Conditions Générales d'Utilisation des Services GRICAD

1. Préambule

Les présentes **Conditions Générales d'Utilisation (CGU)** définissent les règles d'accès et d'usage des services informatiques proposés par l'**UAR GRICAD** (Université Grenoble Alpes, CNRS, Grenoble INP-UGA, Inria), incluant :

- les services de calcul intensif et de stockage associés (Supercalculateur : Dahu, Bigfoot, Luke, Kraken ; Espaces de stockages : Bettik, Silenus, Hoyt, MANTIS) ;
- la plateforme de *cloud computing* (**NOVA**) ;
- le portail de gestion des comptes et projets scientifiques (**PERSEUS**).

Ces CGU s'appliquent à tous les utilisateurs autorisés, dans le cadre de leurs activités d'enseignement, de recherche ou de collaboration scientifique.

Les services GRICAD sont fournis dans le respect des lois et règlements en vigueur, notamment :

- la **loi n°78-17 du 6 janvier 1978** (Informatique et Libertés) ;
- le **Règlement (UE) 2016/679 (RGPD)** ;
- la **loi n°2004-575 du 21 juin 2004** (Confiance dans l'économie numérique) ;
- ainsi que les **chartes informatiques** du CNRS et de l'UGA.

---

2. Accès aux services et création de projet

L'accès aux services GRICAD est réservé :

- aux personnels et étudiants des établissements académiques partenaires ;
- ou aux structures bénéficiant d'un accord ou d'une convention spécifique.

Toute utilisation nécessite :

- la création d'un compte sur PERSEUS ;
- et le rattachement à un **projet scientifique** validé par GRICAD. Ce rattachement est validé par le responsable du projet.

Le responsable du projet renseigne :

- les objectifs scientifiques ;
- les besoins en ressources ;
- et la nature des données traitées (ordinaires, sensibles, de santé).

En outre, le ou la responsable du projet est responsable de la gestion des membres de son projet et doit s'assurer que chaque membre est bien légitime à en faire partie. En cas de non-respect des présentes CGU, son compte peut être désactivé sans avertissement ainsi que son projet.

Les infrastructures sont hébergées dans les datacentres de l'Université Grenoble Alpes, soumis à la réglementation française et européenne.

---

3. Classification et gestion des données

Le **responsable scientifique du projet** est **propriétaire et responsable des données** qu'il confie à GRICAD.

Il lui appartient de :

- classifier les données selon leur sensibilité (publiques, confidentielles, sensibles, HDS) ;
- déclarer toute donnée personnelle et/ou de santé lors de la création du projet ;
- garantir la conformité RGPD et, le cas échéant, HDS des traitements effectués.

Les projets manipulant des données de santé sont soumis à l'Annexe HDS GRICAD.

GRICAD ne garantit pas la sauvegarde des données. GRICAD recommande que le jeu de données déposés à des fins de traitement soit un duplicata.

---

4. Conditions d'utilisation

L'utilisateur s'engage à :

- utiliser les ressources exclusivement pour le projet validé ;
- respecter les bonnes pratiques publiées sur la documentation GRICAD ;
- ne pas détourner les services à des fins commerciales, personnelles ou illégales ;
- respecter les règles de sécurité et d'éthique de la recherche.

Les processus GRICAD encadrent :

- la gestion des droits et habilitations ;

- la protection des supports de données ;
- la supervision des accès et des usages.

Les utilisateurs sont informés que des activités de **journalisation et de surveillance de sécurité** sont en place.

---

5. Durée, renouvellement et cessation

L'accès débute à l'ouverture du compte et la validation du projet sur PERSEUS. Chaque projet est renouvelé annuellement sur présentation d'un rapport d'activité et d'une bibliographie. En cas de cessation du projet ou de départ du responsable, GRICAD doit être informé sans délai pour clôturer le compte.

En cas de projet inactif d'une durée supérieure à 6 mois GRICAD se réserve le droit de le clôturer après en avoir informé le responsable de projet. Ce délai est rapporté à 3 mois en cas de projet HDS.

En cas de défaillance d'un service, GRICAD s'engage à :

- avertir les utilisateurs ;
- faciliter la récupération des données disponibles ;
- orienter vers des services équivalents le cas échéant.

---

6. Suspension et interruption

Les services peuvent être suspendus :

- en cas de maintenance planifiée, d'incident ou de risque pour la sécurité ;
- sur demande d'une autorité administrative ou judiciaire ;
- en cas d'usage frauduleux ou de non-respect manifeste des CGU.

Une suspension immédiate peut être appliquée en cas d'urgence ou de compromission.
Les utilisateurs sont informés et disposent d'un délai de 30 jours pour régulariser leur situation.

---

7. Responsabilités

7.1. Responsabilités des utilisateurs

Les utilisateurs et responsables de projets :

- garantissent la conformité juridique de leurs traitements et données ;
- veillent à la pseudonymisation ou anonymisation des données à caractère personnel ;
- sécurisent leurs environnements logiciels et codes sources ;
- s'interdisent de transmettre des données sensibles par des moyens non sécurisés.
- s'engagent à récupérer leurs données à la fin de leur projet.

7.2. Responsabilités de GRICAD

GRICAD :

- assure l'exploitation et la maintenance des infrastructures ;
- garantit la confidentialité et l'intégrité des services ;
- assure au mieux la disponibilité des services ;
- met en œuvre des mesures de sécurité conformes aux référentiels ISO 27001 et HDS ;
- informe des maintenances non-urgentes au moins dix jours ouvrés à l'avance ;
- ne traite pas les données hébergées au-delà des opérations techniques nécessaires.

GRICAD ne saurait être tenu responsable des pertes de données imputables à l'utilisateur ni des interruptions dues à des cas de force majeure.

L'ensemble des infrastructures soutenant les services de GRICAD est situé en France et donc, notamment pour le stockage de données, est soumis à la réglementation européenne.

7.3. Indicateurs de qualité et de performance des services

Lors de la revue annuelle de direction de GRICAD un ensemble d'indicateurs de qualité et de performance est analysé. Ces indicateurs relèvent aussi bien de la sécurité du système d'information (*e.g.* MTTD,MTTR), de la stabilité des systèmes(*e.g.* taux de disponibilité des systèmes), de leurs usages (*e.g.* temps d'attente moyens, taux d'occupation), etc. Une partie de ces indicateurs sont remontés aux utilisateurs via le COmité Scientifique et Techniques des Utilisateurs de GRICAD.

De plus, l'ensemble des utilisateurs ont accès sans restriction au https://gricad-dashboards.univ-grenoble-alpes.fr regroupant des indicateurs de l'usage des services.

Si GRICAD met tout en œuvre pour assurer la meilleure qualité de service possible, elle ne peut faire l'objet de pénalités de la part des utilisateurs.

8. Propriété intellectuelle

Pour les services où les utilisateurs installent leurs propres logiciels, si ceux-ci sont sous licences privatives, les utilisateurs s'engagent à respecter les conditions de licence.

---

9. Support et communication

- **Support technique** : sos-gricad@univ-grenoble-alpes.fr
- **Contact général** : gricad-contact@univ-grenoble-alpes.fr

Délai de réponse moyen : 10 jours ouvrés.

---

10. Données personnelles et mentions légales

Le portail **PERSEUS** fait l'objet d'un traitement de données personnelles pour la gestion des accès et projets.
Les données d'authentification sont conservées un an après la clôture du projet.
Aucun transfert de données de santé à caractère personnel vers un pays tiers à l'espace économique européen n'est effectué.

GRICAD est responsable de traitement au sens RGPD s'agissant des données à caractère personnel collectées pour la gestion des droits d'accès. Le DPD compétent pour GRICAD est le DPD CNRS. GRICAD a le rôle de sous-traitant au sens RGPD s'agissant des données déposées par le responsable de projet qui a le rôle de Responsable de Traitement. Le DPD CNRS tient un registre de sous-traitance.

Lorsque GRICAD est sous-traitant de données à caractère personnel, utilisées à des fins de recherche et confiées à GRICAD par les utilisateurs, GRICAD assurera : - L'obligation de notification dans les meileurs délais en cas d'incidents pouvant entraîner une violation des données personnelles - L'obligation de collaboration et d'assistance et s'engage à supprimer les données à l'issue du projet - L'obligation de garantir la sécurité et la confidentialité des données - L'obligation de transparence, en mettant à disposition des responsables de traitement tous les éléments (*e.g.* procédures, rapport d'audits techniques) démontrant le bon respect des exigences de sécurité d'une part et de la réglementation d'autre part.

GRICAD s'engage à ne pas faire appel à une sous-traitant pour assurer tout ou partie de l'exploitation des infrastructures et services.

Dans le cadre où GRICAD est sous-traitant du traitement de données à caractère personnel, le Délégué à la Protection des Données est celui rattaché à la/au responsable du projet qui est, de facto, le responsable de traitement. En général, c'est le DPO du laboratoire de rattachement du/de la responsable de projet. Toujours dans ce cadre, pour ouvrir le projet, le responsable de

traiatement devra nous transmettre en écrivant gricad-rgpd@univ-grenoble-alpes.fr l'attestation de conformité de son traitement signé par le DPO désigné ci-dessus.

Les utilisateurs disposent des droits d'accès, de rectification, d'effacement et de portabilité, à exercer auprès de :
gricad-rgpd@univ-grenoble-alpes.fr

---

11. Acceptation

L'utilisation des services GRICAD vaut acceptation sans réserve des présentes CGU.
Les utilisateurs doivent les accepter numériquement à la création de leur compte et à nouveau en cas de modification substantielle.

Voir également : Annexe HDS GRICAD pour les projets manipulant des données de santé.

Annexe PERSEUS – Portail de gestion des comptes et projets scientifiques

1. Objet

Cette annexe complète les CGU GRICAD.
Elle décrit les conditions spécifiques d'utilisation du **portail PERSEUS**, outil central de gestion :

- des **comptes utilisateurs** ;
- des **projets scientifiques** et de leurs responsables ;
- de la **validation scientifique et technique** des demandes d'accès ;
- et du **rattachement** aux services de calcul (CIMENT) et de cloud (NOVA).

---

2. Rôle et finalité

Le portail PERSEUS a pour objectifs de : - centraliser la gestion des identités et des habilitations ; - suivre les projets scientifiques et les ressources allouées ; - garantir la traçabilité et la conformité RGPD/HDS ; - fournir une interface unique d'accès sécurisé aux services GRICAD.

Les données collectées concernent uniquement la gestion administrative, scientifique et technique des utilisateurs et projets.

---

3. Création et gestion des comptes

- La création d'un compte est soumise à une **authentification académique** (fédération Éducation-Recherche ou identité locale validée par un établissement partenaire).
- Chaque compte est **nominal** et **non transférable**.
- L'utilisateur est responsable de la **confidentialité de ses identifiants** et de l'usage de son compte.

Les comptes inactifs depuis plus de 12 mois peuvent être **désactivés** après notification.

---

4. Gestion des projets

Un projet PERSEUS contient : - un **intitulé scientifique** et un **responsable** ; - les **membres rattachés** ; - les **ressources GRICAD** utilisées (calcul, stockage, cloud) ; - et la **nature des données traitées** (scientifiques, sensibles, santé).

Le responsable scientifique : - est garant du respect des CGU et de la conformité RGPD/HDS ; - doit maintenir à jour les informations du projet (membres, données, publications) ; - produit un **rapport annuel** conditionnant le renouvellement du projet.

---

5. Protection des données personnelles

Les données collectées sur PERSEUS sont utilisées pour : - gérer les comptes et projets ; - tracer l'usage des ressources ; - assurer le suivi des activités scientifiques.

Base légale : mission d'intérêt public.
Durée de conservation : un an après la clôture du projet.
Droits RGPD : accès, rectification, effacement, opposition, portabilité via gricad-rgpd@univ-grenoble-alpes.fr

Aucun transfert hors Union européenne n'est effectué.

---

6. Déclaration des projets sensibles ou HDS

Lors de la création d'un projet, le formulaire PERSEUS permet de : - indiquer si le projet traite des données à caractère personnel ou de santé ; - déclencher l'étiquetage **"HDS"** du projet et l'application des mesures renforcées (voir Annexe HDS).

---

7. Sécurité et journalisation

- Authentification forte via LDAP et fédération d'identité ;
- Journalisation des accès et opérations critiques ;
- Conservation des journaux 12 mois ;
- Supervision de la disponibilité et de la conformité du service.

---

8. Support et contacts

Pour toute question liée à PERSEUS : sos-gricad@univ-grenoble-alpes.fr

Annexe CIMENT – Infrastructures de calcul intensif et espaces de stockage associés

1. Objet

Cette annexe complète les CGU GRICAD.
Elle précise les conditions d'utilisation des **plateformes de calcul intensif CIMENT** et des **espaces de stockage associés** : - `/scratch` (stockage temporaire), - `/bettik`, `/silenus`, `/hoyt` (stockages projet à haute capacité), - et **MANTIS**, l'espace de **stockage de données tièdes** basé sur la technologie *iRODS*.

---

2. Finalité et périmètre

Les ressources CIMENT ont pour finalité : - le calcul intensif (simulation, modélisation, IA, etc.) ; - la gestion de données scientifiques volumineuses ; - et la mutualisation des ressources pour la recherche publique.

L'accès est réservé aux projets validés sur PERSEUS.

---

3. Responsabilités des utilisateurs

Les utilisateurs s'engagent à : - lire et appliquer les bonnes pratiques CIMENT ; - respecter les quotas de ressources et les règles de partage équitable ; - stocker uniquement les données nécessaires au projet ; - libérer leurs espaces de calcul et de stockage en fin d'usage.

Le **responsable du projet** est garant : - de la conformité juridique des données stockées ; - et de l'application des mesures de protection appropriées.

---

4. Politique de stockage

Espace	Type de données	Durée de conservation	Sauvegarde
`/scratch`	Données temporaires de calcul	Suppression automatique régulière	Non
`/bettik`, `/silenus`, `/hoyt`	Données projet actives	Selon la durée du projet	Non (sauf HDS)

Espace	Type de données	Durée de conservation	Sauvegarde
`MANTIS (iRODS)`	Données tièdes / archivage intermédiaire	Jusqu'à 2 ans après fin du projet	Sauvegarde partielle (métadonnées iRODS)

Les utilisateurs sont responsables de la sauvegarde finale de leurs données scientifiques.

---

5. Sécurité et supervision

- Accès via authentification nominale ;
- Journalisation des connexions et opérations critiques ;
- Isolation logique des espaces projets ;
- Aucune donnée sensible ou de santé ne doit être stockée hors périmètre HDS.

Les environnements de calcul sont supervisés 24/7.
Les journaux sont conservés 12 mois.

---

6. Données sensibles et HDS

Les projets manipulant des données de santé doivent : - être identifiés comme "HDS" dans PERSEUS ; - utiliser uniquement les volumes HDS de Bettik/MANTIS ; - se conformer à l'Annexe HDS GRICAD.

---

7. Responsabilités GRICAD

GRICAD s'engage à : - garantir un partage équitable des ressources ; - maintenir les performances et la sécurité des systèmes ; - assurer la disponibilité des services 24/7 (hors maintenance planifiée) ; - informer des arrêts programmés avec un préavis minimal de 10 jours ouvrés.

---

8. Support

sos-calcul-gricad@univ-grenoble-alpes.fr
Documentation : https://gricad-doc.univ-grenoble-alpes.fr/hpc/

Annexe NOVA – Plateforme de cloud computing OpenStack

1. Objet

Cette annexe complète les CGU GRICAD.
Elle définit les conditions spécifiques d'utilisation de la **plateforme de cloud computing NOVA**, basée sur la technologie **OpenStack**.

---

2. Finalité et offre de service

NOVA offre un environnement cloud académique permettant : - le déploiement de **machines virtuelles (VMs)** à la demande ; - la gestion de volumes persistants ; - l'utilisation de **quotas par projet** ; - et l'administration via **interface web, CLI ou API OpenStack**.

---

3. Conditions d'utilisation

- L'accès est réservé aux utilisateurs possédant un compate actif et étant dans un projet validé sur PERSEUS.
- Les utilisateurs s'engagent à :
  - libérer leurs VMs lorsqu'elles ne sont plus utilisées ;
  - sécuriser les systèmes déployés (mises à jour, pare-feu, comptes) ;
  - ne pas héberger de services ouverts sans autorisation préalable.

Les volumes NOVA ne sont pas sauvegardés par GRICAD.

---

4. Responsabilités

4.1. Utilisateurs

- Assurent la **sécurisation logicielle** de leurs VMs ;
- Gèrent les comptes, mots de passe et accès aux instances ;
- Veillent à la conformité des traitements RGPD et HDS si applicable.

4.2. GRICAD

- Fournit les ressources virtuelles demandées, dans la limite des capacités disponibles ;
- Supervise les performances et la sécurité du cloud ;
- Peut suspendre ou supprimer une instance compromettant la sécurité du service.

---

5. Sécurité et conformité

- Infrastructure OpenStack isolée en zones de sécurité ;
- Journalisation des actions d'administration et des utilisateurs ;
- Chiffrement des communications (HTTPS, SSH) ;
- Contrôles d'accès par rôles (RBAC) ;
- Surveillance des incidents et alertes automatiques.

Les projets traitant des données de santé doivent se conformer à l'Annexe HDS GRICAD.

---

6. Durée et ressources

Les ressources NOVA sont attribuées pour la durée du projet PERSEUS.
Elles sont **renouvelées annuellement** sur validation du rapport d'activité.
À la fin du projet, les volumes et VMs sont supprimés.

---

7. Support

sos-nova-gricad@univ-grenoble-alpes.fr](mailto:sos-nova-gricad@univ-grenoble-alpes.fr)
Documentation : https://gricad-doc.univ-grenoble-alpes.fr/nova/

Annexe HDS – Hébergement de Données de Santé

1. Objet

La présente annexe complète les **Conditions Générales d'Utilisation (CGU)** de GRICAD dans le cadre de la **certification Hébergeur de Données de Santé (HDS) niveaux 1 à 4**.
Elle s'applique aux projets hébergeant ou traitant des **données de santé à caractère personnel** sur les infrastructures de calcul intensif et de stockage associées.

---

2. Périmètre

Le périmètre de certification HDS datant du ***XX/XX/XXXX*** ne couvre qu'une partie des services rendus par GRICAD, qui sont les suivants :

- les services de calcul intensif et stockage (**CIMENT**) ;
- les espaces de stockage associés (Bettik, Silenus, Hoyt) ;
- et le portail **PERSEUS** pour la gestion des projets et comptes HDS.

Ces services sont hébergés dans des datacentres sécurisés de l'Université Grenoble Alpes, certifiés selon les référentiels **ISO/IEC 27001** et **HDS (v2.1 – ANS)**.

En cas de modification ou d'évolutions techniques impactant le périmètre décrit ci-dessous, GRICAD, s'engage à notifier et à obtenir l'accord préalable des utilisateurs via le portail PERSEUS.

---

3. Classification et identification

- Tout projet manipulant des données de santé est identifié dans PERSEUS par un **préfixe "HDS"**.
- Le responsable scientifique déclare la nature des données et fournit les éléments de conformité RGPD/HDS.

Les espaces de stockage HDS sont isolés logiquement.
Les journaux d'accès sont conservés **12 mois** et audités régulièrement.

---

4. Engagements de GRICAD

GRICAD garantit la mise en œuvre d'un **Système de Management de la Sécurité de l'Information (SMSI)** conforme au référentiel HDS, incluant :

- Gouvernance de sécurité (RSSI, DPO, direction GRICAD) ;
- Supervision et journalisation complètes ;
- Ségrégation des environnements HDS / non HDS ;
- Chiffrement des flux et des supports ;
- Gestion des habilitations et des accès privilégiés ;
- Traçabilité et conservation des journaux ;
- Plans de continuité et de reprise (PCA / PRA) ;
- Audits de conformité internes et externes.

GRICAD n'accède pas de données de santé hébergées, en dehors des opérations d'administration et de maintenance technique nécessaires à la sécurisation desdites données.

GRICAD s'engage à fournir aux utilisateurs qui en font la demande via gricad-contact@univ-grenoble-alpes.fr le dernier rapport d'audit à date de certification HDS.

---

5. Obligations des utilisateurs

Les utilisateurs et responsables de projets HDS s'engagent à :

1. Déclarer les données de santé dans PERSEUS et respecter les procédures HDS ;
2. Utiliser exclusivement les espaces de stockage et nœuds de calcul dédiés HDS ;
3. Anonymiser les données chaque fois que possible ; pseudonymiser à minima ;
4. Ne pas transférer de données à caractère personnel par courriel, ticket ou tout canal non sécurisé ;
5. Signaler immédiatement tout incident de sécurité à GRICAD.

Toute utilisation non conforme peut entraîner la **suspension immédiate** du projet concerné.

---

6. Gestion des incidents et conformité

GRICAD est sous-traitant au sens RGPD. Le responsable de traitement est le responsable du projet.

- Les incidents de sécurité sont consignés et traités selon la procédure « A16.1 – Gestion des incidents ».
- En cas de violation de données de santé, GRICAD notifie :
  - le responsable du projet, qui doit en informer le Délégué à la Protection des Données (DPD) dont il relève en tant que Responsable de Traitement,
  - le Délégué à la Protection des Données (DPD) du CNRS qui est compétent pour GRICAD
  - Le DPD compétent signale la violation auprès de la CNIL dans les 72h et prépare la communication à mener auprès des personnes le cas échéant

Des audits (de sécurité ou relatifs à la certification HDS) sont réalisés annuellement pour garantir l'amélioration continue du système de management du système d'information et du niveau de sécurité.

---

7. Sous-traitance et tiers

Aucun transfert ou sous-traitance hors UE n'est autorisé.

Les prestataires intervenant dans le périmètre HDS sont liés à GRICAD par des **clauses contractuelles de confidentialité et conformité HDS**.
GRICAD reste le **maître d'ouvrage** des opérations d'hébergement et de sécurité.

8. Acteurs et garanties

Les services de GRICAD sont intégralement réalisés en France. Ils n'entrainent aucun transfert de données de santé à caractère personnel vers un pays n'appartenant pas l'Espace Économique Européen.

Acteur Rôle	Certifié HDS	Qualité SecNumCloud 3.2	Activités d'hébergement	Accès depuis un pays tiers à l'EEA	Risque d'accès imposé par la législation d'un pays tiers
GRICAD Hébergeur	Non (au 04/03/2026)	Non	1 à 4	Non	Non

---

9. Références normatives

Ce document s'appuie sur :

- **Référentiel HDS – ANS v2.1 (2023)**
- **ISO/IEC 27001:2023** – Système de Management de la Sécurité de l'Information
- **ISO/IEC 27018:2019** – Protection des données à caractère personnel dans le cloud
- **RGPD (UE 2016/679)**
- **Loi Informatique et Libertés (modifiée)**

---

10. Révision et mise à jour

Cette annexe est revue :

- à chaque évolution du périmètre technique ;
- lors des audits HDS ;
- et au minimum une fois par an.