le cnam

Charte de bon usage des moyens informatiques

juin 2026

1 Préambule

Le bon fonctionnement du système d'information (cf. Glossaire) s'inscrit dans le respect des lois et règlements en vigueur, notamment ceux relatifs à la protection des données, à la propriété intellectuelle et à la cybersécurité.

Cette charte n'a pas vocation à prévoir de manière exhaustive toutes les situations possibles. Elle définit des principes généraux d'utilisation, qui serviront de référence pour guider chaque utilisateur dans les cas non explicitement abordés.

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent au Cnam, ainsi qu'à l'ensemble des utilisateurs :

- personnels ou assimilés de l'établissement concourant aux missions de l'établissement ;
- auditeurs, anciens auditeurs ;
- personnes n'entrant pas dans les deux catégories ci-dessus, dont la désignation et le besoin d'accès sont garantis par un personnel de l'établissement dans le respect de la présente charte ;
- visiteurs (lors de conférences ou d'évènements scientifiques ou culturels ayant lieu dans les murs).

Cette charte, intégrée au règlement intérieur de l'établissement (cf. Glossaire), a pour but :

- d'informer tout utilisateur de ses droits et devoirs en matière d'accès et d'utilisation au système d'information de l'établissement ;

– de porter à la connaissance de chaque utilisateur les moyens utilisés par l'établissement pour assurer le contrôle de l'accès et de l'utilisation du système d'information.

Elle n'a pas pour but :

– de réécrire les lois qui s'appliquent à chacun
– de produire des recommandations ou guide d'usage de chaque outil informatiques ou numérique.

1.1 *Les engagements du Cnam*

Le Cnam facilite l'accès des utilisateurs aux ressources du système d'information.

Les ressources sont destinées aux activités professionnelles en lien avec les missions de l'établissement et le Cnam respecte la vie privée de chaque utilisateur dans les conditions définies dans cette charte.

Le Cnam met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information sous la responsabilité du RSSI (Responsable de la Sécurité du Système d'Information - Cf. Glossaire) désigné par l'établissement, suivant l'Instruction Générale Interministérielle n° 1337. (Cf. Références Légales).

1.2 *Les obligations de l'utilisateur*

Chaque utilisateur respecte cette charte et contribue au bon fonctionnement, à la sécurité et à l'intégrité des ressources informatiques, dans un esprit de respect mutuel et de responsabilité collective.

L'utilisateur est responsable en tout lieu et en tout temps de l'usage qu'il fait du système d'information.

2 Législation et textes en vigueur

2.1 Protection des données à caractère personnel

Le Cnam est soumis au respect des dispositions du RGPD (Règlement Général sur la Protection des Données - cf. Glossaire), qui définissent les conditions dans lesquelles un traitement des données à caractère personnel est licite (art. 6 du RGPD), sous réserve d'adaptations par la loi française.

Il est « responsable du traitement » des données et ses obligations sont définies, à ce titre, par les articles 24 et s. du RGPD.

À ce titre, l'établissement a désigné un DPO (Délégué à la protection des données ou *Data protection officer*) en charge de la protection des données à caractère personnel.

Les créations ou modifications de fichiers comprenant des données à caractère personnel et demandes de traitements afférents, y compris lorsqu'elles résultent de croisement ou d'interconnexion de fichiers préexistants, doivent préalablement être déclarées auprès du DPO du Cnam établissement public.

L'utilisateur a l'obligation d'alerter le DPO et le RSSI s'il constate une atteinte à la protection des données à caractère personnel.

Les mentions relatives à la protection des données à caractère personnel sont publiées sur un site dédié cité en annexe (cf. Sites utiles et contacts).

2.2 Respect de la vie privée

Le droit à la vie privée est régi par l'article 9 du Code civil. Le droit à l'image en découle. Il en résulte qu'aucune image ou information relative à la vie privée d'autrui ne peut être communiquée sans le consentement de la personne intéressée.

2.3 Respect de la propriété intellectuelle

Le droit de la propriété intellectuelle s'applique à l'utilisation des ressources informatiques ou numériques. En conséquence, chaque utilisateur doit notamment :

- utiliser les logiciels et ressources dans le strict respect des licences souscrites ;
- s'abstenir de reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation explicite des ayant droits.

2.4 Principe de responsabilité, accès illégitimes

Les utilisateurs sont soumis à des obligations générales, telles que la confidentialité, la discrétion et la vigilance dans le cadre de leur utilisation des moyens informatiques mis à leur disposition. En conséquence :

- les informations personnelles des usagers ne peuvent être utilisées ou diffusées, que dans le cadre de l'accomplissement des missions du Cnam ;

– les informations de toute nature auxquelles un utilisateur a accès par inadvertance ou de façon illégitime, ne doivent pas être consultées, copiées, diffusées ou modifiées, étant précisé que dans cette hypothèse l'utilisateur doit prévenir, dès que possible le RSSI (Cf. Sites utiles et contacts).

Outre les obligations générales précitées, et conformément aux dispositions du Code général de la fonction publique, les enseignants, chercheurs et personnels administratifs du Cnam sont soumis, en leur qualité d'agents publics de l'État, aux devoirs de réserve, de loyauté et de neutralité, ainsi qu'à une obligation de discrétion professionnelle.

3 Conditions d'utilisation du système d'information

Chaque utilisateur dispose d'accès individuels (nom d'utilisateur, mot de passe, etc.) au système d'information. Ces accès sont attribués suivant la situation de l'utilisateur. Ils sont individuels, confidentiels et incessibles. Ils sont temporaires et sont modifiés ou supprimés en cas de changement de situation. Les ressources fournies sont susceptibles d'être soumises à des quotas d'utilisation.

Les différents accès proposés découlant des changements de situation sont définis de façon détaillée et sont disponibles sur le site de la DSI (cf. Sites utiles et contacts). En cas de changement ou de clôture d'accès, la Direction des Systèmes d'Information s'engage à informer l'utilisateur sur sa messagerie Cnam et sur sa messagerie personnelle (si elle est connue). Ces courriels incluent systématiquement un moyen de contact.

3.1 Cas d'utilisation du système d'information

3.1.1 *Utilisation dans le cadre des missions du Cnam*

Le Cnam met à disposition des outils et ressources numériques pour la réalisation des missions qui lui incombent.

Dans ce cadre, les utilisateurs s'engagent à utiliser les outils et ressources mis à disposition par le Cnam dans la mesure où ils offrent les mêmes fonctionnalités qu'un outil externe qui pourrait comporter des risques pour le système d'information, des surcoûts pour l'établissement ou des difficultés de continuité d'activité.

Sauf mention explicite, toute information présente au sein du système d'information appartient à l'établissement, qui pourra en disposer, notamment à des fins de continuité d'activité.

Le matériel individuel mis à disposition de l'utilisateur par le Cnam reste la propriété de l'établissement. L'utilisation d'autres équipements ne doit pas remettre en cause la sécurité des données et du système d'information et engage la responsabilité de l'utilisateur.

3.1.2 *Utilisation résiduelle à titre privé*

L'utilisation à des fins privées du système d'information doit respecter les conditions suivantes :

- non lucrative et raisonnable : l'utilisation privée doit être ponctuelle, non commerciale et ne doit pas entraîner de coûts supplémentaires pour l'établissement ;
- respect des missions professionnelles et pédagogiques : l'utilisation privée ne doit en aucun cas nuire à la réalisation des missions du Cnam.

Sauf mention explicite précisant le caractère privé des données, ces dernières sont réputées appartenir à l'établissement qui pourra en disposer et les supprimer, notamment lors de départs ou changement de situation des utilisateurs. L'utilisateur est responsable de la sauvegarde régulière de ses données privées et de leur récupération lors de son départ et des fermetures de service.

3.1.3 *Utilisateurs à privilèges, administrateurs*

L'accès privilégié octroyé dans le cadre de fonctions, telles que responsable de ressources ou administrateur, entraine une responsabilité et exige une rigueur accrue dans son utilisation.

L'accès à des informations sensibles implique un respect renforcé des mesures de sécurité et des protocoles de confidentialité. Ces utilisateurs s'abstiendront d'abuser de leurs privilèges, en limitant les accès aux seules personnes autorisées et en faisant un usage des données accédées conformes à leur mission.

Dans le cadre de fonctions d'administration de composant du système d'information, ces utilisateurs s'engagent à respecter les directives du RSSI, et à se tenir à jour des compétences techniques nécessaires.

3.1.4 *Personnels de ZRR*

Certaines équipes du Cnam travaillant sur des sujets jugés sensibles par les tutelles institutionnelles, peuvent héberger en leur sein des ZRR (zones à régime restrictif). Cette classification a des impacts importants sur l'utilisation du système d'information. Dans ce cas, des règles spécifiques s'appliquent à l'ensemble des utilisateurs et équipements concernés, règles consignées dans une PSSI (Politique de Sécurité des Systèmes d'Information) dédiée.

3.1.5 *Usages relevant de l'activité syndicale*

Les usages relevant de l'activité des organisations syndicales sont régis par une charte spécifique. (Charte sur l'usage des réseaux informatiques par les organisations syndicales du Conservatoire national des arts et métiers intégrée à l'annexe "Chartes informatiques" du Règlement intérieur).

3.2 Continuité de service, gestion des départs et absences

Afin d'assurer une continuité de service lors des départs et absences de personnels et de protéger les données de l'établissement, la DSI recommande l'usage d'espaces partagés et d'adresses génériques. Ces sujets incombent aux responsables de services.

Les changements de situation des utilisateurs, notamment le départ définitif, entrainent des changements sur les accès aux ressources numériques et potentiellement la suppression des données rattachées à son compte individuel. Le détail de ces actions est disponible sur le site de la DSI (cf. Sites utiles et contacts).

En cas de décès d'un utilisateur ou d'absence sans préavis sans possibilité de le joindre, la DSI sur demande de la direction de l'établissement pourra accéder aux données de l'utilisateur afin de transmettre les éléments nécessaires à la continuité de service. Ces accès se déroulent en présence d'au moins deux témoins, dont le RSSI ou le DPO, qui garantissent la procédure et le respect des données privées.

4 Mesures de sécurité

Tout utilisateur se tient informé et respecte les consignes de sécurité données par le RSSI sur son site (cf. Sites utiles et contacts) et notamment :

- garde strictement confidentiels son (ou ses) codes d'accès personnels et ne les divulgue pas à un tiers,
- respecte la gestion des accès, en particulier n'utilise pas les codes d'accès d'un autre utilisateur, ni cherche à les connaître,
- ne détourne pas de leur usage premier les outils et applications, ni les données mis à leur disposition.

Par ailleurs, les équipes en charge du système d'information de l'établissement veillent à ce que les ressources ne soient accessibles qu'aux personnes habilitées.

4.1 Adresses de messagerie

L'utilisation d'adresses de messagerie non institutionnelles est proscrite dans le cadre des missions du Cnam, afin de limiter les risques d'usurpation et de fuites de données.

4.2 Mesures de contrôle

Le Cnam met en œuvre les mécanismes de protection appropriés sur le système d'information mis à la disposition des utilisateurs.

L'utilisateur est informé que :

- pour effectuer la maintenance corrective, curative ou évolutive, le Cnam se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- toute donnée bloquante pour le système d'information ou générant une difficulté technique est susceptible d'être isolée voire supprimée ;
- le Cnam supervise le système d'information et, conformément à ses obligations légales, met en place un système de journalisation des accès aux ressources informatiques, incluant les accès Internet ;
- le Cnam se réserve le droit de limiter les accès (par exemple en cas de trafic trop important ou de risque pour la sécurité de l'établissement).

4.3 Devoirs de signalement

L'utilisateur doit avertir le RSSI (cf. Sites utiles et contacts) dans les meilleurs délais s'il soupçonne une utilisation frauduleuse d'une ressource numérique et plus généralement tout dysfonctionnement ou anomalie qu'il constaterait sur le système d'information (telle qu'une usurpation, une intrusion ou une habilitation anormale).

4.4 Sanctions

En cas de manquement aux règles définies dans la présente charte, l'établissement pourra décider de limiter les habilitations données, voire supprimer totalement l'accès aux ressources informatiques du contrevenant.

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins autres que les missions de l'établissement est susceptible de donner lieu à des sanctions disciplinaires.

Tout manquement aux obligations légales et réglementaires est susceptible de poursuites judiciaires.

5 Sites utiles et contacts

- le DPO (délégué à la protection des données) est joignable à l'adresse : ep_dpo@lecnam.net ; il présente les grandes lignes de son action sur le site : https://info-rgpd.cnam.fr/ ;
- le RSSI (responsable de la sécurité du système d'information) est joignable à l'adresse : rssi@cnam.fr ; il présente les règles applicables et recommandations d'usage sur le site : https://securite-informatique.cnam.fr/ ;
- les services de la DSI détaillent les outils et leurs usages sur le site : https://assistancedsi.cnam.fr détaillant les outils et les manières de les utiliser.

5.1 Glossaire

5.1.1 Établissement

Par « établissement », il faut entendre tout service et/ou composante du Cnam établissement public : administration centrale, équipes pédagogiques, laboratoires, musée, etc. telles que définies dans le règlement intérieur.

5.1.2 Système d'information

L'expression « système d'information » désigne généralement l'ensemble des ressources matérielles, immatérielles et humaines pour manipuler des informations (collecte, stockage, modification, distribution, consultation…). Il se décompose alors en deux parties : une partie technique (équipements clients et serveurs, équipements de communication intermédiaires mais aussi logiciels, données…) et une partie sociale (structure organisationnelle, processus…). Ainsi, dans cette acception les utilisateurs et leurs équipements font partie intégrante du système d'information, de même que les procédures afférentes aux traitements.

Dans cette charte, nous appelons « système d'information » la partie technique *i.e.* l'ensemble des ressources matérielles et immatérielles, en incluant les processus.

5.1.3 Utilisateur du système d'information

Le terme d'utilisateur recouvre toute personne ayant accès aux ressources du système d'information quel que soit son statut. Il s'agit notamment :

- des personnels ou assimilés de l'établissement concourant aux missions de l'établissement,

– des auditeurs, anciens auditeurs,
– des personnes n'entrant pas dans les deux catégories ci-dessus, dont la désignation et le besoin d'accès sont garantis par un personnel de l'établissement dans le respect de la présente charte,
– des visiteurs (lors de conférences ou d'évènements scientifiques ou culturels ayant lieu dans les murs).

5.1.4 Données et informations

Les deux termes sont utilisés indifféremment.

5.1.5 Données à caractère personnel

Les données à caractère personnel sont des informations qui permettent l'identification des personnes physiques auxquelles elles se rapportent, directement ou indirectement, et à partir d'une seule donnée ou à partir du croisement d'un ensemble de données.

5.1.6 Données sensibles

L'acception retenue dans cette charte recouvre indistinctement les deux définitions suivantes :

– le terme est défini par la Cnil et recouvre une catégorie de données à caractère personnel révélant ou contenant l'origine ethnique ou raciale, les opinions ou croyances, l'appartenance syndicale, les données biométriques, génétiques ou médicales, l'orientation sexuelle ;
– l'instruction interministérielle n° 901 (cf. Références légales) quant à elle, définit comme informations sensibles celles portant la mention Diffusion Restreinte, Restreint OTAN, Restreint UE et toute information dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs de l'établissement et ce, au regard de la protection du patrimoine scientifique et technique de la nation.

5.1.7 RSSI

Le RSSI est responsable du la sécurité du système d'information tel que défini ci-dessous, au Cnam il dispose de suppléants. Dans cette charte, le terme RSSI signifie le RSSI ou l'un de ses suppléants.

6 Références légales

Les textes en vigueur dans le domaine de la sécurité des systèmes d'information sont notamment les suivants :

- Code de la propriété intellectuelle, notamment les articles L. 335-1 à L. 335-10 [1]
- Code des relations entre le public et l'administration [2] ;
- Code pénal (notamment ses articles 226-1 à 226-7 [3] relatifs aux atteintes à la vie privée, 226-8 à 226-9 [4] relatifs aux atteintes à la représentation de la personne, 226-15 et 432-9 relatif aux atteintes au secret des correspondances, 227-23 [5] relatif à la diffusion, fixation, enregistrement et transmission d'images ou de représentation à caractère pédopornographique et consultation de sites à contenus pédopornographique, 227-24 [6] relatif à la fabrication, transport, diffusion et commerce de message à caractère violent, incitant au terrorisme, à la pornographie ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, 323-1 à 323-7 [7] relatifs aux atteintes aux systèmes de traitement automatisé de données, R. 621-1 et R. 621-2 [8] relatifs à la diffamation et à l'injure non publiques, R. 624-2 relatif à la diffusion de messages contraires à la décence, R. 625-7 à R. 625-8-2 [9] relatifs aux provocations, diffamations et injures non publiques présentant un caractère raciste ou discriminatoire, R. 625-10 à R. 625-13 [10] relatifs aux atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques) ;
- **Code général de la fonction publique, articles L121.6 et L121.7 [11] (secret professionnel et devoir de protection des données professionnelles par les agents de la fonction publique) ;**
-
- Code civil [12] ;
- loi du 29 juillet 1881 sur la liberté de la presse [13] ;
- loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (dite « Loi Informatique & Libertés ») [14] ;

1. https://www.legifrance.gouv.fr/codes/id/LEGIARTI000021212160/2009-11-01
2. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000031366350/
3. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165309/
4. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165310/
5. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043409170
6. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044394218/2026-05-29
7. https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006149839
8. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165410/#LEGISCTA000006165410
9. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165460/2026-05-29
10. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038607906/2026-05-29
11. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000044416551/LEGISCTA000044420673/#LEGISCTA000044427915
12. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070721/
13. https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722
14. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/2026-05-29

- **règlement UE 201**6/679 en date du 27 avril 2016, (dit « RGPD ») [15] ;
- loi n° 82-652 du 29 juillet 1982 modifiée sur la communication audiovisuelle (article 93-2 et suivants) [16] ;
- loi n° 86-1067 du 30 septembre 1986 modifiée relative à la liberté de communication [17];
- loi n° 94-665 du 4 août 1994 relative à l'emploi de la langue française [18] ;
- instruction interministérielle n° 901 en date du 28 janvier 2015 (protection du patrimoine scientifique et technique de la nation, données sensibles) [19];
- Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics [20];
- référentiel général de sécurité, version 2.0 en date du 13 juin 2024 [21] ;
- loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique (dite « LCEN ») [22] ;
- décret n° 2019-768 du 24 juillet 2019 pris en application de l'article 47 de la loi n° 2005-102 du 11 février 2005 modifiée pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées et créant un référentiel d'accessibilité des services de communication publique en ligne [23].

15. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
16. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000880222/2026-05-29
17. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000512205/2026-05-29
18. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000349929/2026-05-29
19. https://www.legifrance.gouv.fr/circulaire/id/39217
20. https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/protection-du-service-numerique-de-letat/
21. https://cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/referentiel-general-de-securite/documents-referentiel-general-de-securite/
22. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/2026-05-29
23. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038811937/2026-05-29