Déclaration de politique de sécurité

Objet

La déclaration de politique de sécurité est un document que le Centre de Calcul de l'Université de Bourgogne (CCuB) partage avec ses usagers. Elle explicite les objectifs et l'organisation du Système de Management de la Sécurité de l'Information (SMSI) mis en place pour la protection de leurs informations.

Elle est complétée par une politique de sécurité détaillée, interne au Centre de Calcul et consultable dans le cadre d'une démarche d'audit.

Engagement de la direction

Voir la lettre d'engagement de la direction.

Contexte

Cadre légal et réglementaire

Les activités du Centre de Calcul sont soumises au respect des exigences légales et réglementaires suivantes :

- RGPD
- PSSI de l'état
- Code de la santé publique :
  - Les exigences HDS (code de la santé publique, article L1111-8)
  - Référentiels opposables pour les services numériques en santé (code de la santé publique L1470-1 - L1470-6)
- Décret 2022-513 relatif à la sécurité numérique du système d'information et de communication de l’État et de ses établissements publics

Les obligations contractuelles peuvent être incluses dans les attentes des parties intéressées.

Domaine d'application

Activités du domaine d'application

Au sein de la Direction du Numérique de l'Université de Bourgogne, qui compte une soixantaine de personnes pour la mise à disposition des moyens numériques auprès des personnels et étudiants, le Centre de Calcul (5 personnes) a pour rôle la mise à disposition de moyens numériques pour la recherche, quel qu'en soit le domaine (physique, météorologie, sociologie, santé, etc.). Il s'agit notamment de moyens de calcul sur des données massives.

Dans le domaine de la santé humaine, le centre de calcul opère avec des entités externes assurant la prise en charge de patients. Les calculs effectués ne relèvent pas forcément que de la recherche, mais également de la prise en charge médicale. Typiquement, il s'agit de retrouver dans des données génomiques individuelles des signatures particulières (variants) issues de données de référence.

Occasionnellement, le centre met à la disposition d'usagers des machines virtuelles susceptibles de porter des données de santé à caractère personnel, notamment une machine porteuse du logiciel Calcium de gestion des dossiers patients pour le Centre de Prévention et de Santé Universitaire.

L'activité du Centre de Calcul est un service bien défini, dont on a vu que la certification 27001 pouvait être pertinente même dans des cas d’usage hors données de santé. Les écarts entre la certification 27001 et la certification HDS sont faibles, et ne justifient pas forcément de mettre en place des processus différenciés dans l’activité du centre.

Informations à protéger

Les informations à protéger sont:

- Les données primaires envoyées pour analyse
- Les résultats de calcul
- Les archives de résultats antérieurs
- Les données de référence (signatures de variants, etc.)
- Les configurations et scripts pour l'exécution des calculs
- Les données portées par les machines virtuelles mises à disposition.

L'ensemble de ces informations peuvent contenir des données de santé à caractère personnel selon les besoins des utilisateurs. Le Centre de Calcul ne traite aucune donnée de santé à caractère personnel en dehors de ces informations.

Périmètre physique

Le Centre de Calcul dispose actuellement de deux salles sur le campus, distantes d'environ 500 mètres, le centre de données et la salle SM2. Une seconde tranche du centre de données est lancée et permettra à terme d'ouvrir une nouvelle salle, comportant deux îlots : l'un pour le HPC généraliste, l'autre dédié au traitement des données de santé.

Un bâtiment indépendant de chaufferie comporte les groupes froid et les groupes

électrogènes.

Périmètre logique

Le Centre de Calcul héberge les données sur les espaces de stockage suivants :

- L’espace de stockage « HOME »
  Il s’agit d’un espace de stockage sécurisé, sauvegardé et historisé, destiné aux données primaires, données de références, configurations et scripts. Ses principales limitations sont :
  - Un coût par volume de données plus élevé que les autres espaces de stockage,
  - Une durée d’historisation limitée (typiquement 1 an),
  - Un volume maximal de modification de données autorisé par période d’historisation (afin de ne pas saturer le système d’historisation, puisque les changements sont conservés).
- L’espace de stockage « ARCHIVE »
  Il s’agit d’un espace de stockage sécurisé, destiné aux résultats archivés. Il est dupliqué sur bandes magnétiques stockées sur un autre site géographiquement distinct. Il n’y a pas d’historisation, seule la dernière version du fichier est conservée.
- L’espace de travail « WORK »
  Il s’agit d’un espace sécurisé haute performance dédié au calcul. Les données qui s’y trouvent ne sont pas sauvegardées et ne doivent idéalement y séjourner que le temps des opérations de calcul.

Acteurs et garanties

Les services du Centre de Calcul 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.

Le Centre de Calcul est le seul acteur du traitement des données.

Acteur	Rôle	Certifié HDS	Qualifié 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
Centre de Calcul	Hébergeur	Non (au 1/4/25)	Non	1 à 4	Non	Non

Enjeux externes et internes

Enjeux externes

Les enjeux externes sont répertoriés ici selon la méthode PESTEL.

Enjeu Politique

Le recours à des moyens de calcul publics est une réponse appropriée à la demande de souveraineté numérique portée par les politiques nationale et européenne.

Enjeu Économique

Les usagers du centre de calcul sont essentiellement des acteurs publics de la recherche et du soin, pour lesquels le coût modéré du service du Centre de Calcul est un argument important.

Enjeu Sociologique

La protection des données personnelles est devenue une attente forte de la population. L'Université bénéficie à ce titre d'une image positive quant à ses objectifs (elle ne va pas chercher à valoriser les données), mais faible quant à ses capacités (elle n'a pas forcément les moyens d'une gestion rigoureuse de la sécurité). La certification permettrait de combattre cette perception.

Enjeu Technologique

Les capacités technologiques des GAFAM sont sans commune mesure avec celles du CCUB. Celles-ci doivent rester à un niveau suffisant pour que les autres enjeux soient déterminants dans le choix de ses usagers.

Enjeu Environnemental

La plupart des marchés publics intègrent désormais des exigences de sobriété numérique. Celles-ci sont peu compatibles du recours au calcul massif que les usagers viennent rechercher auprès du CCUB. Toutefois le recours à un centre de calcul fédéré reste bien plus efficace énergétiquement que l'usage de moyens locaux.

Enjeu Légal

L'activité d'hébergement de données de santé est encadrée par le Code de la Santé Publique (article L1111-8), la certification visée est destinée à répondre à cet enjeu légal.

L'Université de Bourgogne est soumise au décret 2022-513 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Dans ce cadre elle doit appliquer l'instruction interministérielle n°901 relative à la protection des SI sensibles.

Enjeux internes

Enjeu de réputation

L'obtention de certifications 27001 et HDS serait un atout pour le centre de calcul dans la démonstration de sa capacité à protéger tant les données primaires confiées par ses usagers que les processus de calcul et les résultats obtenus, en appui à la démarche de protection du potentiel scientifique et technique de l'Université.

Enjeu de résilience

La mise en œuvre d'un système de management formalisé renforce par ailleurs la structuration du fonctionnement quotidien du CCUB, bénéfique pour sa résilience, le confort de fonctionnement pour ses personnels, l'évaluation et l'amélioration de sa performance.

Enjeu d'attractivité

Les personnels susceptibles d'être attirés par la technicité des solutions déployées par le Centre de Calcul sont a priori peu favorables à la formalisation des processus, perçue comme bureaucratique et chronophage. Il est important dans la mise en œuvre du SMSI de renforcer sa valeur perçue (amélioration continue des performances) et de minimiser les impacts opérationnels (automatisation, inscription dans les processus opérationnels habituels).

Attentes des parties intéressées

Attentes des usagers

Les responsables de traitement portant sur des données de santé à caractère personnel ne peuvent recourir qu'à des hébergeurs certifiés HDS.

Dans le cas de calcul relevant de la prise en charge médicale, les enjeux de confidentialité et d'intégrité sont évidemment essentiels, mais également ceux de disponibilité, sachant que :

- Les données primaires issues des séquenceurs à haut débit sont trop volumineuses pour être stockées sur leur site de production et le centre de calcul en détient donc l'unique exemplaire.
- L'indisponibilité des outils de calcul ou des résultats en temps voulu peut entraîner un retard de prise en charge, une augmentation du nombre des examens complémentaires ou avoir des conséquences graves pour le patient, par exemple l’impossibilité de réaliser ou de prendre la décision de réaliser une IMG avant terme et les risques juridiques associés.

Enfin, les données médicales portées par des machines virtuelles bénéficieront du niveau de protection certifié.

Dans les cas de calcul pour la recherche, même si les conséquences d'une indisponibilité sont moins graves, les moyens de calcul sont une ressource indispensable à l'exécution de la mission de l'utilisateur, et leur indisponibilité prolongée serait considérée comme un incident majeur.

Outre la fonction de calcul, le Centre de Calcul assure un stockage pérenne des données des utilisateurs, que ce soient leurs chaînes de traitement (données de configuration) ou leurs résultats (données finales et archivées). La disponibilité et l'intégrité de ces données pérennes sont également des engagements du CCUB.

Attentes des personnels

Les personnels attendent :

- une expression claire de leurs obligations et responsabilités afin d'éviter des fautes envers les objectifs de sécurité de l'information de l'organisation.
- des moyens techniques et organisationnels leur permettant de remplir ces responsabilités avec un minimum de charge administrative.
- des retours d'information sur les résultats de leur activité au service de la sécurité de l'information.

Attentes des intervenants

Les intervenants, qu'il s'agisse de sous-traitants ou de personnels des services généraux de l'Université, attendent également une expression claire de leurs obligations et responsabilités. Celle-ci peut prendre la forme de contrats (pour les sous-traitants) ou de procédures d'intervention explicites et communiquées.

Attentes de l'Université

L'Université déploie une organisation globale de sécurité de l'information respectueuse du cadre légal et réglementaire, dans laquelle doit s'inscrire le SMSI du CCUB.

Objectifs de sécurité

Objectifs stratégiques

On attend du système de management qu'il contribue aux enjeux et attentes suivants:

1. Souveraineté numérique (enjeu politique)
2. Disponibilité des moyens de calcul (attente des usagers)
3. Intégrité et disponibilité des données pérennes (attente des usagers), dont les données de santé à caractère personnel (DSCP)
4. Confidentialité des données personnelles (enjeux sociologique et légal, attente des usagers), dont les DSCP.
5. Obtention de la certification HDS et de l'homologation de sécurité (enjeu légal)
6. Réputation de maîtrise du Centre de Calcul (enjeu de réputation). L’objectif stratégique du centre de calcul est d’afficher un niveau de protection de l’information compatible de tous les usages potentiels, qu’ils soient dans le domaine de la santé ou dans d’autres domaines sensibles.
7. Confort de fonctionnement pour les personnels et les intervenants via des responsabilités et des instructions claires (enjeu de résilience, attente des personnels et des intervenants)
8. Évaluation et amélioration de la performance (enjeu de résilience, attente des personnels)
9. Cohérence avec le cadre légal et réglementaire (attente de l'Université)

Objectifs opérationnels

Les objectifs opérationnels se déclinent en:

- Des objectifs de conformité, liés à la maîtrise par le Centre de Calcul de ses actions et de ses moyens
- Des objectifs de performance dans le service rendu aux utilisateurs

Ils se rattachent aux objectifs stratégiques comme suit:

Objectif stratégique	Conformité	Performance
1 - Souveraineté numérique	X	
2 - Disponibilité des moyens de calcul		X
3 - Intégrité et disponibilité des données pérennes et DSCP		X

Objectif stratégique	Conformité	Performance
4 - Confidentialité des données personnelles et DSCP	X	
5 - Certification et homologation	X	
6 - Réputation de maîtrise du Centre de Calcul	X	X
7 - Responsabilités et instructions claires	X	
8 - Évaluation et amélioration de la performance		X
9 - Cohérence avec le cadre légal et réglementaire	X	

Objectifs de conformité

La conformité est assurée par la définition correcte et le fonctionnement régulier du SMSI:

La définition correcte est attestée par:

- les audits de conformité, pouvant éventuellement mener à des relevés de non-conformités

Le fonctionnement régulier est attesté par:

- La régularité dans la tenue du planning et des contenus des réunions de pilotage et des audits
- La tenue des échéances programmées des actions de remédiation ou d'amélioration

Objectifs de performance

L'objectif de disponibilité est évalué selon deux indicateurs:

- Le temps d'arrêt du service de calcul dans son ensemble, qui doit être inférieur à 5% par année.
- le taux de disponibilité des cœurs de calcul existants, qui doit rester au dessus de 80%

L'objectif de capacité est évalué directement par le temps moyen passé en file d'attente par les travaux avant exécution, qui doit être inférieur à 1 semaine.

Il est aussi apprécié indirectement par la capacité résiduelle et la résilience des moyens de maintien en condition opérationnelle:

- l'alimentation et le secours électrique
- la production de froid

L'objectif de disponibilité et d'intégrité des données pérennes est évalué au travers de:

- l'exécution quotidienne correcte des opérations de sauvegarde
- la validation de leur contenu à l'occasion de tests réguliers

La fiabilité des fournisseurs de systèmes ou de services, qu'ils soient internes (services de l'UB) ou externes, contribue également à tous les objectifs de performance. Elle est évaluée par une revue annuelle.

Risques et opportunités

S'assurer que le système de management peut atteindre les résultats escomptés

Le système de management contribue aux objectifs stratégiques comme suit:

Objectif stratégique	Contribution du SMSI
1 - Souveraineté numérique	L'existence même du Centre de Calcul contribue à la souveraineté numérique, dans la mesure où les usagers choisiront de recourir à ses services plutôt qu'à des offres commerciales extra-européennes. C'est donc la réputation et la performance améliorées par le fonctionnement du SMSI qui y contribueront.
2 - Disponibilité des moyens de calcul	L'analyse de risque considère les scénarios portant sur les moyens de calcul et permet de déterminer les mesures adéquates de mitigation. Le SMSI inclut la vérification de l'efficacité de ces mesures.
3 - Intégrité et disponibilité des données pérennes et DSCP	L'analyse de risque considère les événements redoutés d'indisponibilité ou de corruption sur toutes les classes d'information et permet de déterminer les mesures adéquates de mitigation. Le SMSI inclut la vérification de l'efficacité de ces mesures.
4 - Confidentialité des données personnelles et DSCP	Le Centre de Calcul n'a pas connaissance a priori de l'inclusion de données personnelles dans les jeux de données qu'il traite. Dans la démarche d'analyse des risques, on traitera toutes les données primaires ou celles résultant des calculs comme potentiellement personnelles.
5 - Certification et homologation	L'objet même du SMSI est d'obtenir la certification HDS pour le traitement des données de santé. Le soutien à l'homologation de sécurité en sera un bénéfice collatéral. Toutefois, la certification HDS se fera sur le nouveau référentiel, permettant de s'appuyer sur l'ISO 27001:2022, dès lors que celui-ci sera applicable. Ceci crée une fenêtre entre la certification 27001 et la certification HDS durant laquelle la conformité légale ne sera pas encore atteinte.
6 - Réputation de maîtrise du Centre de Calcul	Le Centre de Calcul est aujourd'hui pionnier parmi les centres de calcul publics pour cette démarche de certification. L'expérience acquise pourra être alors partagée avec les autres mésocentres. Par ailleurs, le partage avec les usagers d'indicateurs de fonctionnement clairs avec des engagements contractualisés est également un facteur de confiance.
7 - Responsabilités et instructions claires	L'expression des responsabilités et de leurs limites inhérente à la formalisation des processus sécurise les personnels et les intervenants.
8 - Évaluation et amélioration de la performance	Le suivi régulier des indicateurs opérationnels et la planification des actions en cas de dégradation, par exemple sur la capacité résiduelle de traitement, contribuent à l'amélioration de la performance.

Objectif stratégique	Contribution du SMSI
9 - Cohérence avec le cadre légal et réglementaire	Une étude spécifique a été effectuée pour s'assurer de la conformité du SMSI et des pratiques du Centre de Calcul avec la PSSI de l'Etat, matérialisée par l'instruction interministérielle n°901 .

Empêcher ou limiter les effets indésirables

Les effets indésirables, risques de lourdeur et de surcoût, sont couverts par un pilotage serré par les acteurs opérationnels et les usagers, regroupés dans un Comité de Pilotage du SMSI. Ils veillent notamment à :

- Minimiser les impacts opérationnels (enjeu d'attractivité, attente des personnels)
- Maintenir un niveau technologique approprié pour les usagers (enjeu technologique)
- Minimiser les surcoûts (enjeu économique)

Obtenir une démarche d'amélioration continue

Le pilotage du SMSI est guidé par l'analyse des risques. Notamment, lors de chaque réunion du COPIL SMSI, elle est réexaminée au regard des incidents, dérives d'indicateurs, non-conformités au cours du trimestre écoulé. Les niveaux de risque et/ou la mise en œuvre des mesures de sécurité peuvent alors être révisés, avec la création d'actions planifiées de déploiement ou de renforcement des mesures.

Des actions spontanées d'amélioration peuvent être également programmées par le COPIL SMSI et rentrent dans le suivi des actions.

Gouvernance de la sécurité de l'information

Organisation

Un Comité de Pilotage du SMSI (CoPil SMSI) est mis en place, qui réunit les rôles suivants:

- La directrice de la Direction du Numérique
- Le responsable du Centre de Calcul
- Le directeur technique du Centre de Calcul
- Le chargé d'exécution du SMSI
- Un représentant des usagers

Le CoPil SMSI pilote le fonctionnement du SMSI et en rend compte auprès du Comité de Pilotage de la Sécurité de l'Information de l'Université.

Il se réunit au moins selon une périodicité trimestrielle, les premières semaines de mars, juin, septembre et décembre. En dehors de ces réunions planifiées, le CoPil SMSI peut se réunir pour traiter des événements exceptionnels: intégration d'un nouveau projet présentant des spécificités de sécurité, modification des exigences réglementaires, survenue d'incidents graves, etc.

Les personnels du Centre de Calcul gèrent au quotidien la sécurité des services hébergés dans le respect des procédures d'exploitation. Le chargé d'exécution du SMSI valide les écarts à ces procédures sur la base d'une analyse des risques spécifiques, les documente et en rend compte au CoPil SMSI. Il propose les mesures et développements complémentaires éventuellement nécessaires pour l'amélioration de la politique de sécurité.

Le CoPil SMSI est globalement responsable du SMSI. Il valide la politique de sécurité et le plan de traitement des risques, et pilote leur déclinaison en actions. Il gère la communication auprès des usagers sur la mise en place et l'entretien du SMSI.

Gestion des risques

Classification de l'information

Les classes d'informations sont celles identifiés dans le domaine d'application :

- Données primaires
- Données de configuration
- Données de référence
- Données finales (résultats de calcul)
- Données archivées
- Dossiers patients (données des machines virtuelles)

Les données primaires, finales et archivées sont toutes susceptibles d'être des DSCP. L'appréciation des gravités des événements redoutés est établie en conséquence.

Événements redoutés

Les critères de sécurité retenus sont :

- La disponibilité des informations au moment où elles seraient nécessaires
- L'intégrité des informations
- La confidentialité des informations
- L'auditabilité, comprise comme l'imputabilité à des personnes physiques des accès aux informations

Les événements redoutés sont les pertes d'un critère sur une classe d'information. Leurs gravités ont été évaluées au regard de la classification proposée par la Haute Autorité de

Santé comme suit:

Classe	Disponibilité	Intégrité	Confidentialité	Auditabilité
Données primaires	Majeur	Majeur	Critique	Significatif
Données de configuration	Majeur	Majeur	Mineur	Sans impact
Données de référence	Significatif	Significatif	Sans impact	Sans impact
Données finales	Majeur	Critique	Critique	Significatif
Données archivées	Mineur	Majeur	Critique	Significatif
Dossiers patients	Majeur	Critique	Critique	Majeur

Appréciation du risque

L'appréciation des risques est fondée sur l'évaluation:

- De la gravité en cas de survenue de l'événement redouté
- De la vraisemblance de cette survenue, compte tenu des différents scénarios susceptibles de mener à l'occurrence de l'événement redouté.

Trois niveaux de risque sont identifiés: prioritaire, à surveiller et acceptable, et attribués comme suit:

G/V	Très improbable	Très peu probable	Peu probable	Possible/Probable	Très probable
Catastrophique	A surveiller	Prioritaire	Prioritaire	Prioritaire	Prioritaire
Critique	Acceptable	A surveiller	Prioritaire	Prioritaire	Prioritaire
Majeur	Acceptable	A surveiller	A surveiller	Prioritaire	Prioritaire
Significatif	Acceptable	Acceptable	A surveiller	A surveiller	Prioritaire
Mineur	Acceptable	Acceptable	Acceptable	Acceptable	A surveiller

Traitement des risques

Les risques de niveau Prioritaire ne sont pas acceptables et doivent faire l'objet d'une décision de traitement, visant à en réduire la vraisemblance.

Les risques de niveau A surveiller peuvent être acceptés sous justification. Cette règle pourra être durcie ultérieurement au titre de l'amélioration continue.

A niveau de risque équivalent, la priorité de traitement va au risque présentant la gravité la plus élevée.

Un plan de traitement des risques est tenu à jour.

Gestion des incidents de sécurité

Les événements susceptibles d'être des incidents de sécurité sont notifiés par mail à l'adresse incidents.hds@u-bourgogne.fr ou par la création d'un ticket de service. Les événements notifiés par mail feront également l'objet d'un ticket.

Tous les événements portant sur la confidentialité des données sont considérés comme des incidents de sécurité.

Les événements portant sur l'intégrité ou la disponibilité sont considérés comme des incidents de sécurité uniquement s'ils sont imputables au CCUB. Par exemple, une indisponibilité résultant d'une erreur de manipulation d'un utilisateur ou d'une défaillance de son fournisseur d'accès ne sera pas classé comme incident de sécurité.

Le niveau d'urgence des incidents est basé sur la gêne occasionnée pour les utilisateurs :

- **Basse** - Le problème peut être contourné sans difficulté ou n'entraine aucun risque significatif (exemple - une opération échoue immédiatement et doit être répétée pour aboutir)
- **Moyenne** : Le problème est gênant pour effectuer les tâches requises ou présente un risque de sécurité potentiel (exemples: déconnexions intempestives, une sauvegarde n'est pas effectuée en temps utile)
- **Haute** : Le problème empêche d'effectuer certaines tâches ou présente un risque de sécurité avérée. Il touche une part significative des utilisateurs.
- **Critique** : Le problème interdit le fonctionnement ou présente un risque de sécurité certain (exemples : site inaccessible, accès à un port inapproprié ouvert sur Internet)

Le niveau de priorité d'un incident détermine son mode de traitement, ainsi que le délai au bout duquel l'outil de ticketing escaladera vers l'ensemble des membres du COPIL SMSI :

Délais/Priorités	**Basse**	**Moyenne**	**Haute**	**Critique**
Prise en compte	3 jours	3 jours	2 jours	6 heures
Résolution	14 jours	7 jours	5 jours	2 jours

Les délais indiqués sont en heures et jours ouvrés.

Le Centre de Calcul communique avec les usagers impactés sur l'avancement de la résolution:

- Au moins une fois par jour ouvré pour les incidents de niveau haut.
- Toutes les deux heures pour les incidents de niveau critique.

Les incidents survenus enrichissent l'analyse et le plan de traitement des risques.