

CCTP - ANNEXE

PLAN ASSURANCE SECURITE

Modèle type de Plan d'Assurance Sécurité Amue (annexe du CCTP)

06 FEVRIER 2024

VERSIONS DU DOCUMENT

Version	Date	Émetteur	Statut/Suivi des modifications
0.1	14/04/2017	Geoffrey Gaillard (Sogeti)	Création document
1.0	03/10/2017	Geoffrey Gaillard (Sogeti)	Finalisation document
2.0	10/06/2021	Cédric Servaes (Amue)	Compléments et mise en forme
2.1	05/02/2024	Cédric Servaes (Amue)	Revue et compléments (§2, §9.2)
2.2	16/12/2024	Cédric Servaes (Amue)	Mise à jour liens PSSIE / RGS

A noter : Une fois instancié, ce document confidentiel est à usage restreint et ne doit être diffusé qu'aux personnes ayant le besoin d'en connaître (personnels Amue et prestataires identifiés). Le document finalisé devra porter la mention :

Document Confidentiel



TABLE DES MATIERES

1. INTRODUCTION.....	3
1.1. Objet du document.....	3
1.2. Documents de référence	3
1.3. Responsabilités liées au PAS	3
1.4. Applicabilité du PAS.....	3
2. DESCRIPTION DU SYSTEME EXTERNALISE.....	4
3. ORGANISATION MISE EN PLACE CONCERNANT LES ASPECTS SECURITE.....	5
3.1. Le comité de suivi de la sécurité	5
3.2. Organisation Amue	5
3.3. Organisation du candidat	5
4. FORMATION.....	5
5. SOUS-TRAITANCE	6
6. RESPECT DU DROIT D'AUDIT DE L'AMUE.....	6
7. MESURES DE SECURITE	6
8. GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION	6
9. CONFIDENTIALITE	7
9.1. Clauses de confidentialité professionnelles	7
9.2. Classification de documents	7
10. RGPD.....	7
11. PROCEDURE D'EVOLUTION DU PAS	8
12. DOCUMENTATION DE SUIVI.....	8
13. CONTACTS	9
14. ANNEXES.....	9



1. Introduction

1.1. Objet du document

Ce document est modèle à personnaliser individuellement par chaque candidat. Son objectif est de décrire les dispositions que le candidat s'engage à mettre en œuvre pour répondre aux exigences de sécurité de l'Agence de Mutualisation des Universités et Etablissements, nommée AMUE dans la suite du document. Il définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet d'externalisation et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre.

Le candidat précisera le circuit d'approbation du Plan d'Assurance Sécurité, ses modalités d'application et l'étendue de sa diffusion

1.2. Documents de référence

Ce paragraphe liste les documents de référence pour le Plan d'Assurance Sécurité.

À titre d'exemple, les documents applicables peuvent être les suivants :

- Le contrat ;
- Le cahier des charges, incluant les exigences de sécurité de l'Amue ;
- Le plan d'assurance qualité ;
- Les normes et politiques de sécurité du candidat ;
- La Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) : <https://cyber.gouv.fr/cadre-de-gouvernance-de-la-securite-numerique-de-letat-pssie> ;
- Le Référentiel Général de Sécurité (RGS) : <https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs> ;
- Le Référentiel Général sur la Protection des Données (RGPD) : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679> ;
- Etc ...

1.3. Responsabilités liées au PAS

Le Plan d'Assurance Sécurité s'applique à :

- l'ensemble des équipes de la maîtrise d'œuvre
- aux sous-traitants éventuels.

Sa rédaction relève du responsable sécurité désigné par le candidat et doit être approuvé par l'Amue.

Toutes les équipes du candidat qui participent à la livraison des services au client sont tenues de lire et de comprendre le présent plan de gestion de la sécurité

1.4. Applicabilité du PAS

L'applicabilité du PAS s'articule autour des trois points suivants :

- Quelles sont les procédures à suivre lors de non-respect du PAS ?
- Quelle est la procédure à suivre pour une demande de dérogation ?
- Quelles sont les pénalités encourues ?

Le Plan d'Assurance Sécurité est applicable à l'ensemble des acteurs du projet, au même titre que le Plan d'Assurance Qualité et avec la même priorité.

Les éventuels sous-traitants du candidat, ainsi que tout personnel du candidat, ou de l'Amue identifiant un non-respect du PAS, dans ses procédures et mesures, doit en référer immédiatement à



son responsable. Un modèle type de rapport de non-respect sera annexé au PAS définitif, spécifiant la forme du rapport, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la clause de non-respect.

Si la cause du non-respect n'est pas corrigée dans un délai de <délai à estimer>, le candidat subira une pénalité suivant la formule : <formule à calculer>.

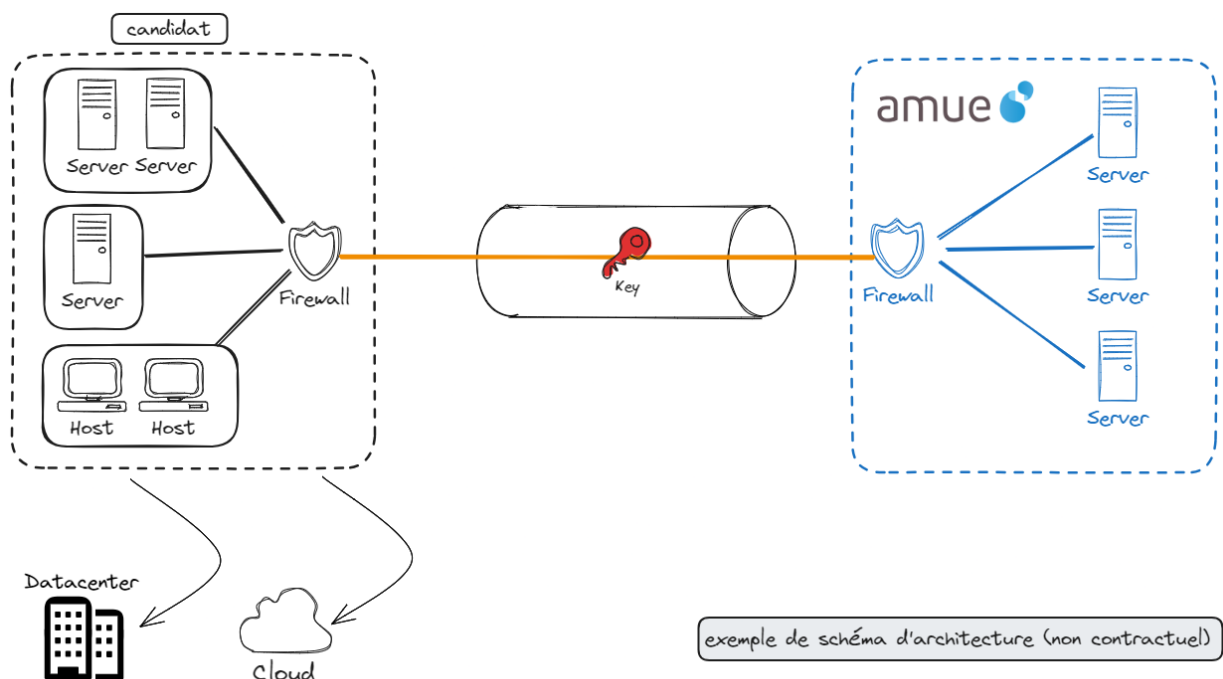
Un acteur du projet n'étant pas à même de remplir l'ensemble des clauses du PAS devra effectuer une demande de dérogation auprès du candidat, qui négociera avec l'Amue l'ensemble des demandes de dérogation. Un modèle type de demande de dérogation devra être disponible, spécifiant la forme de la demande, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la demande de dérogation.

2. Description du système externalisé

Ce paragraphe présente succinctement l'architecture d'interconnexion des systèmes d'information, les éléments de sécurité mis en œuvre, etc. en respect des règles de sécurité appliquées par l'AMUE et le Candidat.

L'accent sera mis sur les points qui justifient la mise en œuvre de mesures de sécurité particulières.

Le candidat présentera un schéma de principe de l'interconnexion entre les systèmes d'information :





3. Organisation mise en place concernant les aspects sécurité

3.1. Le comité de suivi de la sécurité

Le candidat décrit ici les objectifs du comité de suivi de la sécurité, le profil des participants, la fréquence, localisation et les livrables associés.

A titre d'exemple, les documents mis à disposition :

- Ordre du jour, support et relevé de décision ;
- Plan d'Assurance Sécurité mis à jour, le cas échéant ;
- Indicateurs et tableau de bord de suivi des engagements de sécurité ;
- Liste actualisée des personnels autorisés à réaliser les prestations ;
- Tout autres documents d'assurance de sécurité concernés ;
- Planning général et opérationnel détaillé mis à jour ;

3.2. Organisation Amue

L'Amue désigne un interlocuteur responsable de la sécurité du projet <nom du projet>. Cet interlocuteur unique a pour mission de faciliter les relations entre les différents intervenants et de mettre à disposition du candidat l'ensemble des documents nécessaire à la bonne prise en compte de la sécurité liée aux opérations d'externalisation.

3.3. Organisation du candidat

Le candidat désigne un interlocuteur responsable de la sécurité, pilotant l'ensemble de la sécurité du projet : sécurité des développements, sécurité du système d'information cible et intégration des composants sécurité.

Le responsable de la sécurité désigné par le candidat prend en charge l'organisation des comités de suivi sécurité : convocation, proposition d'ordre du jour, rédaction des comptes rendus. Il a l'obligation d'informer l'Amue de la sécurité du projet, les incidents apparus sur le système ou les évolutions du contexte opérationnel. Il est responsable de la diffusion du plan d'assurance sécurité et des documents de suivi.

4. Formation

Le candidat décrit ici les formations suivies par les personnes intervenant sur le marché (sensibilisation formations standards, formations spécialisées).

Les formations suivies par les profils développeur devront être précisées (exemple : formation OWASP).



5. Sous-traitance

Cette section présente les exigences en matière de sécurité de la gestion des tiers qui travaillent pour le candidat ou en son nom. Elle définit les obligations du candidat envers les tiers, les règles de sécurité qui régissent l'accès, par des tiers, aux locaux et aux actifs d'information du candidat, les contrôles de sécurité à la fois physiques et logiques des installations de traitement et de gestion de l'information.

Le candidat doit préciser les éléments de confidentialité, les éléments de sécurité à respecter par les tiers ainsi que les contrôles d'accès donnés aux tiers.

6. Respect du droit d'audit de l'Amue

L'Amue peut réaliser un audit des services fournis par le candidat pour s'assurer que les règles et les contrôles convenus dans le PAS sont appliqués.

7. Mesures de sécurité

Le candidat décrira les mesures destinées à assurer la sécurité du système cible de l'opération d'externalisation pendant les différentes phases contractuelles : phase de transfert, phase d'exploitation, phase de réversibilité ou fin de contrat.

Le candidat précise ici les règles d'accès aux sites, les mesures de sécurité apportées aux postes utilisateur.

Le candidat décrit les mesures de journalisation et de surveillance mises en place.

Le candidat décrit ici les processus et mesures mises en place pour assurer la surveillance des vulnérabilités et la mise en place des correctifs sur les actifs.

8. Gestion des incidents liés à la sécurité de l'information

Le candidat précise les procédures de réception, notification, résolution et documentation de tous les incidents ayant une incidence sur les activités opérationnelles de l'Amue.

La gestion des incidents vise à minima les objectifs suivants :

- Rétablir le service dans les plus brefs délais
- Limiter les conséquences sur les activités par une intervention et une résolution rapides
- Communiquer l'état de l'incident et l'avancement de sa résolution
- Tenir des dossiers d'incident précis
- Limiter l'incidence financière des incidents

Le candidat décrit ici les actions, les acteurs, les délais et moyens de communication dans les processus de traitement et d'escalade des incidents de sécurité.



9. Confidentialité

9.1. Clauses de confidentialité professionnelles

Le candidat décrit les modalités du respect de la confidentialité dans les contrats de travail.

9.2. Classification de documents

Le candidat utilise systématiquement la classification des documents de l'Amue sur tous les documents en relation avec l'Amue :

Niveau de sensibilité	Préjudice potentiel	Risque accepté (résiduel)	Mesure de protection (réduction du risque)	Exemple de donnée	Référentiels	Localisation de l'hébergement des données / accès aux données
Information publique (0)	Aucun préjudice	Pas de risque pour l'AMUE et ses adhérents	Aucune	- Plaquette de présentation produit - Vidéos marketing, promotionnels	- PSSIE - RGS - RGPD	- WorldWide si services non administrés par l'AMUE (exemple : YouTube, Twitter, ...) - Europe si services administrés par l'AMUE (DC dans les pays membres de l'UE/EEE) (gestion des données personnelles dans les fichiers journaux)
Diffusion contrôlée (1)	- Préjudice faible - Aucune incidence pour l'AMUE et ses adhérents	- Les risques sont pris en toute connaissance des conséquences par le propriétaire et les destinataires - Perte d'image	- Marquage des documents - Liste de diffusion interne et externe	- Documentation produit sur le site web - CCI (Cahier des Charges d'implantation) - Code source ouvert - Données à caractère personnel	- PSSIE - RGS - RGPD	Europe (DC dans les pays membres de l'UE/EEE)
Confidentiel AMUE (2)	- Préjudice grave (RGPD) - Conséquences graves avec incidences fortes sur l'AMUE et/ou ses adhérents	- Les risques doivent être limités et sont inacceptables pour les informations les plus sensibles - Perte financière	- Procédure de manipulation et de diffusion restrictives - Chiffrement des informations les plus sensibles - Marquage des documents	- Document de conception produit - Document de sécurité produit - Base de données établissement - Code source fermé	- PSSIE - RGS - RGPD - II 901 sur la protection des SI sensibles (partie 1) - Doctrine d'utilisation de l'informatique en nuage par l'État ("cloud au	France (DC ESR / fournisseurs Cloud français / infra AMUE)
Secret AMUE (3)	- Préjudice inacceptable - Conséquences graves - Condamnation	- Aucun risque ne peut être pris - Risques intolérables - Vol ou diffusion involontaire d'information entraînant une atteinte à la vie privée ou à la	- Personnes habilitées dans l'entreprise - Chiffrement des fichiers et des mails - Coffre-fort pour les documents électroniques - Marquage des documents	- Information établissement manipulée dans le cadre de l'assistance - Contrat - Dossier de R&D	- PSSIE - RGS - RGPD - II 901 sur la protection des SI sensibles (partie 1) - Doctrine d'utilisation de l'informatique en nuage par l'État ("cloud au	Infra AMUE uniquement

Le candidat décrit le système de classification des documents internes et fournira une table de correspondance avec les documents Amue.

10. RGPD

En fonctionnement normal, aucune ressource du candidat ne doit accéder, stocker ou divulguer des données personnelles de production.

Pour les besoins de base de formation ou de tests de masse (tests de performance ou de charge basées sur données issues des établissements), le candidat n'est pas autorisé à récupérer les données réelles des bases de production. L'anonymisation des données à caractère personnel avant transmission au candidat est mise en place par l'Amue.

Seule l'assistance à l'exploitation (consultation, enregistrement, transmission, extraction, effacement, destruction) constitue un cas d'accès aux données personnelles. Dans ce cas, le candidat demandera systématiquement l'autorisation écrite aux établissements avant intervention, via l'outil de ticketing Amue. Les données récoltées sont ensuite immédiatement détruites dès la fin de l'intervention.



11. Procédure d'évolution du PAS

En cas d'évolution du système, de son environnement, ou du périmètre des opérations d'externalisation, le candidat vérifie si le PAS doit être modifié. La cohérence de l'ensemble des mesures pourra être analysée et réévaluée lors des comités de suivi de la sécurité. Si tel est le cas, le candidat propose une modification à l'Amue. Si cette modification est acceptée, le PAS est révisé et soumis à l'Amue pour validation formelle.

Une révision du Plan d'Assurance Sécurité pourra être réalisée en cas d'évolution du périmètre de l'opération ou des exigences de l'Amue, après accord du candidat.

Voici une liste des situations susceptibles d'entraîner une modification du PAS :

- évolution du système d'information : configuration logicielle ou matérielle ;
- évolution de l'environnement du système d'information : locaux, personnels, procédures, etc. ;
- évolution du périmètre de l'opération.

Cette révision sera réalisée par le responsable sécurité désigné par le candidat. La version révisée du PAS sera transmise à l'Amue pour validation, et diffusée à l'ensemble des acteurs pour application.

12. Documentation de suivi

Le candidat recensera dans ce paragraphe l'ensemble de la documentation concernant la sécurité qu'il s'engage à fournir au titre du projet. Ces documents pourront être les suivants :

Nature du document	Date de remise
Plan d'Assurance Sécurité, version 1	Remise du dossier de réponse à consultation
Plan d'Assurance Sécurité, version définitive	Début de phase de transfert
Plan de secours	Début de phase d'exploitation
Plan de gestion des incidents	Début de phase d'exploitation
Comptes rendus de réunion du comité de suivi	Une semaine après chaque réunion



13. Contacts

Tableau donnant les contacts Amue et du candidat.

Pour l'Amue :

Titre	Nom, prénom	Adresse de messagerie	Num. téléphone
Chef de projet			
RSSI			
DPO			

Pour le candidat :

Titre	Nom, prénom	Adresse de messagerie	Num. téléphone
Chef de projet			
RSSI			
DPO			

14. Annexes

Le candidat pourra placer ici les annexes, comme par exemple, un glossaire.