètres de connexion aux applications métiers dont le compte utilisateur est créé par un Administrateur d'application et non par la DSI.

B. Les usages autorisés

L'utilisation des ressources du SIC, l'usage des services Internet et du réseau pour y accéder sont autorisés exclusivement dans le cadre de l'activité professionnelle des utilisateurs, conformément aux règles en vigueur.

Leur usage à des fins personnelles est toutefois toléré, dans un cadre " raisonnable " en quantité et en durée et qui n'affecte pas la sécurité des systèmes d'information ou la productivité du service.

4. Règles de sécurité – protection des ressources et du SIC

Les CCI mobilisent les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. À ce titre, il leur appartient de limiter les accès aux ressources sensibles et d'acquiescer les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

A. Administrateur SI et personnel de la DSI

Afin de conduire les actions quotidiennes d'administration et d'exploitation informatique afférentes à leurs missions (configuration, supervision, maintenance, évolution, support...), les Administrateurs réseau, systèmes et télécoms, et en général le personnel de la Direction des Systèmes d'Information, sont dotés de droits d'accès étendus sur les ressources du SIC placées sous leur responsabilité.

La DSI est responsable du contrôle du bon fonctionnement du système d'information et de communication et veille à l'application des règles de la présente charte. Les membres de la DSI sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître.

Les membres du personnel de la DSI sont tenus d'observer des prescriptions particulières de sauvegarde, de protection et d'intervention dans le cadre de la sécurité du réseau, des systèmes et des données. Ils ont donc signé une charte des Administrateurs réseau et systèmes du personnel de la DSI qui fixe les règles de déontologie qu'ils doivent impérativement respecter, en sus des droits et obligations indiqués dans la présente charte.

B. Devoirs de l'utilisateur du SIC

L'utilisateur est responsable des matériels et ressources qui lui sont confiés ou qu'il utilise dans le cadre de ses fonctions. Il doit concourir à leur sécurité et à leur protection en faisant preuve de prudence, de vigilance et de loyauté.

L'utilisateur prend toute précaution utile pour éviter ou limiter les risques de vol ou de perte des matériels ainsi que des ressources enregistrées sur ces matériels.

En cas de vol ou de perte, l'utilisateur doit informer sans délai la DSI.

En cas d'absence, même temporaire, de son bureau, il est impératif que l'utilisateur verrouille l'accès à son poste de travail.

Il est interdit à l'utilisateur d'installer ou de s'abonner à des logiciels sur le matériel mis à sa disposition, sans l'accord préalable de la DSI. Ladite installation sera réalisée par un membre de la DSI.

Il est de même interdit de copier ou installer des fichiers illégaux ou contraires à l'ordre public ou susceptibles de créer des risques d'insécurité pour le SIC.

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Cette copie de sauvegarde doit être effectuée par la personne habilitée à cette fin par la DSI.

Par ailleurs, l'utilisateur ne doit pas contourner les restrictions d'usage d'un logiciel, ni effectuer toute intervention technique de nature à modifier, détruire, altérer ou dégrader des biens, services et ressources du SIC ou nuire à leur bon fonctionnement.

Les fichiers, documents et bases réalisés par l'utilisateur dans le cadre de ses fonctions professionnelles doivent être enregistrés sur le système réseau appartenant à la CCI. En aucun cas, l'utilisateur ne doit pas effectuer d'enregistrements sur clé USB ou disque externe hors matériel fourni et pré-contrôlé par la DSI à usage exclusivement professionnel par l'utilisateur.

Chaque utilisateur veillera à supprimer ou archiver ses données devenues obsolètes, afin de ne pas surcharger le système réseau de la CCI.

L'accès par les utilisateurs aux informations et documents conservés sur le SIC doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.

Si dans l'accomplissement de ses missions, l'utilisateur est amené à constituer des fichiers comportant des données nominatives, il doit auparavant en informer le DPO afin de vérifier la conformité RGPD du traitement.

La création d'un dossier pour l'usage personnel de l'utilisateur est tolérée. La taille de ce dossier devra rester raisonnable et son intitulé devra être « Personnel et confidentiel + nom-prénom ». À défaut, le dossier sera considéré comme professionnel. Il est interdit à l'utilisateur de classer dans ce dossier des fichiers ou documents professionnels.

Tout stockage de données / fichiers illicites est prohibé qu'ils soient dans un dossier identifié comme « personnel et confidentiel » ou pas.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou susceptible de porter atteinte aux intérêts des CCI.

c. Obligations de l'utilisateur du SIC

Tout nouvel arrivant accèdera uniquement à son compte Microsoft et aux applications internes mais n'aura aucun accès internet tant qu'il n'aura pas suivi et validé les actions de sensibilisation au RGPD et à la Cybersécurité déployées par la CCI Auvergne-Rhône-Alpes.

L'utilisateur s'engage à suivre toute action de sensibilisation au RGPD et à la Cybersécurité déployée par la CCI Auvergne-Rhône-Alpes dans les délais indiqués. En cas de relance par

le DPO (Délégué à la Protection des données) ou le RSSI (Responsable Sécurité du Système d'Information), l'utilisateur devra se mobiliser et réaliser les suivis demandés.

5. Modalités d'utilisation des moyens informatiques et de télécommunications

A. Matériels et logiciels

La DSI met à disposition des utilisateurs, sur demande de leur responsable hiérarchique, les matériels, logiciels et applications nécessaires à l'exercice de leurs missions.

La mise à disposition de matériels nomades, notamment téléphonique, donne lieu à signature d'une feuille de remise à disposition de matériel par la DSI définissant les modalités d'utilisation du matériel.

Les utilisateurs peuvent, sous réserve de respecter les principes de cette charte et en fonction des habilitations qui leur auront été délivrées par la DSI sous la responsabilité de leur supérieur hiérarchique, se connecter à distance aux applications de la CCI à l'aide du matériel nomade fourni par la DSI ou à l'aide de leur matériel personnel. L'authentification multi-facteurs (MFA) est obligatoire pour tout accès VPN effectué depuis l'extérieur de nos sites.

Dans ce cas, il leur appartient de s'assurer de la sécurité du matériel utilisé ainsi que de la légalité et de la sécurité des logiciels installés sur ce matériel. La DSI se réserve le droit de refuser la connexion dudit matériel pour maintenir la sécurité du SIC. La DSI mettra à disposition des utilisateurs des guides de bonnes pratiques en la matière.

La solution anti-virus est installée systématiquement sur le matériel professionnel, PC comme smartphone professionnel et doit être installée sur tout smartphone personnel dès lors que la synchronisation de la messagerie professionnelle ou tout autre accès au SIC sont demandés.

Les logiciels sont installés sur les ordinateurs des CCI uniquement par l'équipe technique de la DSI.

Il est interdit en tant que collaborateur d'utiliser du matériel PC personnel dans les locaux de la CCI à des fins professionnelles. Par ailleurs, les accès à distance sont réduits en cas d'utilisation du matériel PC personnel (consultation mail uniquement).

Tous les matériels mis à disposition devront être restitués à la CCI en cas de départ définitif de l'utilisateur ou en cas de besoin lié à la continuité de services.

B. Espaces de stockage et sauvegarde des données

L'utilisateur dispose, pour l'exercice de son activité professionnelle, d'espaces de stockage alloués par la DSI. Il doit enregistrer régulièrement ses données et fichiers sur les espaces réseau (nominatif, de service ou collaboratif) mis à sa disposition et non sur son disque dur.

Seules les données enregistrées sur le réseau sont sauvegardées.

Il est demandé d'effectuer régulièrement un archivage ou une suppression des données devenues obsolètes.

Le stockage de données privées est toléré dans une limite raisonnable d'utilisation des ressources. Les dossiers privés doivent être intitulés « Personnel et confidentiel + nom-prénom ». En cas de manquement à ces règles, les données enregistrées sont présumées être à caractère professionnel et accessibles à l'employeur.

Il est rappelé qu'il est possible à l'employeur d'accéder à ce répertoire « Personnel et confidentiel + nom-prénom », en présence du titulaire du compte en cas de suspicion de données / fichiers illicites.

En cas de manque d'espace sur le réseau, les dossiers identifiés « Personnel et confidentiel + nom-prénom » pourront être supprimés par l'Administrateur réseau de la DSI, après information faite à l'utilisateur selon un délai convenu.

Lors de son départ définitif de la CCI, l'utilisateur doit supprimer son dossier « Personnel et confidentiel + nom-prénom » de son espace de stockage. A défaut, les données seront détruites par l'administrateur à la date de clôture du compte, dans le respect des règles de confidentialité.

C. Messagerie électronique

La DSI attribue à l'utilisateur, pour l'exercice de son activité professionnelle, une boîte à lettres professionnelle à laquelle est associée une adresse nominative de messagerie électronique.

Des boîtes aux lettres de service, accessibles à plusieurs utilisateurs, peuvent également être créées à la demande du responsable de service.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam et anti-robot. Les utilisateurs sont invités à informer la DSI des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

- Principes généraux d'utilisation de la messagerie

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il faut donc respecter un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de la CCI et/ou de l'utilisateur.

Avant tout envoi, il est impératif de vérifier l'identité et l'adresse électronique des destinataires du message et de leur qualité à recevoir communication des informations transmises.

En cas d'envoi à une liste de diffusion, l'utilisateur doit respecter les dispositions relatives à la lutte contre les spams. Il peut également dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires. Il doit également prévoir les modalités de désabonnement à cette liste de diffusion.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale.

La forme des messages professionnels doit respecter les règles définies par le service Communication et l'utilisation de sa signature professionnelle se faire conformément à la charte graphique en vigueur.

Enfin, les utilisateurs doivent régulièrement purger leur boîte mail des messages obsolètes ou sans intérêt.

- **Limites techniques**

La taille et le type des pièces jointes peuvent être limités par la DSI pour éviter l'engorgement du système de messagerie et assurer la bonne réception des messages par les messageries destinataires.

- **Utilisation personnelle de la messagerie**

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber le fonctionnement du SIC et de respecter les principes posés dans la présente charte.

Les utilisateurs s'engagent à ne pas communiquer notamment leur adresse courriel professionnelle aux sites d'achats non professionnels (vente-privée, Groupon ou autres vécépistes, ...) afin de ne pas saturer les ressources du SIC avec des sollicitations privées.

Les messages envoyés doivent être signalés par la mention "privé" ou "personnel" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé « Personnel et confidentiel + nom-prénom ». Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « Personnel et confidentiel + nom-prénom ». À défaut, les messages sont présumés être à caractère professionnel.

- **Echanges personnels avec les représentants du personnel et les délégués syndicaux**

Les collaborateurs échangeant des messages comportant des informations personnelles avec une institution représentative du personnel, devront signaler et classer de la même manière lesdits messages comme « Personnel et confidentiel + nom-prénom ».

Les membres du CSE (comité social et économique) et des commissions du CSE, les représentants de proximité ainsi que les titulaires d'un mandat syndical, devront archiver dans un répertoire clairement identifié (ex : Représentant du Personnel, CSE...) les messages envoyés ou reçus dans le cadre de leur mission. Ces répertoires seront alors également protégés par le régime de confidentialité des correspondances.

D. Téléphonie

L'usage des lignes téléphoniques, fixe ou mobile, mises à disposition des utilisateurs pour remplir leurs missions, est réservé aux besoins de l'activité professionnelle. Toutefois, un usage personnel raisonnable est toléré. Les SMS envoyés et reçus peuvent être consultés par l'employeur s'ils ne sont pas identifiés comme personnels (mention "privé" ou "personnel").

La comptabilisation des flux entrants et sortants permet d'imputer par service ou par poste les dépenses liées et éventuellement d'identifier une utilisation personnelle abusive.

E. Usage des services internet

Dans le cadre de leur activité professionnelle, les utilisateurs ont accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par la DSI. Celle-ci est habilitée à restreindre le téléchargement de certains fichiers.

Les utilisateurs doivent respecter strictement l'obligation de discrétion professionnelle et de neutralité du service public. Ils ne peuvent pas exprimer d'opinions personnelles susceptibles de porter préjudice aux CCI, à leurs collaborateurs ou leurs ressortissants.

Toute publication d'informations à caractère privé sur les sites internet ou intranet des CCI est interdite.

L'utilisation d'internet est réservée à l'activité professionnelle de l'utilisateur ; une utilisation à des fins privées est néanmoins tolérée dans les limites raisonnables, sous réserve que cet usage n'entrave en aucune façon l'accès professionnel et se fasse dans le respect de la législation en vigueur et celui de la présente charte.

En particulier :

- Il est interdit de se connecter à certains sites en raison de leur contenu contraire à l'ordre public et aux bonnes mœurs : les sites présentant toute forme d'apologie, les sites appelant à la haine raciale, les sites pornographiques et d'une manière générale tout site ne respectant pas la législation en vigueur,
- L'utilisateur ne doit pas utiliser ces services pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ou sans rapport avec ses missions.

Les utilisateurs peuvent être amenés, dans le cadre de leur activité professionnelle, à bénéficier d'accès à des bases de données via internet dont les abonnements ont été contractés auprès de fournisseurs d'informations par la CCI. Ils s'engagent à ne faire usage des données que pour leur seul besoin professionnel. Ils ne peuvent reproduire, diffuser ou céder tout ou partie desdites données au bénéfice d'un tiers, à titre gratuit ou onéreux, et ce quels que soient leurs rapports avec ce tiers.

Il en va de même de la publication et/ou de la diffusion d'informations à partir de données accessibles à l'utilisateur du fait de ses fonctions.

- **Services externes**

Internet propose de nombreux services pour faciliter le quotidien des utilisateurs (partage de fichiers, agenda partagé, espace de stockage en ligne, coffre-fort numérique...).

Pour des raisons de sécurité et de conformité, les utilisateurs doivent utiliser les services équivalents proposés par la DSI.

Les outils à proscrire sont notamment Ilovepdf, Googledocs, Wetransfert, GoogleDrive, Dropbox, la liste étant évolutive. Tout utilisateur rencontrant des difficultés doit contacter la DSI.

- **Médias sociaux**

Les médias sociaux (forum, blog, wiki, réseau social, service de partage...) sont des vecteurs de communication incontournables d'une stratégie de communication digitale au sein des entreprises et des CCI.

Les utilisateurs et animateurs de ces médias sociaux, qu'ils soient professionnels ou non, se doivent d'adopter un comportement loyal vis-à-vis du réseau des CCI. Il est rappelé qu'ils engagent sa réputation à chacune de leurs contributions sur ces médias et qu'ils se doivent de respecter la législation en vigueur.

Il est recommandé de mettre en œuvre une authentification multi-facteurs sur ces comptes d'accès aux réseaux sociaux pour limiter les usurpations d'identité.

F. Utilisation d'outils d'Intelligence Artificielle (IA)

Une charte spécifique dédiée à l'usage de l'IA est mise en place conjointement à cette charte.

Les employés doivent suivre préalablement une sensibilisation adéquate sur l'utilisation des systèmes d'IA afin de s'approprier les bonnes pratiques en matière d'IA, d'appréhender les risques associés à la perte de données professionnelles, d'avoir une bonne connaissance des règles et préconisations en matière de respect des données personnelles.

Chaque salarié utilisant des outils d'IA doit respecter les règles suivantes :

- **N'utiliser que les outils autorisés par la DSI.**
- **Réaliser un contrôle humain sur toute production de données issue de l'IA.**
- **Respecter les règles de la charte informatique relatives au droit de propriété intellectuelle des tiers et au RGPD, à la sécurité et habilitation à l'accès des données considérées comme sensibles ou confidentielles.**
- **Ne pas porter atteinte aux droits des personnes lorsque l'IA conduit à une prise de décision à leur encontre (ex : recrutement). En cas de doute, l'IA ne doit pas être utilisée.**
- **Ne pas utiliser des outils d'IA pour des finalités interdites par le RGPD et l'IA Act européen : extraction non ciblée d'images faciales sur internet ou par système de vidéosurveillance pour créer des bases de données de reconnaissance faciale, de reconnaissance des émotions sur les lieux de travail, de notation sociale.**

Par ailleurs, en cas d'utilisation d'IA « ouvert » (ex : abonnement Chat GPT), **il est interdit d'y injecter des données professionnelles, confidentielles ou non, ainsi que des données à caractère personnel**, ces systèmes d'IA étant susceptibles d'aspirer les données injectées en vue de l'accomplissement d'une tâche et donc susceptibles de porter atteinte au droit de la propriété intellectuelle, au secret des affaires et plus généralement à la confidentialité d'informations relatives aux CCI de notre région en les mettant à disposition d'autres utilisateurs d'IA.

6. Protection des ressources par l'utilisateur

A. Respect strict de la confidentialité

L'utilisateur veille au respect de la confidentialité des informations en sa possession, notamment les informations qui figurent dans l'outil de la gestion de la relation client et autres systèmes connectés tels que ceux listés précédemment et toutes les autres applications régionales et locales.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes d'information doit être limité à ceux qui leur sont propres et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par

d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Cette règle s'applique également aux conversations privées de type courrier électronique ou messagerie instantanée professionnelle dont l'utilisateur n'est destinataire ni directement, ni en copie.

B. Respect de la réglementation

L'utilisateur doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, le respect de la vie privée, la sécurité et la confidentialité des données personnelles, le secret des affaires, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables.

C. Obligation d'information

L'utilisateur doit signaler sans délai à la DSI tout dysfonctionnement ou anomalie ainsi que toute intrusion ou tentative d'intrusion dans le SIC dont il aurait connaissance.

7. Accès aux dossiers, fichiers et courriels des utilisateurs et récupération du matériel mis à disposition

Sauf s'ils portent la mention « Personnel et confidentiel + nom-prénom », dans les conditions exposées ci-avant dans la présente charte, les dossiers et fichiers créés par l'utilisateur sont présumés avoir un caractère professionnel. En conséquence, l'employeur peut y accéder hors la présence de l'utilisateur.

En ce qui concerne les seuls dossiers identifiés par la mention « Personnel et confidentiel + nom-prénom », l'employeur ne peut y avoir accès qu'en présence de l'utilisateur et sous réserve d'une suspicion de fichiers / données illicites.

A. En cas d'absence imprévue

La procédure d'accès à la messagerie et aux serveurs fichiers peut être déclenchée, à la demande d'un supérieur hiérarchique, sans condition de durée, en cas d'absence imprévue (notamment maladie, accident, événement personnel...) lorsqu'un besoin professionnel réel et documenté le justifie (ex. client bloqué, échéance contractuelle, dossier critique).

Pour assurer une continuité dans l'activité professionnelle, l'administrateur DSI peut, à la demande d'un supérieur hiérarchique, avec une argumentation détaillée du besoin et pour la durée de l'absence uniquement :

- rediriger la boîte de réception du collaborateur absent vers celle de son supérieur hiérarchique ou de toute autre personne du service désignée,
- donner un accès complet à la messagerie du collaborateur absent, au supérieur hiérarchique après validation de la DRH (hors dossier « Personnel et confidentiel + nom-prénom », afin que cette personne puisse consulter les mails en cours et prendre connaissance de leur contenu pour le bon fonctionnement du service.

De même, l'administrateur DSI peut donner accès aux répertoires réseau du collaborateur absent à son responsable hiérarchique ou de toute autre personne désignée du service

après validation de la DRH et hors dossier « Personnel et confidentiel + nom-prénom », si le partage de dossiers ou fichiers n'a pas été précédemment prévu par le service. Le hiérarchique ou la personne habilitée se connectera ainsi avec ses propres identifiants pour accéder au répertoire de l'utilisateur absent, ce dernier ne devant en aucun cas communiquer ses identifiants (cf. § 3.A).

B. En cas d'absence prolongée de l'utilisateur

Une absence prolongée concerne une absence supérieure à 30 jours calendaires, absence liée à une suspension du contrat de travail et hors Congés Payés.

Pour assurer une continuité dans l'activité professionnelle, l'administrateur DSI peut, à la demande d'un supérieur hiérarchique et pour la durée de l'absence uniquement :

- rediriger la boîte de réception du collaborateur absent vers celle de son supérieur hiérarchique ou de toute autre personne du service désignée,
- donner un accès complet à la messagerie du collaborateur absent, au supérieur hiérarchique après validation de la DRH (hors dossier « Personnel et confidentiel + nom-prénom », afin que cette personne puisse consulter les mails en cours et prendre connaissance de leur contenu pour le bon fonctionnement du service.

De même, l'administrateur DSI peut donner accès aux répertoires réseau du collaborateur absent à son responsable hiérarchique ou de toute autre personne désignée du service après validation de la DRH et hors dossier « Personnel et confidentiel + nom-prénom », si le partage de dossiers ou fichiers n'a pas été précédemment prévu par le service. Le hiérarchique ou la personne habilitée se connectera ainsi avec ses propres identifiants pour accéder au répertoire de l'utilisateur absent, ce dernier ne devant en aucun cas communiquer ses identifiants (cf. § 3.A).

Cette procédure ne concerne pas les dossiers identifiés comme « Personnel et confidentiel + nom-prénom » dont l'accès est réservé à leur seul propriétaire.

Pour les absences d'une durée supérieure à 30 jours calendaires, les accès aux outils hors YR4YOU, à la messagerie et à la téléphonie sont suspendus. A titre dérogatoire, sur demande du collaborateur, les accès à la messagerie, à la téléphonie et aux outils pourront être conservés sous réserve d'une double validation supérieur hiérarchique et RH. Au retour effectif du collaborateur, ses accès seront réactivés.

L'utilisateur concerné est informé de ces actions au travers de cette charte.

C. En cas de départ définitif de l'utilisateur de la CCI

Toute sortie définitive fait l'objet d'un processus de sortie dans GLPI, initié par le référent RH de la CCI d'appartenance et complété par le chef de service qui doit indiquer les données à conserver et à transférer et la durée de conservation de la boîte mail si elle est supérieure à 3 mois.

L'utilisateur doit avant son départ :

- Supprimer son dossier « Personnel et confidentiel + nom-prénom » de sa messagerie et de son répertoire réseau,
- Transférer les messages professionnels à son supérieur hiérarchique ou à la personne remplaçante qui pourra prendre connaissance de leur contenu,
- Veiller à ce que tous les fichiers professionnels soient enregistrés sur le réseau et accessibles à son responsable hiérarchique.

Le compte de l'utilisateur est clôturé par la DSI le lendemain de son départ quel qu'en soit le motif, ou le lendemain du début de la dispense de son préavis ou de la dispense de service le cas échéant, et à tout le moins dans le mois qui suit son départ.

Les messages personnels qui n'auraient pas été supprimés sont détruits par l'administrateur dans le respect des règles de confidentialité.

D. Droit à la déconnexion

Le droit à la déconnexion est le droit pour chaque salarié de ne pas être sollicité par son employeur en dehors de ses heures de travail (dont les congés). Ce droit vise à garantir un équilibre entre vie professionnelle et vie personnelle et à prévenir les risques liés au surmenage.

Le droit à la déconnexion s'applique à tous les collaborateurs de l'entreprise, quel que soit leur statut ou leur poste. Il concerne l'ensemble des outils numériques mis à disposition par l'entreprise, tels que les téléphones portables, les ordinateurs, les tablettes et les messageries électroniques.

La note de service DSI - *Réduction de la surface d'attaque du SI du réseau régional consulaire* du 6 novembre 2025 rappelle les restrictions des accès au SI en conformité avec le droit à la déconnexion.

8. Contrôle des activités

A. Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux (" logs "), créés automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les serveurs et permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de la CCI, en détectant des erreurs matérielles ou logicielles et en enregistrant les accès au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de vérifier le bon fonctionnement du système d'information et de communication, pour détecter les anomalies liées à l'utilisation des ressources et surveiller les tentatives d'intrusion, ce dans le respect des règles en vigueur.

Sont notamment conservées et peuvent faire l'objet de statistiques anonymisées les données relatives :

- à l'utilisation des logiciels applicatifs et notamment les outils de gestion de la relation client (GRC et outils connectés), de gestion de la Formation et de gestion du Fichier Consulaire,
- à l'utilisation des ressources situées sur internet,
- aux connexions aux réseaux internes et à la messagerie,
- à l'utilisation du téléphone.

B. Procédure de contrôle manuel

En cas de dysfonctionnement constaté par la DSI, l'administrateur, dans le respect de la confidentialité peut procéder à un contrôle manuel et à une vérification de toute opération

effectuée par un ou plusieurs utilisateurs. C'est le cas notamment de toute opération détectée à risque par notre outil de cybersécurité, l'EDR.

Le contenu des messages privés (tels que définis à l'article 5.3) ne peut en aucun cas être contrôlé par l'administrateur.

Toutefois, lorsque le contrôle est effectué dans le cadre d'une suspicion de fichiers / données illicites, l'administrateur peut ouvrir les fichiers identifiés comme « Personnel et confidentiel + nom-prénom » en présence du collaborateur.

9. Données à caractère personnel au sens de la loi

Pour assurer leurs différentes missions, les CCI sont amenées à collecter et traiter de nombreuses données, économiques, confidentielles ou personnelles, concernant les entreprises, les partenaires, prestataires ainsi que les employés de ces entreprises, notamment dans l'outil de gestion de la relation client et autres applications régionales et locales.

Ces données visent à mieux connaître les entreprises de la région, structurer et faciliter les actions à destination de nos clients et à la promotion des services consulaires ainsi que leur suivi dans le temps. Certaines applications, comme la GRC (gestion de la relation client) ou la gestion de la formation, sont alimentées par des contributions des collaborateurs de la CCI (utilisateur) dans un objectif de qualité, de sécurité et de vérification des informations publiées.

Chaque utilisateur est tenu pour responsable des informations qu'il saisit dans ces applications, notamment la GRC, et s'engage, pour les données à caractère personnel, à respecter de façon stricte le RGPD (Règlement Général sur la Protection des Données).

L'utilisateur sera notamment vigilant lorsqu'il complète une zone de commentaires :

- Il aura toujours à l'esprit que la personne concernée peut, à tout moment, exercer son droit d'accès à lire ces commentaires,
- Il sera objectif, jamais excessif ou insultant, inscrira des mentions neutres et factuelles en lien avec des opportunités d'affaires,
- Il sera vigilant quant aux données sensibles visées par l'article 9 du RGPD : données relatives à la santé, ou à la vie sexuelle des personnes. Ces informations ne peuvent être, sauf exceptions, renseignées qu'avec le consentement exprès des personnes et accessibles uniquement aux personnes en charge du programme pour lequel ces données sont collectées.

L'utilisateur est informé que la CCI pourra recourir à des outils informatiques vérifiant les mots contenus dans ces zones de commentaires ou réaliser des extractions des commentaires pour s'assurer du respect du RGPD.

Ces données sont utilisées par les différents services des CCI dans le cadre de leurs missions respectives, en fonction des habilitations qui leur sont attribuées.

Les traitements de données ainsi réalisés peuvent être imposés par les textes, tels ceux relatifs à la tenue de bases économiques, à l'enregistrement de contrats d'apprentissage, au suivi de la scolarité des étudiants..., ou créés dans le cadre de dispositifs mis en œuvre pour répondre aux besoins des ressortissants, ou encore sont nécessaires au fonctionnement des CCI.

Le RGPD pose les principes de la protection des données à caractère personnel. On entend par donnée à caractère personnel toute donnée permettant d'identifier une personne physique, directement ou indirectement.

Tous les traitements de données à caractère personnel doivent être, au préalable, inscrits au registre des traitements de la CCI, l'ensemble des registres étant tenu par le DPO.

L'utilisateur se doit de :

- communiquer aux personnes les finalités et destinations des informations enregistrées et leur durée de conservation,
- utiliser les données à caractère personnel uniquement pour les strictes finalités pour lesquelles elles sont collectées,
- garantir aux personnes un droit d'accès et de rectification des données nominatives les concernant,
- ne pas collecter d'informations concernant les croyances, idéologies, appartenances politiques, raciales ou ethniques, mœurs sexuelles et données de santé.

De la même façon, l'utilisateur est informé des données nominatives le concernant enregistrées dans les traitements internes de la CCI.

Le transfert de données à caractère personnel en dehors de l'Union européenne est encadré par le RGPD.

10. Conservation et archivage

La conservation et l'archivage des données, fichiers et courriels peuvent être soumis à des obligations imposées par différentes réglementations, notamment, réglementation fiscale et sociale, RGPD, loi du 17 juillet 1978 sur l'accès aux documents administratifs, code du patrimoine imposant l'archivage des documents administratifs.

Les collaborateurs doivent gérer leurs ressources, procéder à leur suppression, conservation et/ou archivage en conformité avec la loi et les procédures mises en place dans ce but par la CCIR et les CCI rattachées. Cette gestion concerne également les documents papiers (ex : CV) ainsi que les fichiers de travail contenant des données personnelles.

11. Responsabilités et sanctions encourues en cas de non-respect de la charte

Chaque visiteur individuel est sous la responsabilité du collaborateur le recevant : ce visiteur n'accèdera au wifi visiteur qu'après validation du collaborateur CCI et ne doit en aucun cas se connecter en mode filaire.

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés.

12. Adoption de la charte et information des collaborateurs

- Entrée en vigueur de la charte

Conformément à l'article 6.2.4.2 du statut du personnel administratif des CCI, le projet de charte d'utilisation des ressources des systèmes d'information et de communication a été soumis pour avis à la réunion de CSE du 02 avril 2026 après information préalable le 03 mars 2026. Elle a également été validée en bureau CCIR du 25 février 2026.

La charte entre en vigueur à compter de sa diffusion par le Directeur Général de la CCI de région Auvergne-Rhône-Alpes. Elle sera communiquée aux collaborateurs par message électronique adressé à chacun d'eux et publié sur le site intranet régional dans l'onglet RH.

- Consultation de la charte

La présente charte est consultable sur l'intranet régional.

La DSI est à la disposition des collaborateurs pour leur fournir toute information concernant l'utilisation des systèmes d'information. Elle informe les utilisateurs régulièrement sur l'évolution des systèmes d'information et sur les menaces susceptibles de peser sur leur sécurité.

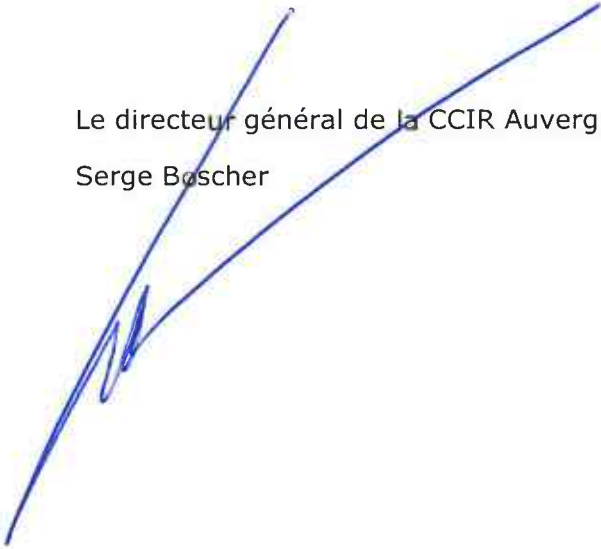
Des opérations de communication internes sont organisées, de manière régulière, afin d'informer les collaborateurs sur les pratiques d'utilisation des systèmes d'information.

- Evolution de la charte

La présente charte annule et remplace la charte relative à l'utilisation des systèmes d'information et de communication du 16 octobre 2024 pour les CCI d'Auvergne-Rhône-Alpes.

Les règles fixées par la charte pourront être modifiées pour tenir compte des évolutions légales, réglementaires et technologiques. Toute modification interviendra dans les mêmes conditions que lors de l'adoption de la charte.

Conformément aux dispositions du Code du travail, cette charte est considérée comme une adjonction au règlement intérieur de la CCIR et s'impose à tous les collaborateurs.



Le directeur général de la CCIR Auvergne-Rhône-Alpes
Serge Boscher