Charte d’utilisation du système d'Information du CINES

Ministère de l’Enseignement Supérieur et de la Recherche
CENTRE INFORMATIQUE NATIONAL DE L'ENSEIGNEMENT SUPERIEUR
950 rue de Saint-Priest – 34097 Montpellier cedex 5 – FRANCE
Tél. 04 67 14 14 14 - https://www.cines.fr

TABLE DES MATIERES

Table des matières

Table des matières 2
Table des matières 2
1.1 Contexte stratégique et engagement de la direction 3
1.2 Cadre légal et réglementaire 3
1.3 Engagements et responsabilités des utilisateurs 3
1.4 Non-respect et sanctions 4
2 Généralités 4
2.1 Objet et champ d'application 4
2.2 Acronymes, termes et définitions 5
2.3 Droits et devoirs du CINES 6
2.4 Droits et devoirs de l'utilisateur 6
3 Conditions d'utilisation du système d'information 6
3.1 Conditions d'accès 6
4 Principes de sécurité 7
4.1 Règles générales de sécurité 7
4.2 Réseaux sociaux 7
4.2.1 Usage personnel 7
4.3 Mesures de contrôle de la sécurité 8
4.4 Journalisation des accès 8
5 Conformité aux règlements et lois en vigueur 8
5.1 Respect de la propriété intellectuelle 8
5.2 Respect du RGPD et de la loi « Informatique et Libertés » 9
5.2.1 Principes 9
5.2.2 Information des utilisateurs 9
5.2.3 Respect de la vie privée et des lois sur la diffusion de l'information 9
5.2.4 Respect de la charte RENATER 10
6 Limites d'usage et sanctions 10
7 Entrée en vigueur et révision 10

Préambule

1.1 CONTEXTE STRATEGIQUE ET ENGAGEMENT DE LA DIRECTION

Le Centre Informatique National de l'Enseignement Supérieur (CINES) est un établissement public administratif (EPA) placé sous la tutelle du ministère chargé de l'Enseignement supérieur, de la Recherche et de l'Espace (MESRE). Il assure trois missions nationales critiques : le calcul numérique intensif (HPC), l'archivage pérenne de données électroniques numériques et l'hébergement de plateformes stratégiques, dont des plateformes certifiées Hébergeur de Données de Santé (HDS).

La réalisation de ces missions repose sur un capital informationnel d'intérêt national dont la protection constitue un impératif absolu et une obligation légale. Le CINES est classé Zone à Régime Restrictif (ZRR) au sens du décret n° 2011-1425 du 2 novembre 2011.

Conformément à la Politique de Sécurité de l'Information (PSI) approuvée par le Directeur en sa qualité d'Autorité Qualifiée pour la Sécurité des Systèmes d'Information (AQSSI), le CINES a mis en place un Système de Management de la Sécurité de l'Information (SMSI) visant la double conformité aux référentiels ISO/IEC 27001:2022 et HDS V2.0.

1.2 CADRE LEGAL ET REGLEMENTAIRE

L'utilisation des systèmes d'information du CINES s'inscrit dans un cadre juridique strict. Ce cadre comprend notamment :

- ✓ La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) rendue obligatoire par circulaire du Premier ministre ;
- ✓ Le Règlement Général sur la Protection des Données (RGPD — Règlement UE 2016/679) et la loi Informatique et Libertés (loi n° 78-17 du 6 janvier 1978 modifiée) ;
- ✓ Le Code de la Santé Publique (articles L.1111-8 et suivants) régissant l'hébergement et la protection des données de santé (DSCP) ;
- ✓ La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles ;
- ✓ La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) ;
- ✓ Le Code pénal, notamment ses articles 410-1, 411-9 et 413-7 relatifs aux atteintes aux intérêts fondamentaux de la nation et aux ZRR ;
- ✓ Le Code pénal, articles 323-1 à 323-7, réprimant les atteintes aux systèmes de traitement automatisé de données ;
- ✓ La charte déontologique d'usage du réseau RENATER, réseau à vocation strictement professionnelle.

1.3 ENGAGEMENTS ET RESPONSABILITES DES UTILISATEURS

Dans ce contexte de haute exigence, la sécurité est l'affaire de tous. L'accès aux ressources informatiques du CINES non classées publiques est conditionné à l'acceptation de la présente charte.

Dans le cadre de la présente charte, le terme **«** utilisateur **»** désigne toute personne physique ou morale accédant aux ressources informatiques du CINES, quels que soit son statut et son mode d'accès : agent, partenaire, prestataire externe ou tout autre tiers autorisé.

L'utilisateur s'engage notamment à :

- ✓ Garantir la sécurité de l'information : veiller à la confidentialité, l'intégrité et la disponibilité des informations traitées, avec une vigilance accrue pour les données non classifiée ou classifiée à sensible ou restreinte.
- ✓ Utiliser les ressources de manière conforme : n'utiliser les ressources informatiques que dans le cadre professionnel autorisé et pour les finalités prévues par les activités du CINES ;
- ✓ Protéger ses moyens d'authentification : les mots de passe, badges et tokens MFA sont strictement personnels et ne doivent jamais être partagés ;
- ✓ Signaler sans délai au RSSI et au support tout incident de sécurité, dysfonctionnement ou événement suspect.

1.4 NON-RESPECT ET SANCTIONS

Tout manquement aux règles de la présente charte, qu'il résulte d'une négligence ou d'une malveillance, expose son auteur à :

- ✓ Des sanctions civiles et pénales prévues par les textes législatifs et réglementaires en vigueur ;
- ✓ La suspension, la suppression ou la limitation de ses accès au système d'information du CINES.

2 GENERALITES

2.1 OBJET ET CHAMP D'APPLICATION

La présente charte :

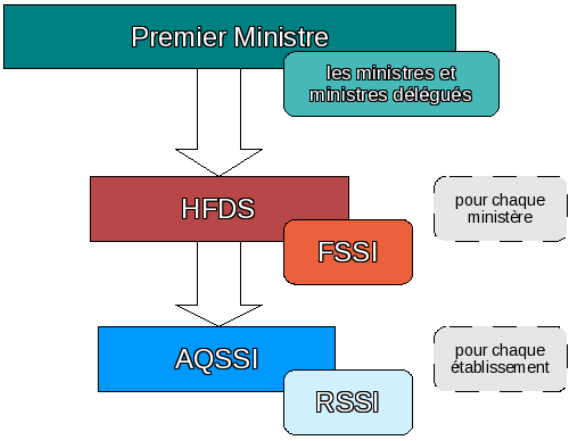
- ✓ explicite les règles d'utilisation des moyens informatiques au CINES ;
- ✓ précise les droits et devoirs du CINES et de ses utilisateurs ;
- ✓ rappelle les dispositions législatives et réglementaires applicables ainsi que les sanctions encourues en cas de non-respect ;
- ✓ constitue un code de bonne conduite à valeur juridique, élément fondamental de la politique de sécurité du CINES ;

Elle s'applique à toute personne susceptible d'accéder et d'utiliser le système d'information du CINES : fonctionnaires, contractuels, prestataires, stagiaires, régie, etc. Elle pourra évoluer en fonction du contexte légal et de la politique de sécurité en vigueur.

2.2 ACRONYMES, TERMES ET DEFINITIONS

AQSSI : Autorité Qualifiée pour la Sécurité du Système d'Information. Rôle tenu par le Directeur du CINES. Définit la politique de sécurité et en fixe les objectifs et les moyens.

Chaîne fonctionnelle SSI : Constituée dans l'ordre par l'AQSSI, le RSSI et le CSSI, conformément à la directive interministérielle n° 901.



Localement la *chaine fonctionnelle sécurité du système d'information* est constituée dans l'ordre par AQSSI, RSSI, CSSI.

DSCP : Données de Santé à Caractère Personnel. Catégorie de données spécifiquement protégée dans le cadre de la certification HDS.

Donnée sensible : Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, ainsi que les données génétiques ou biométriques ou encore relatives à l'appartenance syndicale, la santé, l'orientation sexuelle ou la vie sexuelle d'une personne physique. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes ; (RGPD 2016/679 Art 9).

DPO / DPD : Délégué à la Protection des Données. Placé sous l'autorité directe du Directeur, il assure la conformité RGPD du CINES.

Mobilité / Travail à distance : Situation dans laquelle l'utilisateur accède au système d'information du CINES depuis un lieu autre que les locaux du CINES (domicile, déplacement professionnel, colloque, conférence, etc.).

Réseau social : Plateforme numérique permettant aux utilisateurs de publier du contenu, d'interagir et de partager des informations (exemples : LinkedIn, X/Twitter, Facebook, Instagram, TikTok, Mastodon …).

Supports amovibles : Tout dispositif de stockage portable pouvant être connecté à un poste de travail ou un serveur (clé USB, disque dur externe, carte SD, etc.).

Utilisateur : Toute personne ayant accès, dans le cadre de son activité, aux ressources du système d'information du CINES.

ZRR : Zone à Régime Restrictif au sens du décret n° 2011-1425 du 2 novembre 2011. Le CINES est classifié ZRR. L'accès non autorisé est puni de 6 mois d'emprisonnement et 7 500 € d'amende (art. 413-7 du Code pénal).

2.3 DROITS ET DEVOIRS DU CINES

Le CINES :

- ✓ porte la présente charte à la connaissance de l'utilisateur ;
- ✓ met en œuvre les mesures nécessaires pour assurer la sécurité (disponibilité, intégrité, confidentialité) du système d'information et la protection des utilisateurs ;
- ✓ met en œuvre les mesures nécessaires pour assurer la protection des données dont il a la charge ;
- ✓ facilite l'accès des utilisateurs aux ressources du système d'information selon leurs besoins légitimes.

2.4 DROITS ET DEVOIRS DE L'UTILISATEUR

L'utilisateur :

- ✓ est responsable, en tout lieu et à tout moment, de l'usage qu'il fait du système d'information auquel il a accès ;
- ✓ est soumis à une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède ;
- ✓ collabore avec le CINES dans l'identification et la résolution de toute difficulté relative à l'utilisation du système d'information ;

3 CONDITIONS D'UTILISATION DU SYSTEME D'INFORMATION

3.1 CONDITIONS D'ACCES

Le CINES étant classé Zone à Régime Restrictif (ZRR) selon le décret n°2011-1425 du 2 novembre 2011, le droit d'accès physique ou virtuel au système d'information non public du CINES est soumis à autorisation préalable et protégé par des moyens d'authentification (identifiants, mots de passe, badges, MFA). Ce droit est personnel, temporaire et incessible. Il disparaît dès que l'utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès.

En application de l'article 413-7 du Code pénal, les personnes qui pénètrent sans autorisation dans une ZRR risquent une peine de 6 mois d'emprisonnement et 7 500 € d'amende. Les atteintes aux intérêts fondamentaux de la nation sont sanctionnées jusqu'à 15 ans de détention criminelle et 225 000 € d'amende (art. 411-9 du Code pénal).

4 PRINCIPES DE SECURITE

4.1 REGLES GENERALES DE SECURITE

L'utilisateur s'engage à :

- ✓ respecter les consignes relatives à la gestion des mots de passe;
- ✓ garder strictement confidentiel(s) son ou ses mot(s) de passe et ne pas les dévoiler à un tiers ;
- ✓ utiliser des mots de passe différents pour des environnements ou périmètres différents ;
- ✓ choisir un mot de passe suffisamment robuste conformément à la politique de contrôle d'accès et le changer en cas de doute ou d'utilisation depuis un équipement non sécurisé ;
- ✓ signaler immédiatement le vol ou la perte de tout moyen d'authentification à la chaîne fonctionnelle SSI ;
- ✓ ne pas utiliser le système d'information du CINES au-delà de ce qui est nécessaire dans le cadre de ses attributions et missions ;
- ✓ ne pas tenter d'accéder à des ressources pour lesquelles il ne dispose pas d'habilitation explicite ;
- ✓ ne pas connecter aux réseaux locaux du CINES des équipements non autorisés par le CINES ;
- ✓ ne pas installer, télécharger ou utiliser sur le matériel du CINES des logiciels ou fichiers exécutables dont les droits de licence n'ont pas été acquittés ou ne provenant pas de sources dignes de confiance ;
- ✓ assurer la protection des informations sensibles et ne pas les transporter sans chiffrement sur des supports mobiles ;
- ✓ signaler à svp@cines.fr ou par appel téléphonique, toute violation ou tentative de violation suspectée de son compte informatique.

4.2 RESEAUX SOCIAUX

Les réseaux sociaux sont des espaces publics ou semi-publics dans lesquels les informations publiées peuvent être diffusées largement et de manière incontrôlable. Leur usage, même à titre personnel depuis les équipements du CINES ou dans le cadre professionnel, requiert une vigilance particulière.

4.2.1 Usage personnel

Lors de l'utilisation des réseaux sociaux à titre personnel, l'utilisateur :

- ✓ Peut mentionner son utilisation des ressources du CINES, ainsi que des informations génériques sur ses missions ou projets, à condition que celles-ci :
  - ne révèlent aucune donnée sensible (architecture système, vulnérabilités, configurations techniques, etc.) ;
  - ne portent pas atteinte à la confidentialité des projets en cours ou des partenaires ;
  - respectent les règles de propriété intellectuelle et les accords de non-divulgation en vigueur.
- ✓ Faire preuve de prudence sur les informations apparemment anodines (lieu de travail, déplacements professionnels, organisation de l'équipe, outils utilisés) qui peuvent être exploitées par des acteurs malveillants ;
- ✓ Ne pas accepter de demandes de mise en relation émanant de personnes inconnues ou dont l'identité ne peut pas être vérifiée, lorsque cette connexion pourrait exposer des informations sur le CINES ;
- ✓ Rappeler que publier des informations confidentielles ou diffamatoires sur les réseaux sociaux engage la responsabilité civile et pénale de leur auteur.

4.3 MESURES DE CONTROLE DE LA SECURITE

L'utilisateur est informé que le CINES se réserve le droit de réaliser des interventions sur les ressources mises à sa disposition à des fins de maintenance corrective, curative ou évolutive. Toute intervention est précédée d'une information de l'utilisateur. Les données recueillies du système d'information peuvent être exploitées à des fins statistiques, de traçabilité réglementaire, d'optimisation, de sécurité ou de détection des abus. Un système de vidéoprotection et de surveillance périmétrique est en place 24h/24 et 7j/7 autour des bâtiments du CINES.

4.4 JOURNALISATION DES ACCES

Le CINES est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des accès physiques. À cet effet, le CINES se réserve le droit de mettre en place des outils de traçabilité sur toutes les ressources du système d'information. Les données de journalisation sont traitées conformément au RGPD et conservées selon les durées définies dans la politique de journalisation du CINES.

5 CONFORMITE AUX REGLEMENTS ET LOIS EN VIGUEUR

5.1 RESPECT DE LA PROPRIETE INTELLECTUELLE

L'utilisation des ressources informatiques implique le respect des droits de propriété intellectuelle. L'utilisateur doit :

- ✓ utiliser les logiciels dans les conditions des licences souscrites ;

- ✓ ne pas reproduire, copier, diffuser, modifier ou utiliser tout document numérique protégé par le droit d'auteur sans autorisation préalable des titulaires ;
- ✓ respecter le droit des marques.

5.2 RESPECT DU RGPD ET DE LA LOI « INFORMATIQUE ET LIBERTES »

5.2.1 Principes

L'utilisateur est tenu de respecter les dispositions légales en matière de traitement de données à caractère personnel, conformément au RGPD (Règlement UE 2016/679) et à la loi n° 78-17 du 6 janvier 1978 modifiée. Tout manquement est susceptible de sanctions disciplinaires et pénales.

Toute création de fichier comprenant des données à caractère personnel est soumise aux formalités prévues par le RGPD. L'utilisateur souhaitant procéder à un tel traitement doit s'assurer de sa conformité et informer le DPO du CINES.

5.2.2 Information des utilisateurs

Le CINES s'engage à ce que les données à caractère personnel des utilisateurs soient collectées et traitées de manière loyale et licite. Les utilisateurs sont informés que :

- ✓ Le responsable du traitement est : CINES, 950 rue de Saint Priest, 34097 Montpellier Cedex 5 — dpo@cines.fr ;
- ✓ Les finalités poursuivies : gestion des accès au SI et aux locaux, maintenance et sécurité du SI, obligations de contrôle en ZRR, préservation de la confidentialité des données ;
- ✓ La base juridique : exécution du contrat liant le CINES aux utilisateurs, intérêt légitime du responsable du traitement, respect d'obligations légales ;
- ✓ Les données sont conservées pendant la durée du contrat augmentée des durées légales applicables ; les données de contrôle sont conservées 12 mois ;
- ✓ Les données ne font pas l'objet de transfert à destination d'un pays tiers ni de prise de décision automatique.

L'utilisateur dispose des droits d'accès, de rectification, d'effacement, de limitation, à la portabilité et d'opposition. Ces droits s'exercent auprès du DPO (dpo@cines.fr) ou par réclamation auprès de la CNIL (www.cnil.fr).

5.2.3 Respect de la vie privée et des lois sur la diffusion de l'information

Le droit à la vie privée, le droit à l'image et le droit de représentation impliquent qu'aucune image ou information relative à la vie privée d'autrui ne doit être mise en ligne sans l'autorisation de la personne intéressée. La diffusion de messages diffamatoires ou injurieux, les provocations et apologies, l'accès,

la détention ou la diffusion d'images à caractère pédopornographique, la publication d'informations confidentielles sans autorisation sont strictement interdits.

5.2.4 Respect de la charte RENATER

Le CINES est membre de la communauté RENATER. Les règles d'usage de ce réseau réservé à un usage professionnel s'imposent à tous les utilisateurs. L'usage commercial à titre privé de RENATER est proscrit.

6 LIMITES D'USAGE ET SANCTIONS

L'utilisateur est passible de sanctions dans les cas suivants :

- ✓ non-respect des règles définies dans la présente charte ;
- ✓ publication d'informations internes ou confidentielles sur les réseaux sociaux.

Les sanctions applicables sont :

- ✓ les sanctions civiles et pénales prévues par les textes législatifs et réglementaires en vigueur ;
- ✓ la suspension, suppression ou limitation des accès et droits d'utilisation du système d'information.

7 ENTREE EN VIGUEUR ET REVISION

La présente charte annule et remplace tous les documents ou chartes relatifs à l'utilisation des systèmes d'information du CINES, et notamment la version V1 de la charte informatique (adoptée le 27/11/2020, révisée le 15/01/2026).

Elle a été adoptée en Conseil d'administration du CINES le **25 juin 2026** Elle entre en vigueur à compter de la date d'approbation par l'AQSSI.