



Règles de sécurité à l'Amue

Dossier de sécurité



Modification	Version	Emetteur	Date
Création du document	1.0	Sogeti	12/10/2017
Mise à jour	1.1	Amue - DSPSI	23/11/2017
Mise à jour	1.2	Amue - DSPSI	12/12/2017
Mise à jour	1.3	Amue - DSPSI	22/05/2018
Mise à jour mineures	1.4	Amue - DSPSI	28/11/2018
Ajout référentiel, changement nom document et corrections mineures	1.5	Amue – DCSI	28/10/2019
Mise à jour de la méthodologie Ajout des règles sur les offres de service	1.6	Amue – DSSE – pôle technique	06/07/2023
Mise à jour	1.7	Amue – DSSE – pôle technique	13/06/2025

Table des matières

1	Introduction.....	3
2	La cybersécurité à l'Amue.....	4
2.1	PSSI	4
2.2	Organisation SSI.....	4
2.3	Référentiels.....	4
2.4	SSI dans les projets	5
2.4.1	Bonnes pratiques SSI (Conformité GISSIP)	5
2.4.2	Analyse de risques	5
2.4.3	Gestion des évolutions et des incidents de sécurité	5
2.4.4	Environnement de développement et de tests.....	6
2.4.5	SSDLC	6
2.5	Gestion des ressources humaines	6
2.5.1	Cycle de vie des agents.....	6
2.5.2	Sensibilisation	6
2.6	Gestion des données à caractères personnelles	6
2.7	Interconnexion avec les acteurs externes	7
2.8	PRA.....	7
2.9	Contrats avec les prestataires	7
3	La cybersécurité pour les offres de service Amue.....	8
3.1	L'homologation de sécurité	8
3.2	Les principaux principes de sécurité.....	8

1 Introduction

L'Amue est consciente des risques actuels qui pèsent sur tous les systèmes d'information et des enjeux que représentent ces systèmes pour ses adhérents. L'Amue prend en compte la sécurité du SI à son juste niveau dans la réalisation de ses solutions.

Dans ce contexte, l'Amue, toujours préoccupée de fournir une offre SI en conditions de sécurité contrôlées et pilotées, souhaite répondre aux besoins de ses adhérents qui doivent homologuer les différents produits de l'agence intégrés au sein de leur SI.

L'objet de ce document est de présenter la prise en compte de la sécurité dans les produits Amue.

2 La cybersécurité à l'Amue

2.1 PSSI

L'Amue s'est dotée d'une **PSSI** en conformité avec la PSSI de l'Etat (PSSIE)¹.

Les indicateurs de la PSSIE sont présentés au HFDS du Ministère de l'Enseignement Supérieur et de la Recherche de façon périodique.

2.2 Organisation SSI

Au niveau de l'Amue, l'organisation de la chaîne SSI se décline suivant les préconisations nationales donnant lieu à une structure dont les acteurs sont :

- L'autorité hiérarchique qualifiée en SSI est l'**AQSSI** (Autorité Qualifiée de Sécurité des Systèmes d'Information) et représenté par le directeur de l'Amue. Il est juridiquement responsable de la sécurité des systèmes d'information de ses entités et du respect des réglementations.
- Le **Responsable SSI** (RSSI) est nommé et mandaté par l'autorité qualifiée (le directeur de l'Amue) pour définir et veiller à la bonne réalisation de la politique de sécurité. Son rattachement direct auprès de l'AQSSI lui confère toute sa légitimité et lui permet d'assurer pleinement sa mission.
- Il s'appuie lui-même sur un **expert sécurité** en charge des aspects sécurité pour les projets du DSSE (méthodologie, conseil, veille, alertes).

2.3 Référentiels

L'Amue s'appuie sur différents référentiels afin d'établir sa politique de sécurité :

- EBIOS, méthode d'analyse de risques préconisée par l'ANSSI²
- ISO 27001/27002/27004³
- RGS⁴
- PSSIE
- II901⁵ et IGI 1300⁶
- Loi Informatique et Liberté⁷
- RGPD⁸

¹ <https://cyber.gouv.fr/cadre-de-gouvernance-de-la-securite-numerique-de-letat-pssie>

² <https://cyber.gouv.fr/la-methode-ebios-risk-manager>

³ <https://www.iso.org/fr/isoiec-27001-information-security.html>

⁴ <https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs>

⁵ <https://cyber.gouv.fr/instruction-interministerielle-n901>

⁶ <https://cyber.gouv.fr/instruction-generale-interministerielle-n1300>

⁷ <https://www.cnil.fr/fr/le-cadre-national/la-loi-informatique-et-libertes>

⁸ <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

2.4 SSI dans les projets

2.4.1 Bonnes pratiques SSI (Conformité GISSIP)

L'Amue dispose d'une méthodologie projet qui intègre la sécurité des systèmes d'information. Elle est inspirée du **guide d'intégration de la sécurité des systèmes d'informations dans les projets** (GISSIP) édité par l'ANSSI⁹. Cette méthodologie permet d'intégrer la sécurité dans toutes les étapes d'un projet, c'est-à-dire de son étude d'opportunité à sa mise en production. En reprenant un cycle en V adapté aux différents besoins des projets, des points de sécurité ainsi que des livrables (analyse de risques, audit de code, PAS...) sont exigés des équipes afin de maintenir un niveau de sécurité satisfaisant, tout en restant dans une optique d'**amélioration continue**.

Cette méthodologie est aussi adaptée aux besoins spécifiques du mode agile et de la co-construction pour les nouveaux projets de l'Amue. L'adaptation de la méthodologie s'appuie sur les travaux menés par l'ANSSI et la DINSIC¹⁰.

Dans le cas d'un offre de service, l'Amue procède en plus à une **homologation de sécurité de type RGS** conformément à l'ordonnance n°2005-1516 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Pour l'ensemble des produits, une **veille régulière des vulnérabilités** est effectuée. Chaque projet utilise, dès que possible, des applicatifs récents et maintenus à jour par leurs éditeurs.

2.4.2 Analyse de risques

L'Amue réalise périodiquement des **analyses de risques** sur ses différents projets. Une analyse de risques est obligatoirement réalisée à partir de la phase d'expression des besoins et jusqu'à la phase conception technique du cycle en V. Pour les projets en mode agile, une adaptation de la méthodologie impose de produire cette analyse de risques en suivant l'évolution des sprints projet (en mode itératif).

L'analyse de risques est maintenue à jour suite au développement du projet et aux ajouts majeurs imprévus (fonctionnels ou majeurs). De plus, en vue de l'amélioration continue, l'analyse est mise à jour au fur et à mesure des ajouts de fonctionnalités et/ou mesures de sécurité.

Dans tous les cas, l'analyse de risques est alimentée par des **audits techniques**. A minima, un audit de code est produit régulièrement. Lorsqu'un audit de code n'est pas possible, dans le cas par exemple de l'utilisation d'une solution propriétaire, des tests d'intrusion sont effectués.

Pour des besoins particuliers, un audit d'architecture est aussi mené.

2.4.3 Gestion des évolutions et des incidents de sécurité

L'Amue dispose d'une solution de suivi et de gestion permettant de gérer les évolutions des solutions et les incidents de sécurité sur chaque produit.

L'Amue a formalisé une procédure à suivre en cas d'incident de sécurité permettant une réaction rapide et une remédiation efficace en cas d'incident de sécurité affectant un service ou un produit.

⁹ <https://cyber.gouv.fr/publications/gissip-guide-dintegration-de-la-securite-des-systemes-dinformation-dans-les-projets>

¹⁰ <https://www.ssi.gouv.fr/guide/integrer-la-securite-numerique-dans-une-demarche-agile>

2.4.4 Environnement de développement et de tests

Dans chaque équipe projet et pour chaque solution, l'Amue dispose d'une plateforme de développement dédiée et sécurisée, qui permet de tester les évolutions avant de les envoyer sur la plateforme de téléchargement des mises à jour. Les versions sont testées ainsi que les documents permettant leur installation afin de faciliter leur intégration par les adhérents.

L'exploitation de la plateforme projet prend en compte la politique de gestion des comptes et mots de passe mise en œuvre à l'Amue. Cette politique s'appuie sur le document de l'ANSSI intitulé « Recommandations de sécurité relatives aux mots de passe »¹¹.

2.4.5 SSDLC

Pour certaines solutions, les équipes de l'Amue développent certains modules en interne. Pour ce faire, elles utilisent des environnements de développement dont l'architecture s'inspire du Secure Software Development Life Cycle. Le SSDLC combine une usine de développement avec les best practices de l'OWASP¹².

2.5 Gestion des ressources humaines

2.5.1 Cycle de vie des agents

La gestion des habilitations des agents de l'Amue sur son SI s'effectue tout au long du cycle de vie de ceux-ci dans l'organisme :

- Les droits sont attribués à l'embauche et à l'arrivée dans un nouveau service.
- Les droits sont retirés au départ d'un service et à la fin de la carrière.

De plus, les agents suivent un processus de recrutement fidèle à la PSSI de l'Etat. Ainsi les agents peuvent être amenés à prouver leur honnêteté et à fournir un extrait de casier judiciaire. Dans le cas des SI sensibles, une clause de confidentialité est signée par chaque agent.

2.5.2 Sensibilisation

Le personnel Amue est sensibilisé à la sécurité informatique et plus particulièrement à la sécurité des systèmes d'information.

2.6 Gestion des données à caractères personnelles

Une attention particulière est portée par l'Amue à la gestion des données personnelles et au RGPD sous l'autorité du DPO. Toutes les applications concernées font l'objet d'une déclaration à la CNIL.

¹¹ <https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe>

¹² https://www.owasp.org/index.php/Main_Page

2.7 Interconnexion avec les acteurs externes

Toutes les connexions avec les SI des partenaires (prestataires et établissements de co-construction) sont sécurisées :

- VPN IPSec site à site
- VPN client avec MFA
- Identification avec compte nominatif (la liste des comptes est maintenue à jour)
- L'hébergement informatique et les équipes sont présents sur le territoire national

De plus, toutes les connexions sur les environnements des établissements par un agents Amue ou un partenaire et dans le cadre du support d'assistance, doivent toujours passées par l'architecture sécurisée Amue.

2.8 PRA

Le SI de l'Amue est protégé par un Plan de Reprise d'Activité.

2.9 Contrats avec les prestataires

L'Amue dispose d'un clausier de sécurité qui permet de fixer et identifier les exigences de sécurité ainsi que les bonnes pratiques de développement sécurisé incombant à ses prestataires.

Ce clausier est inspiré du guide de l'externalisation de l'ANSSI.¹³

Les appels d'offre sont assortis d'un Plan d'Assurance Sécurité (PAS) qui permet de vérifier les engagements de sécurité des fournisseurs et de faciliter la gestion de crise. Ce PAS est défini notamment avec les prestataires d'hébergement et/ou de maintenance logicielle.

¹³ <https://cyber.gouv.fr/publications/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les>

3 La cybersécurité pour les offres de service Amue

3.1 L'homologation de sécurité

L'Amue est considérée comme une Autorité Administrative (au sens de l'ordonnance n°2005-1516 relative aux échanges électroniques). Les offres de service Amue doivent être conformes aux **règles du Référentiel Général de Sécurité (RGS)**. Cette obligation a été renforcée par le décret 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics.

Conformément à la réglementation, la mise en production d'un service implique la production d'un **dossier d'homologation (DH)** basé sur les référentiels ISO27001, le RGS et la PSSIE (ainsi que le RGPD). Le dossier d'homologation repose sur le dossier de sécurité produit par l'équipe projet de la solution avec le soutien du Pôle Technique de l'Amue. L'analyse de risques de type **EBIOS** (2010 ou RM) est révisée à chaque nouvelle mesure de sécurité ou nouvelles fonctionnalités.

Les travaux d'homologation sont menés avec un groupe d'experts d'établissements de l'ESR pour constituer une commission d'homologation qui accompagne l'Autorité d'Homologation (AH) dans sa décision.

3.2 Les principaux principes de sécurité

Les offres de services de l'Amue suivent notamment les règles ci-dessous :

- Hébergement du service et des données en France
- Equipes d'exploitation et de maintenance localisées au sein de l'Union européenne
- Identification des exigences de sécurité incombant aux partenaires (prestataires ou membres de la communauté ESR)
- Utilisation d'environnements dédiés et sécurisés
- Vérifications techniques automatiques de la sécurité du service
- Sensibilisation des administrateurs aux consignes de sécurité liées à l'utilisation du service
- Chiffrement du trafic des données avec un certificat de sécurité conforme à la réglementation RGS
- Désactivation de tout flux non chiffré
- Fermeture de tous les ports non strictement nécessaires
- Limitation au strict nécessaire du nombre de personnes disposant d'un accès administrateur au service
- Limitation des droits de chaque administrateur au strict nécessaire
- Utilisation d'un coffre-fort de mots de passe
- Veille régulière des vulnérabilités et utilisation des applicatifs récents et maintenus à jour par leurs éditeurs
- Bonnes pratiques de développement sécurisé du service (basées sur le référentiel OWASP)