☐ Nom de la base	Résultat d'évaluation projet Poppy Éducation (1) Parcourt scolaire (2)
☐ Objectif de cette base (finalité du traitement)	Stocker des données particiellement anonyme, pour analyse statistique à des fin de recherche, les données sont receuillie via la plateforme de sondage en ligne sécurise de Inria (1). Stocker des données particiellement anonyme, pour les croiser avec la base "Résultat d'évaluation projet Poppy Éducation", les données sont transférer par l'établissement partenaire (2). La population regroupe des enseignants volontaire (non anonyme) issu d'établissement scolaire lier par une convention de partenaria avec le projet Poppy Éducation ; ainsi que leur élèves identifié par leur numéro d'étudient (1&2)
☐ responsable de la base	Thibault Desprez, doctorant et responsable de la partie évaluation du projet Poppy Éducation
☐ responsable(s) technique(s)	Thibault Desprez, Théo Segond (ingénieur du projet Poppy Éducation)
☐ personnes ayant accès aux données en lecture	Thibault Desprez, Pierre-Yves Oudeyer (directeur équipe FLOWERS & responsable projet Poppy Éducation), Théo Segond
☐ personnes ayant accès aux données en écriture	Thibault Desprez
☐ date de mise en service	01/09/2017
☐ Description de la méthode pour informer les utilisateurs du traitement de ces données et de leur caractère personnel.	Le doctorant, via "un concentement éclairé" à signer, spécifie que l'étude est partiellement anonymisée ; que les données ne serons utiliser qu'à des fin de recherche ; que les données brut serons conservé après l'étude mais que les données d'identification (nom, prénom et adresse mail pour les enseignants ; numéros d'étudient pour les élèves) seront suprimé dès la fin de l'étude. (1&2)
☐ Description de la méthode pour permettre aux utilisateurs de consulter leurs données.	Les données ne sont pas directement accéssible, l'utilisateur doit contacter le doctorant pour les obtenirs (1&2)
☐ Description de la méthode pour permettre aux utilisateurs de modifier/supprimer leurs données (le cas échéant).	Si un élève ou un enseignant souhaite se retirer de l'étude ils doivent contacter le doctorant qui les retirera de la base à tout moment (1&2).
☐ Demande d'autorisation à l'utilisateur pour insertion des données nominatives (et si oui, lesquels)	Autorisation demandé via "un concentement éclairé" signé. La population d'enseignants, fournie nom et prénom ; la population d'élèves fournie sont numéro d'étudient. (1&2)
☐ Description de la méthode pour protéger les données	Serveur sécurisé Inria (1) Fichier local, protégé par un mot de passe (chiffrement AES-256) (1&2)
☐ Base déjà déclarée à la CNIL (numéro identifiant) ?	Non
☐ Eléments les plus caractéristiques	Enseignant: Nom, prénom, adresse mail, age, sexe, niveau d'étude, expérience professionelle, ancienneté dans l'établissement. Élève: Numéro étudient, age, sexe, établissement scolaire d'affectation, classe. Plus données d'étude non personnel : questionnaires d'utilsabilité, de satisfaction, de motivation, de connaissance, suite à l'utilisation du matériel mis à disposition (1) Élèves: apprésiation/observation de ses enseigants, bulletins scolaires, taux d'absentéisme, redoublement/ré-orientation (2)

☐ Stockage ou Transmission hors europe	Non
☐ Stockage ou transmission à un autre pays européen	Non
☐ Délai de conservation des données	Cinq ans
☐ Mention CNIL	Oui sur le formulaire de consentement : la mention précise les modalités d'exercice des droits d'accès, de modification et de suppression et qui indique que le traitement est conforme à la règlementation.
☐ Remarques	
☐ Date de la déclaration	août-17
☐ Adéquation des données avec la finalité, la durée, les mesures de sécurité, etc	

~~*Indiquez le centre ou le service de la DSI*~~*CRI Bordeaux - Sud-Ouest*

Auteur : ~~*Indiquer l'auteur du dossier*~~Aurélien Dumez

~~*SICIndiquez le service*~~

Date : 27/11/2017

Objet :

Dossier d'homologation - Flowers

Analyse écologique et expérimentale

des usages de la robotique à l'école

en terme de motivation et de connaissances ~~de XXX~~

Diffusion Limitée

Nature *: Version de travail*

Destinataires *: liste exhaustive des destinataires*

Diffusion *: Diffusion limitée aux destinataires*

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

Pièces jointes :

- ***Tous documents utilisés pour l'analyse de risque afin de constituer le dossier d'homologation. Dans la mesure du possible, celui-ci doit être « autoporteur » et éviter des références à des documents en lige (les joindre en version PDF, par exemple)***

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

Contexte

Base de travail

~~Indiquer ici la façon dont s'est déroulée l'homologation et les documents utilisés pour faire l'analyse, les réunions qui ont été organisées, etc...~~Réunion de travail : 31 août 2017 – T. Desprez, A. Dumez – documents : présentation du projet

Réunion de travail

Indiquer s'il y a eu une réunion de travail avec la MOA et/ou MOE, les noms des participants. Il peut y avoir plusieurs réunions.

Description du service

Description fonctionnelle du service

~~Décrire le service en indiquant quelles sont les différentes parties prenantes, quel est le cheminement des données, etc...~~L'expérimentation porte sur l'évaluation de l'impact du dispositif Poppy Éducation dans les établissements scolaires. En particulier, l'étude s'intéresse aux progrès réalisés par les élèves, aux difficultés rencontrées par les enseignants et/ou leurs élèves pour réaliser les exercices proposés. La finalité est d'affiner la méthode pédagogique mise en œuvre lors de l'utilisation des kits de robotique dans les établissements.

Le service concerne le transfert et le stockage sécurisé des données recueillies auprès des établissements scolaires (réponses aux questionnaires, bulletins scolaires).

Description de l'architecture technique mise en œuvre

Les questionnaires adressés aux enseignants et à leurs élèves sont hébergés sur la plateforme Sondages d'Inria (https://sondages.inria.fr/).

~~Décrire l'architecture technique mise en œuvre, où sont hébergées les données, si le service est internalisé, externalisé, s'il y a des serveurs physiques, des serveurs virtuels, une description du réseau de stockage, etc~~Les données recueillies auprès des établissements scolaires sont stockées sur la plateforme Partage d'Inria (https://partage.inria.fr/).

Moyens humains dédiés à l'administration

Indiquer ici les moyens humains dédiés à l'administration de la solution. À la fois au niveau fonctionnel (MOA) que technique (MOE).

Si applicable, indiquez la durée des contrats des personnes en charge de l'administration.

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

Expression des besoins de sécurité

Données manipulées

Les données recueillies et manipulées sont :

- les réponses aux questionnaires adressés aux enseignants et à leurs élèves
- les bulletins scolaires des élèves participant à l'expérimentation

Une charte de partenariat avec les établissements scolaires sera établie afin de fournir le même niveau d'information à chaque établissement, ainsi qu'à chaque personne impliquée dans le projet (y compris leur hiérarchie proche). Par ailleurs, cette charte devra présenter la procédure d'anonymisation des données recueillies.

Au niveau des établissements, le logiciel Pronote (https://fr.wikipedia.org/wiki/Pronote) est souvent mis en œuvre. Cet outil permet notamment une extraction des seules données utiles, tout en garantissant dès l'extraction l'anonymat des élèves.

L'anonymisation repose sur l'utilisation du numéro d'Identification Nationale des Étudiants (INE). Les bulletins ne devraient comporter que ce numéro et c'est lui qui est demandé aux élèves lorsqu'ils répondent aux questionnaires. Il convient de noter que l'anonymat peut facilement être levé par les enseignants ayant accès à la base de données des effectifs de l'établissement.~~Décrire ici les besoins de sécurité pour les données manipulées.~~

Voici une caractérisation des besoins de sécurité des données manipulées. La classification du caractère identifiant et du caractère préjudiciable des données se base sur la classification introduite par la CNIL et décrite en annexe.

Décrire ici l'événement redouté auquel correspond la colonne « caractère préjudiciable ». Il s'agit en général de la diffusion de la donnée

Donnée	Caractère identifiant	Caractère préjudiciable	Disponibilité	Intégrité	Confidentialité	Traçabilité
~~Donnée 1~~Réponses aux questionnaires	Limité~~Maximal~~	Négligeable	Moyen	Important	~~Moyen~~Moyen	Important~~Moyen~~
~~Donnée 2~~Bulletins scolaires	Maximal~~Limité~~	Maximal~~Limité~~	Moyen	Important	Maximal~~Moyen~~	Maximal~~Moyen~~

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

Service

Le transfert des données s'effectue depuis les établissements scolaires vers Inria. Ce transfert doit garantir l'intégrité des données et l'identification de leur source. Par ailleurs, un établissement ne doit jamais avoir accès aux données envoyées par un autre établissement.

Le stockage des données doit être effectué dans un environnement fiable et sécurisé. Tout accès doit être contrôlé, notamment par identification des personnes habilitées à accéder à ces données. Les comptes d'accès seront nominatifs.

~~*Décrire ici le besoin de sécurité concernant le service. Il est généralement lié aux besoins de sécurité sur les données (max du tableau dans le § ci-dessus pour chaque colonne), mais pas nécessairement. Ex : un service peut avoir un besoin de disponibilité important pour des raisons liées à l'image.*~~

Service	Disponibilité	Intégrité	Confidentialité	Traçabilité
~~Composant 1~~Transfert des données	Moyen	Important	Important	Important
~~Composant 2~~Stockage des données	Moyen	Moyen	Maximal	Maximal

Scénarios de menace

Lister les différents scénarios de menace envisagés. Quelques exemples pour trouver des scénarios :

- *Demander aux représentants de la MOA ce qu'elle « craint », ce qui est « redouté » (en général ils le savent)*
- *Suivre pas à pas le cheminement des données. S'interroger sur des possibilité d'intrusion ou d'interception à chaque étape*
- *S'interroger sur des attaques sur les postes de travail des utilisateurs de la solution (virus, chevaux de Troie)*
- *Éventuellement s'interroger sur la résistance de la solution à un utilisateur malveillant*

1. *Interception des données pendant leur transfert*~~*Scénario 1*~~
2. *Accès non autorisé aux données*~~*Scénario 2*~~

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

3. ~~Scénario 3~~

Chaque scénario est examiné et son impact évaluée (agent, Inria).

On essaie d'envisager tous les moyens imaginables pour empêcher que le scénario puisse se produire (mesures de prévention), pour le détecter s'il se produit (mesures de détection) et les mesures à prendre s'il est détecté (réponse).-

~~et~~ Ensuite, on vérifie si l'architecture ~~si~~ les processus prévus permettent de limiter les risques identifiés. Dans la négative, on propose des évolutions du processus afin de limiter le risque.

In fine, on évalue les risques résiduels.

Scénario 1 : interception de données

Impact ~~Agent~~ Individu : ~~évaluation de l'impact pour un agent individu (voir tableau CNIL en annexe) dans le cas où le scénario imaginé se produirait~~si l'interception porte sur le bulletin de notes, l'impact est maximum, l'image de l'individu concerné peut être atteinte.

Impact Inria : ~~évaluer l'impact pour Inria, il n'est pas nécessairement le même que pour un agent.~~perte de confiance des établissements partenaires et atteinte à l'image d'Inria

Analyse d'impact : en fonction des évaluations d'impact ci-dessus indiquer si le scénario doit être couvert par la solution ou si c'est souhaitable ou si ce n'est pas nécessaire.

Description du scénario ~~de menace. Décrire en quelques phrases en quoi consiste le scénario de menace.~~ : au cours d'un transfert de données depuis les établissements scolaires vers Inria, il y a interception (MitM, par exemple) des données.

Mesures permettant de traiter le scénario de menace.

~~*Lister ici l'ensemble des mesures auxquelles on pense pour éviter que le scénario envisagé ne se produise (prévention), pour le détecter s'il se produit (détection) et les actions ou mesures à envisager dans le cas où il serait détecté (réponse).*~~

Type de mesures	Mesures
Prévention	Utiliser des outils institutionnels (pas Google)
Détection	Mise en œuvre d'un protocole d'accusé de réception du transfert des données. Si utilisation de partage, l'utilisation d'un workflow peut aider à atteindre ce but.

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

Type de mesures	Mesures
Réponse	Information immédiate des partenaires, des acteurs de la SSI chez Inria et suspension du transfert de données avec tous les établissements. Évaluation la plus précise possible des données interceptées. Aucune reprise sans aval du RSSI

~~et analyse~~ Analyser ~~des~~ les éléments ***actuels*** de la solution qui ~~permettent d'éviter qu'il se produise ou qui sont de nature à diminuer la probabilité d'occurrence ou l'impact si le scénario se produit.~~implémentent les mesures envisagées ci-dessus en prévention, détection, réponse.

Les mesures peuvent être :

- *Des processus (faire telle chose de telle façon), des consignes (changer le mot de passe tous les XX semaines)*
- *Des mesures de confinement physique (locaux fermés), d'habilitation (décision formelle de donner accès à…)*
- *Des mesures de confinement logique*
- *Des solutions d'architecture SI*
- *Des outils de détection*
- *etc*

Scénario 2 : accès non autorisé aux données

Impact Individu : maximal notamment si les données récupérées sortent de chez Inria. L'image de l'individu peut être atteinte.

Impact Inria : perte de confiance des établissements partenaires et atteinte à l'image d'Inria si les données sont diffusées hors Inria.

Analyse d'impact :

Description du scénario de menace : une personne de l'équipe obtient un accès aux données de l'expérimentation (exemple : accès depuis un poste de travail non verrouillé)

Mesures permettant de traiter le scénario de menace.

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

Lister ici l'ensemble des mesures auxquelles on pense pour éviter que le scénario envisagé ne se produise (prévention), pour le détecter s'il se produit (détection) et les actions ou mesures à envisager dans le cas où il serait détecté (réponse).La solution envisagée pour le transfert doit s'appuyer sur des outils institutionnels reconnus (pas chez Google…). Ici, le site https://partage.inria.fr/ conviendrait parfaitement.

Type de mesures	Mesures
Prévention	Stocker les données sur un espace dont l'accès est finement contrôlé (outil permettant la gestion de l'authentification et de l'autorisation) Traiter les données sur des postes de travail sécurisés (chiffrement du disque dur) et exploités selon de bonnes pratiques (mot de passe de session, verrouillage session si absence, même de courte durée).
Détection	
Réponse	Informer les acteurs de la SSI chez Inria.

*et analyse Analyser des les éléments **actuels** de la solution qui implémentent les mesures envisagées ci-dessus en prévention, détection, réponse.*

Les mesures peuvent être :

- *Des processus (faire telle chose de telle façon), des consignes (changer le mot de passe tous les XX semaines)*
- *Des mesures de confinement physique (locaux fermés), d'habilitation (décision formelle de donner accès à…)*
- *Des mesures de confinement logique*
- *Des solutions d'architecture SI*
- *Des outils de détection*

etc

~~*Idem pour le scénario 2*~~

Scénario 3

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

Idem pour le scénario 3

Informatique et Liberté

Si la solution manipule des données à caractère personnel, ce § est à traiter en lien avec le Relais Informatique et Libertés du centre ou avec le Correspondant Informatique et Libertés.

Information préalable des personnes

~~*Vérifier que les personnes dont les données sont manipulées ont été préalablement informées et préconisations*~~*Chaque participant signe un formulaire de consentement éclairé.*

Proportionnalité et pertinence

~~*Est ce que les différentes données à caractère personnel sont proportionnelles à la finalité et pertinentes ?*~~*Le recueil de données à caractère personnel est strictement limité aux besoins de l'étude.*

Durée de conservation

~~*Quelle est la durée de conservation pour les données à caractère personnel*~~*Les données à caractère personnel sont conservées pendant 5 ans.*

Consultation et modification des données par les personnes

~~*Comment les personnes peuvent-elles accéder aux données les concernant ou les modifier ?*~~*Le formulaire de consentement éclairé précise que l'accès aux données se fait par email à l'adresse cil@inria.fr*

Opt-in / opt-out

~~*Est ce que les personnes se voient donner le choix d'accepter ou de refuser de participer au traitement ?*~~*Le formulaire de consentement éclairé mentionne le droit de ne pas participer à l'étude ou de la quitter sans préavis ni conditions.*

Anonymisation / cloisonnement

~~*Est ce qu'il serait possible d'anonymiser les DCP manipulées, est ce qu'il serait possible de cloisonner les DCP des autres données manipulées et de permettre que moins de personnes aient accès aux DCP, pour une expérimentation où sont conservés les formulaires de consentement ?*~~*La mise en place d'une anonymisation des données recueillies est prévue par l'expérimentation.*

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

Recommandations

~~Lister ici les différentes recommandations issues de l'analyse des scénarios ci-dessus afin de les rendre clairement visible. Indiquer le caractère facultatif ou obligatoire de la recommandation ou les délais de mise en œuvre.~~

- Transfert et stockage des données : utilisation d'outils institutionnels
- Poste de travail : maintien à jour et bonne utilisation de la session utilisateur

Recommandation 1

Utiliser obligatoirement des outils institutionnels (ici https://partage.inria.fr/ convient)~~Indiquer ici la description de la recommandation.~~

Recommandation 2

Utiliser obligatoirement des postes de travail à jour (système d'exploitation + applications), dont le disque dur est chiffré. Respecter quelques bonnes pratiques en tant qu'utilisateur :

- ne pas utiliser ce poste pour d'autres activités que professionnelles
- garder le contrôle de sa session (pas de prêt à un autre utilisateur, verrouillage si absence)

~~Indiquer ici la description de la recommandation.~~

Risques résiduels

Indiquer ci-dessous la liste des risques résiduels. Il s'agit de risques identifiés qui ne sont pas traités. La probabilité d'occurrence du risque peut-être estimée faible ou le préjudice pour un individu ou Inria peut-être estimé comme faible.

Si les préjudices sont limités à important et la probabilité est significative, la raison pour laquelle le risque résiduel ne sont pas réduits peut-être le coût financier ou humain du traitement.

Si le préjudice est maximal, la probabilité ne peut-être que faible ou très faible et les raisons pour lesquelles le risque n'est pas réduit doivent être bien argumentés.

Risque	Probabilité	Préjudice pour individu	Impact pour Inria
~~Risque 1~~Perte des données (réponses sondage, bulletins de notes)	Faible	Nul	Faible
Risque 2			

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

~~Décrire ici les risques du tableau ci-dessus en utilisant des renvois.~~Le premier risque résiduel porte sur la perte des données suite à une erreur de manipulation ou une erreur technique. Il ne s'agit pas de vol. Seules les données issues de réponses à des sondages semblent difficiles à reconstituer. Les bulletins de notes peuvent toujours être récupérés sur l'outil ProNote.

Avis de sécurité

Avis de la DSI

Indiquer ici l'avis du Directeur du Système d'Information.

Avis du RSSI

Indiquer ici l'avis du Responsable de la Sécurité du Système d'Information.

Avis de la commission d'homologation

Indiquer ici l'avis de la commission d'homologation.

Annexe A – Données à caractère personnel

Caractère identifiant des données

Le caractère identifiant de l'ensemble des DCP (précédemment identifiées) doit être estimé : avec quelle facilité peut-on identifier les personnes concernées ?

1. ***Négligeable** : il semble quasiment impossible d'identifier les personnes à l'aide des DCP les concernant (ex. : prénom seul à l'échelle de la population française).*
2. ***Limité** : il semble difficile d'identifier les personnes à l'aide des DCP les concernant, bien que cela soit possible dans certains cas (ex. : nom et prénom à l'échelle de la population française).*
3. ***Important** : il semble relativement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom et date de naissance, à l'échelle de la population française).*
4. ***Maximal** : il semble extrêmement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom, date de naissance et adresse postale, à l'échelle de la population française).*

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

On retient la valeur dont la description correspond le mieux aux DCP identifiées. Des mesures existantes ou prévues peuvent avoir pour effet de réduire le caractère identifiant. Il convient alors de les mentionner en tant que justification.

Caractère préjudiciable d'un événement redouté

Le caractère préjudiciable doit être estimé pour chaque évènement redouté.

1. ***Négligeable** : les personnes concernées ne seront pas impactées ou pourraient connaitre quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement…).*
2. ***Limité**: les personnes concernées pourraient connaitre des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure…).*
3. ***Important**: les personnes concernées pourraient connaitre des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé…).*
4. ***Maximal**: les personnes concernées pourraient connaitre des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès…).*

On retient la valeur dont la description correspond le mieux aux impacts potentiels identifies. Des mesures existantes ou prévues peuvent avoir pour effet de réduire le caractère préjudiciable. Il convient alors de les mentionner en tant que justification.

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

Annexe B – Sécurité des données et des services

Sécurité des données

*La sécurité des données dépend de plusieurs critères, chacun traitant un aspect de la sécurité, qui sont la **disponibilité**, l'**intégrité**, la **confidentialité** et la **traçabilité**.*

La disponibilité

Ce critère reflète le besoin qu'une donnée soit accessible. Elle peut correspondre à la durée maximale acceptable pour avoir accès à la donnée ou à un taux de disponibilité (ex : 99 % du temps).

L'échelle de graduation suivante sera utilisée pour exprimer les besoins de sécurité d'une donnée en termes de disponibilité :

Besoin de sécurité	Description détaillée de l'échelle
Nul	*La donnée peut être indisponible au-delà de deux jours ouvrés.* [1]
Moyen	*La donnée doit être disponible dans les deux jours ouvrés.*
Important	*La donnée doit être disponible dans les 8 heures ouvrées.*
Haut	*La donnée doit être disponible dans les 4 heures*[2]*.*

L'intégrité

L'intégrité reflète le besoin que la donnée ne soit pas altérée. Elle correspond autant au niveau de conformité qu'à la stabilité, l'exactitude, la complétude, etc.

L'échelle de graduation suivante sera utilisée pour exprimer les besoins de sécurité d'une donnée en termes d'intégrité :

Besoin de sécurité	Description détaillée de l'échelle
Nul	*La donnée peut ne pas être intègre sans aucune conséquence.*
Moyen	*La donnée peut ne pas être intègre si l'altération est identifiée.*
Important	*La donnée peut ne pas être intègre, si l'altération est identifiée et*

1 *Heures et jours ouvrés : de 09h00 à 17h00 du lundi au vendredi, hors jours fériés.*

2 *L'organisation interne d'Inria ne permet pas d'atteindre ce niveau qui devrait être réservé aux applications externalisées avec un contrat de service adapté.*

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr

Besoin de sécurité	Description détaillée de l'échelle
	l'intégrité de la donnée retrouvée (par exemple depuis une sauvegarde)
Haut	*La donnée doit être rigoureusement intègre.*

La confidentialité

Ce critère reflète le besoin qu'une donnée[3] ne soit pas compromise ni divulguée. Il correspond au nombre ou catégories de personnes autorisées à y accéder.

L'échelle de graduation suivante sera utilisée pour exprimer les besoins de sécurité d'une donnée en termes de confidentialité :

Besoin de sécurité	Description détaillée de l'échelle
Nul	*La donnée est publique.* *Sa diffusion est sans impact pour la personne concernée ou pour Inria.*
Moyen	*La donnée ne doit être accessible qu'aux personnes autorisées.* *L'impact en cas de diffusion au-delà des personnes autorisées est faible pour la personne concernée ou Inria.*
Important	*La donnée ne doit être accessible qu'aux personnes autorisées.* *L'impact en cas de diffusion au-delà des personnes autorisées est important pour la personne concernée ou Inria.*
Haut	*La donnée ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.* *L'impact en cas de diffusion au-delà des personnes autorisées est critique pour la personne concernée ou Inria.*

La traçabilité

Ce critère reflète le besoin que l'accès à une donnée en soit connu et journalisé. Il correspond au type d'accès à la donnée.

L'échelle de graduation suivante sera utilisée pour exprimer les besoins de sécurité d'une donnée en termes de traçabilité :

Besoin de sécurité	Description détaillée de l'échelle
Nul	*Il n'est pas nécessaire d'identifier les accès à la donnée.*
Moyen	*L'accès à l'application (connexion) qui accède à la donnée doit être identifié.*

3 *S'il s'agit d'une donnée à caractère personnel, la divulgation de la donnée aura un impact à la fois pour la personne concernée et Inria.*

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

Besoin de sécurité	Description détaillée de l'échelle
Important	*L'accès à la donnée en écriture doit être identifié.*
Haut	*L'accès à la donnée en lecture et/ou écriture doit être identifié.*

Sécurité des services

La sécurité des services dépend de plusieurs critères, chacun traitant un aspect de la sécurité, qui sont la ***disponibilité****, l'****intégrité****, la* ***confidentialité*** *et la* ***traçabilité****.*

La disponibilité

Ce critère reflète le besoin qu'un service soit accessible. Il peut correspondre à la durée maximale acceptable pour avoir accès à la donnée ou à un taux de disponibilité (ex : 99 % du temps).

L'échelle de graduation suivante sera utilisée pour exprimer les besoins de sécurité d'un service en termes de disponibilité :

Besoin de sécurité	Description détaillée de l'échelle
Nul	*Le service peut être indisponible au-delà de deux jours ouvrés*[4]*.*
Moyen	*Le service doit être disponible dans les deux jours ouvrés.*
Important	*Le service doit être disponible dans les 8 heures ouvrées.*
Haut	*Le service doit être disponible dans les 4 heures*[5]*.*

L'intégrité

L'intégrité d'un service n'est pas évaluée en tant que telle. On prend le maximum du besoin d'intégrité des données manipulées.

La confidentialité

Ce critère reflète le besoin qu'un service ne soit pas compromis. Il correspond au nombre ou catégories de personnes autorisées à y accéder.

4 Heures et jours ouvrés : de 09h00 à 17h00 du lundi au vendredi, hors jours fériés.

5 L'organisation interne d'Inria ne permet pas d'atteindre ce niveau qui devrait être réservé aux applications externalisées avec un contrat de service adapté.

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30
www.inria.fr

L'échelle de graduation suivante sera utilisée pour exprimer les besoins de sécurité d'un service en termes de confidentialité :

Besoin de sécurité	Description détaillée de l'échelle
Nul	*L'accès au service est public.* *L'utilisation du service est sans impact pour Inria.*
Moyen	*Le service ne doit être accessible qu'aux personnes autorisées.* *L'impact en cas d'utilisation du service au-delà des personnes autorisées est faible pour Inria.*
Important	*Le service ne doit être accessible qu'aux personnes autorisées.* *L'impact en cas d'utilisation du service au-delà des personnes autorisées est important pour Inria.*
Haut	*Le service ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.* *L'impact en cas d'utilisation du service au-delà des personnes autorisées est critique pour Inria.*

La traçabilité

Ce critère reflète le besoin que l'accès à un service soit connu et journalisé. Il dépend du type d'utilisation du service.

L'échelle de graduation suivante sera utilisée pour exprimer les besoins de sécurité en termes de traçabilité :

Besoin de sécurité	Description détaillée de l'échelle
Nul	*Il n'est pas nécessaire d'identifier les accès au service.*
Moyen	*L'accès au service (connexion) doit être identifié.*
Important	*L'accès au service pour des actions conduisant à une modification des données manipulées doit être identifié.*
Haut	*L'accès au service ainsi que toutes les actions effectuées sur les données manipulées (lecture et/ou écriture) doit être identifié.*

Domaine de Voluceau - Rocquencourt BP 105
78153 Le Chesnay Cedex France
Tél. : +33 (0)1 39 63 55 11
Fax : +33 (0)1 39 63 53 30

www.inria.fr