



DOCUMENT DE RÉFÉRENCE DES STANDARDS ET NORMES



AVERTISSEMENT

Toute utilisation ou reproduction intégrale ou partielle faite sans le consentement de l'Amue est illicite. Cette représentation ou reproduction par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les dispositions des articles L.335-1 et suivants du Code de la Propriété Intellectuelle et, de manière générale, une atteinte aux droits de l'Amue. Les informations contenues dans ce document pourront faire l'objet de modifications sans préavis et n'engagent en aucune manière l'Amue.

AGENCE DE MUTUALISATION DES UNIVERSITES ET ETABLISSEMENTS

Reproduction interdite sans autorisation écrite préalable.



Table d'approbation du document

Approbateur	Service	Date d'approbation
Frédéric DESENZANI	Cellule Qualité	25/11/2015

Table des révisions du document

Version	Auteur	Date	Objet de la mise à jour
1.00	Frédéric DESENZANI	03/03/2015	Création du document
1.01	Frédéric DESENZANI	27/02/2017	Mise à jour du document avec un nouveau chapitre lié à la sécurité des systèmes d'information.
1.02	DSPSI	29/03/2018	Révision du document
1.03	Frantz Gourdet (DPO)	16/04/2018	Actualisation RGPD
1.04	DSPSI	26/04/2018	Corrections diverses
1.05	DCSI	03/12/2019	Actualisation des références
1.06	DCSI	03/11/2021	Actualisation des références
1.07	DSSE	01/02/2024	Actualisation des références
1.08	DSSE	15/12/2025	Ajout de la doctrine Cloud de l'état
1.09	DSSE	20/03/2026	Ajout de normes

Modifications depuis la dernière version

Paragraphe	Page	Nature de la Modification
2.6	12	Ajout des informations sur la directive NIS2
2.4	10	Ajout de la PPST
2.9	15	Suppression guide GISSIP (plus de référence à l'ANSSI)
2.9	15	Ajout de la démarche EBIOS RM
2.13	18	Précisions sur le RGAA

A chaque nouvelle version du document, la table des révisions et des modifications doit être mise à jour.



Table des matières

1. PRESENTATION DES STANDARDS ET NORMES	5
2. DETAIL ET REFERENCES DES STANDARDS ET NORMES.....	6
2.1. SCHEMA DIRECTEUR DES ESPACES NUMERIQUES DE TRAVAIL (SDET)	6
2.2. RECOMMANDATION POUR LES ANNUAIRES DE L'ENSEIGNEMENT SUPERIEUR (SUPANN)	8
2.3. POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DE L'ÉTAT (PSSIE)	9
2.4. PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION (PPST)	10
2.5. CLOUD AU CENTRE : LA DOCTRINE DE L'ÉTAT	11
2.6. REFERENTIEL GENERAL DE SECURITE (RGS)	11
2.7. DIRECTIVE NIS2	13
2.8. GUIDE D'HYGIENE INFORMATIQUE.....	14
2.9. METHODE EBIOS RISK MANAGER.....	15
2.10. GUIDE DE LA SECURITE NUMERIQUE DANS UNE DEMARCHE AGILE	15
2.11. REFERENTIEL GENERAL D'INTEROPERABILITE (RGI)	16
2.12. SOCLE INTERMINISTERIEL DES LOGICIELS LIBRES (SILL)	17
2.13. REFERENTIEL GENERAL D'AMELIORATION DE L'ACCESSIBILITE (RGAA)	18
2.14. CONTRAINTES LEGALES « INFORMATIQUE ET LIBERTES » (IL) INSCRITES OU DECOULANT DU REGLEMENT EUROPEEN GENERAL POUR LA PROTECTION DES DONNEES (RGPD).....	20
2.15. POLITIQUE ET GOUVERNANCE « INFORMATIQUE ET LIBERTES » (RGPG) DE L'AMUE	21
2.16. NOTATION BPMN	23



1. PRESENTATION DES STANDARDS ET NORMES

Dans le cadre de la politique de modernisation de l'action publique, les établissements publics de l'état doivent se conformer aux standards et normes construits et maintenus par les différents services de l'état (Direction Interministérielle de la Transformation Publique (DITP) et Direction Interministérielle du Numérique (DINUM), Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), etc.).

Ces standards et normes ont pour objectif d'accroître la cohérence des systèmes d'information conçus, développés et maintenus par les services centraux et déconcentrés de l'État, collectivités publiques, éditeurs de logiciel, prestataires de services, etc.

Les standards et normes supportés par les solutions informatiques constituant le SI de l'Amue sont les suivants :

- Schéma directeur des espaces numériques de travail (SDET) et ses annexes : Dans l'attente d'un nouveau schéma directeur spécifique à l'enseignement supérieur et à la recherche, le SDET applicable à l'enseignement scolaire est proposé ci-dessous dans sa dernière version,
- Recommandation pour les annuaires de l'enseignement supérieur (SUPANN),
- Politique de sécurité des systèmes d'information de l'état (PSSIE),
- Protection du potentiel scientifique et technique de la Nation (PPST)
- Doctrine Cloud de l'état,
- Référentiel général de sécurité (RGS),
- Directive européenne NIS2,
- Guide d'intégration de la sécurité des systèmes d'information dans les projets (GISSIP),
- Référentiel général d'interopérabilité (RGI),
- Socle Interministériel des Logiciels Libres (SILL),
- Référentiel général d'accessibilité pour les administrations (RGAA),
- Contraintes légales « informatique et libertés » (IL) inscrites ou découlant du règlement européen général pour la protection des données (RGPD),
- Politique informatique et libertés de l'Amue dans le cycle de vie d'un SI,
- Notation BPMN.



2. DETAIL ET REFERENCES DES STANDARDS ET NORMES

2.1. SCHEMA DIRECTEUR DES ESPACES NUMERIQUES DE TRAVAIL (SDET)

SCHEMA DIRECTEUR DES ESPACES NUMERIQUES DE TRAVAIL (SDET)	
Présentation	Pour définir les services attendus dans les espaces numériques de travail et pour formaliser les préconisations organisationnelles, fonctionnelles et techniques, le ministère publie le SDET. Le SDET s'inscrit dans le plan d'ensemble que constitue le S3it (schéma stratégique des systèmes d'information et des télécommunications). La version 1 du schéma directeur des espaces numériques de travail a été publiée en janvier 2004. La version 2 du schéma directeur des espaces numériques de travail a été publiée en novembre 2006. La version 3 du schéma directeur des espaces numériques de travail a été publiée en juillet 2011. Les modifications apportées au SDET avec cette version 3 concernent essentiellement l'annexe AAS (Authentification, Autorisation, SSO), qui a été complétée afin d'apporter les recommandations nécessaires à l'articulation entre les ENT et les autres portails de l'Éducation nationale (en particulier les téléservices), et entre les ENT et les autres services applicatifs distants. Cette montée en version a également permis d'amender le cahier des charges de l'annuaire ENT et ses annexes, afin de tenir compte de la mise en œuvre et de l'instruction des problèmes d'alimentation des annuaires ENT par le système d'information du ministère. La version 4.0 a complété les évolutions inscrites dans la version 3 (publiée en juillet 2011) en soulignant la nécessaire approche des ENT par les besoins des usagers (en particulier les élèves et les enseignants). À cette fin, les services pédagogiques nécessaires dans les bouquets proposés par les projets ENT ont été précisés et les documents modifiés dans l'optique d'accompagner les projets dans la définition des besoins fonctionnels Les principales mises à jour de la version 5 concernaient : - l'introduction d'un chapitre 9 dédié aux « accès multisupports » ; celui-ci présente les diverses familles de terminaux utilisés, renseigne sur la façon dont les services ENT peuvent être accédés et fait état de différents types de préconisations ; - un complément pour le premier degré dans l'ensemble « annuaire ENT » prenant en compte les résultats des travaux menés dans le cadre de l'expérimentation de l'alimentation des annuaires ENT par l'annuaire fédérateur ; - des recommandations relatives à l'exploitation du service annuaire ENT et à son exploitabilité pour le premier et le second degré. L'objectif de la version 6 est de rendre ce référentiel davantage opérationnel, les ENT se devant de répondre du mieux possible aux besoins et aux attentes de la communauté éducative. Ainsi cette version, résultat d'une action de restructuration et de refonte conduite depuis le deuxième semestre 2015, s'attache-t-elle à prendre en compte autant que possible les préconisations ou souhaits d'évolution recueillis à l'occasion du cycle de consultation des acteurs ENT (dont l'étude sur le rôle du SDET, 2013), des ateliers organisés pour valider les grilles de conformité au SDET (2014), et des contributions à l'appel à commentaires du SDET V5 (2015). La version 6.6 du SDET est la version en vigueur à partir de juillet 2023 et se caractérise par la rationalisation et la simplification du document principal et de l'annexe opérationnelle et prend en compte les évolutions suivantes : - La simplification des chapitres Introduction et Présentation générale des ENT et du SDET ;



	- La restructuration des chapitres Qualités et Architecture de référence ENT ; - L'introduction des principes directeurs de type fonctionnels, techniques, de sécurité et d'interopérabilité, en lieu et place des exigences et recommandations ; - L'introduction de cartographies fonctionnelles et des schémas de dépendances entre les services ENT et d'interopérabilité ; - La mise à jour de l'ensemble annuaire ; - La mise à jour du kit de conventionnement « Informatique et Libertés » et des aspects juridiques de l'annexe opérationnelle ; - L'adaptation de la grille de conformité ; - Un nouveau document d'accompagnement intitulé « kit de conservation et d'archivage des données ENT ».		
Cadre législatif	Sans objet.		
url présentation	https://www.education.gouv.fr/les-referentiels-450069		
Propriétaire	<table><tr><td> Liberté • Égalité • Fraternité REPUBLIQUE FRANÇAISE</td><td>MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE</td></tr></table>	 Liberté • Égalité • Fraternité REPUBLIQUE FRANÇAISE	MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE
 Liberté • Égalité • Fraternité REPUBLIQUE FRANÇAISE	MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE		
Commentaire	Sans objet.		



2.2. RECOMMANDATION POUR LES ANNUAIRES DE L'ENSEIGNEMENT SUPERIEUR (SUPANN)

RECOMMANDATION POUR LES ANNUAIRES DE L'ENSEIGNEMENT SUPÉRIEUR (SUPANN)	
Présentation	Les Technologies de l'Information et de la Communication font aujourd'hui partie intégrante du fonctionnement des établissements d'enseignement supérieur. Les services et les ressources numériques accessibles par les étudiants, enseignants, chercheurs et personnels administratifs recouvrent l'ensemble des domaines fonctionnels. Les ressources numériques et les services numériques d'un établissement sont généralement accessibles via un dispositif de type ENT (Espace Numérique de Travail) via l'Intranet ou au travers de l'Internet. L'accès via Internet ouvre la voie au nomadisme, au télétravail, au partage des ressources entre établissements, il permet d'élargir l'offre de formation à de nouvelles populations (EAD/FOAD) et de renforcer les relations de l'établissement avec le grand public et le tissu socio-économique. Il y a un intérêt stratégique à faciliter l'accès aux services et aux ressources numériques de l'établissement mais cet objectif ne doit pas éluder la nécessité de contrôler les accès pour certaines ressources à protéger et qui ne doivent être accessibles qu'aux personnes dûment autorisées. Le contrôle d'accès aux ressources et services se traduit généralement par la mise en œuvre de mécanismes d'identification, d'authentification et de gestion des autorisations s'appuyant sur un ensemble de données géré au sein d'un référentiel de type « annuaire ». Les annuaires, initialement mis en œuvre pour des fonctions contrôle d'accès et de pages blanches ont vu croître la liste des applications et des services qui en dépendent. Ils occupent une place cruciale au cœur du « Système Global d'Information » (SGI) des établissements. De leur qualité (complétude, exactitude et fiabilité) dépend le bon fonctionnement des Systèmes d'Informations. Pour différentes raisons il est nécessaire d'avoir un cadre de cohérence commun matérialisant la structure et le contenu de ces annuaires: lisibilité des données, portabilité des applications, facilitation des échanges entre établissements. Un ensemble de documents normatifs (RFC LDAP) élaborés au niveau international a établi un premier cadre pour la mise en œuvre des annuaires. Cet effort initial a dû être complété afin de satisfaire les spécificités de communautés particulières. Pour les Établissements d'Enseignement Supérieur (EES) les premières recommandations appelées SupAnn v1 furent publiées en juillet 2003. Elles définissaient un ensemble d'éléments jugé suffisant au moment de leur publication. Depuis de nouveaux besoins sont apparus justifiant la parution de la mouture 2008 et des suivantes, la dernière recommandation datant de 2020.
Cadre législatif	Sans objet.
url présentation	https://services.renater.fr/documentation/supann/index
Propriétaire	 RENATER CONNECTEUR DE SAVOIRS https://www.renater.fr/
Commentaire	Sans objet.



2.3. POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DE L'ÉTAT (PSSIE)

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT (PSSIE)	
Présentation	La PSSIE fixe les règles de protection applicables aux systèmes d'information de l'État. Essentiels à l'action publique, les systèmes d'information sont porteurs d'efficacité, mais aussi de risques : menaces d'exfiltration de données confidentielles, d'atteinte à la vie privée des usagers, voire de sabotage des systèmes d'information. Afin de prendre en compte ces risques, le Premier ministre a défini une politique volontariste, mais également pragmatique par laquelle l'État affiche sa volonté de se montrer exemplaire en matière de cybersécurité. La PSSIE s'inscrit dans le cadre des mesures annoncées en Conseil des ministres le 25 mai 2011 pour faire face à la montée des cyber-attaques. La première version a été publiée par circulaire le 17 juillet 2014. La PSSIE s'applique à tous les systèmes d'information des administrations de l'État : ministères, établissements publics sous tutelle d'un ministère, services déconcentrés de l'État et autorités administratives indépendantes. Ces administrations sont dénommées « entités » dans le texte. La PSSIE concerne l'ensemble des personnes physiques ou morales intervenant dans ces systèmes d'information, qu'il s'agisse des administrations de l'État et de leurs agents ou bien de tiers agissant au nom et pour le compte des administrations de l'État (prestataires ou sous-traitants) et de leurs employés. La PSSIE s'adresse à l'ensemble des agents de l'État, et tout particulièrement : – aux autorités hiérarchiques, qui sont responsables de la sécurité des informations traitées au sein de leurs services ; – aux agents chargés des fonctions de directeurs des systèmes d'information (DSI) ; – aux personnes chargées de la sécurité et de l'exploitation des systèmes d'information. La PSSIE décline dix principes fondamentaux portant sur le choix d'éléments de confiance pour construire les systèmes d'information, sur la gouvernance de la sécurité et sur la sensibilisation des acteurs. Parmi ces principes, la circulaire met en exergue la nécessité pour les administrations de l'État de recourir à des produits et à des services qualifiés par l'ANSSI ainsi qu'à un hébergement sur le territoire national de leurs données les plus sensibles. Chaque ministère est désormais responsable de l'application de la PSSIE entrée en vigueur le 29 août 2014. Celle-ci a également été conçue pour constituer une base méthodologique pour tout organisme ou institution, extérieur à l'État, ayant à élaborer un document de cette nature.
Cadre législatif	Circulaire du Premier ministre du 17 juillet 2014
url présentation	https://cyber.gouv.fr/cadre-de-gouvernance-de-la-securite-numerique-de-letat-pssie
Propriétaire	 https://cyber.gouv.fr/
Commentaire	Sans objet.



2.4. PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION (PPST)

RÉFÉRENTIEL GÉNÉRAL DE SECURITE (RGS)	
Présentation	Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) vise à protéger les savoirs, savoir-faire, technologies et connaissances sensibles des établissements publics et privés (laboratoires de recherche, entreprises, etc.) situés sur le territoire français. Ces éléments, essentiels à l'activité scientifique fondamentale ou appliquée, constituent des intérêts fondamentaux de la nation au sens de l'article 410-1 du code pénal. Les établissements bénéficient d'un soutien personnalisé pour renforcer leur sécurité, notamment en matière de cybersécurité (politique de sécurité des systèmes d'information - PSSI). Elle est mise en œuvre par six hauts fonctionnaires de défense et de sécurité (HFDS) rattachés aux ministères de l'Éducation nationale, de la Recherche, de la Défense, de l'Économie, de l'Agriculture et de la Santé. Elle est fondée sur des textes réglementaires clés : décret n° 2011-1425 du 2 novembre 2011, décret n° 2024-430 du 14 mai 2024, arrêté du Premier ministre du 3 juillet 2012 (modifié en 2024), et instruction interministérielle du 9 mai 2025.
Cadre législatif	Article 413-7 du Code pénal Décret n° 2024-430 du 14 mai 2024 Arrêté du Premier ministre du 3 juillet 2012 modifié par l'arrêté du Premier ministre du 24 octobre 2024 Instruction interministérielle relative à la mise en œuvre du dispositif (publiée le 9 mai 2025) Instruction interministérielle no 901/SGDSN/ANSSI du 28 janvier 2015 sur la protection des systèmes d'information sensibles ou Diffusion Restreinte
url présentation	https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/protection-information-sensible-diffusion-restreinte/protection-du-potentiel-scientifique-et-technique-de-la-nation-ppst/
Propriétaire	 https://cyber.gouv.fr/
Commentaire	Sans objet.



2.5. CLOUD AU CENTRE : LA DOCTRINE DE L'ÉTAT

RÉFÉRENTIEL GÉNÉRAL DE SECURITE (RGS)	
Présentation	Avec l'adoption de la doctrine « Cloud au centre », le Gouvernement fait du Cloud un prérequis pour tout nouveau projet numérique au sein de l'État ou refonte substantielle de l'architecture applicative existante. L'objectif : accélérer la transformation numérique au bénéfice des usagers et dans le strict respect de la cybersécurité et de la protection des données des citoyens et des entreprises. L'informatique en nuage va au-delà d'un simple socle d'hébergement : elle sous-tend toute une culture, depuis le mode de production des applications (mode produit, DevOps) jusqu'aux principes d'architecture à la base de la conception de ces nouveaux services (architecture nativement cloud).
Cadre législatif	Doctrine « cloud au centre » sur l'usage de l'informatique en nuage au sein de l'État : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039281619 https://www.legifrance.gouv.fr/circulaire/id/45446
url présentation	https://www.numerique.gouv.fr/offre-accompagnement/cloud-administrations/la-doctrine-de-l%C3%A9tat/
Propriétaire	 https://www.numerique.gouv.fr/dinum/ https://cyber.gouv.fr/
Commentaire	Sans objet.

2.6. REFERENTIEL GENERAL DE SECURITE (RGS)

RÉFÉRENTIEL GÉNÉRAL DE SECURITE (RGS)	
Présentation	Le Référentiel Général de Sécurité (RGS) définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose également des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont libres d'appliquer. Le RGS a été élaboré conformément à l'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives. Il fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique. Le RGS apporte les éclairages nécessaires aux autorités administratives pour prendre en compte pleinement les dispositions de l'ordonnance.
Cadre législatif	Arrêté du 18 janvier 2012 relatif au référencement de produits de sécurité ou d'offres de prestataires de services de confiance



	Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques (dit "arrêté RGS") (abrogé) Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques Arrêté du 10 juin 2015 prorogeant les délais de mise en œuvre du référentiel général de sécurité Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives Décret n°2010-112 du 2 février 2010 (dit "décret RGS") Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique 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 Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique (abrogé) Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique Loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations	
url présentation	https://www.numerique.gouv.fr/publications/referentiel-general-de-securite/	
Propriétaire		https://www.numerique.gouv.fr/dinum/ https://cyber.gouv.fr/
Commentaire	Sans objet.	



2.7. DIRECTIVE NIS2

RÉFÉRENTIEL GÉNÉRAL DE SECURITE (RGS)	
Présentation	La directive NIS2 (Network and Information Security 2) est une réglementation européenne adoptée en décembre 2022 pour renforcer la cybersécurité et la résilience des infrastructures critiques au sein de l'Union européenne. Elle vise à harmoniser les pratiques de sécurité à l'échelle de l'UE, en réponse à l'augmentation des cybermenaces et à la dépendance croissante des secteurs essentiels à la numérisation. Principales obligations : - Mise en place d'une approche par les risques pour évaluer et gérer les menaces cybers, - Adoption de mesures techniques, organisationnelles et opérationnelles adaptées, - Sécurité de la chaîne d'approvisionnement : encadrement contractuel des fournisseurs et prestataires, - Notification des incidents importants au CSIRT national (Organisme national de réponse aux incidents) dans un délai strict.
Cadre législatif	<u>Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union</u>
url présentation	<u>https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/directive-nis-2/</u>
Propriétaire	 <u>https://cyber.gouv.fr/</u>
Commentaire	La transposition de la NIS2 en droit français a pris du retard, mais le cadre est en vigueur.



2.8. GUIDE D'HYGIENE INFORMATIQUE

GUIDE D'HYGIENE INFORMATIQUE	
Présentation	Les enjeux de sécurité numérique doivent se rapprocher des préoccupations économiques, stratégiques ou encore d'image qui sont celles des décideurs. En contextualisant le besoin, en rappelant l'objectif poursuivi et en y répondant par la mesure concrète correspondante, ce guide d'hygiène informatique est une feuille de route qui épouse les intérêts de toute entité consciente de la valeur de ses données. Le guide vous accompagne dans la sécurisation de votre système d'information Vous êtes responsable de la sécurité des systèmes d'information de votre organisation ou, plus simplement, c'est à vous que revient la responsabilité du bon fonctionnement de son informatique. Ce guide s'adresse à vous. Il vous présente les 42 mesures d'hygiène informatique essentielles pour assurer la sécurité de votre système d'information et les moyens de les mettre en œuvre, outils pratiques à l'appui. Renforcer la sécurité de son système d'information en 42 mesures Non exhaustives, ces mesures représentent cependant le socle minimum à respecter pour protéger les informations de votre organisation. Une fois ces règles partagées et appliquées, vous aurez accompli une part importante de votre mission : permettre à votre organisation d'interagir avec ses partenaires et de servir ses clients en respectant l'intégrité et la confidentialité des informations qui les concernent.
Cadre législatif	Sans objet.
url présentation	https://messervices.cyber.gouv.fr/guides/guide-dhygiene-informatique
Propriétaire	https://cyber.gouv.fr/
Commentaire	Sans objet.



2.9. METHODE EBIOS RISK MANAGER

GUIDE D'INTÉGRATION DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DANS LES PROJETS (GISSIP)	
Présentation	La méthode de référence française EBIOS accompagne les organisations pour identifier et comprendre les risques numériques qui leurs sont propres. Elle permet de déterminer les mesures de sécurité adaptées à la menace et de mettre en place le cadre de suivi et d'amélioration continue à l'issue d'une analyse de risque partagée au plus haut niveau.
Cadre législatif	Sans objet.
url présentation	https://cyber.gouv.fr/securisation/analyse-des-risques/methode-ebios-rm/
Propriétaire	 https://cyber.gouv.fr/
Commentaire	Sans objet.

2.10. GUIDE DE LA SECURITE NUMERIQUE DANS UNE DEMARCHE AGILE

GUIDE DE LA SECURITE NUMERIQUE DANS UNE DEMARCHE AGILE	
Présentation	Ce guide a pour vocation d'aider les organismes publics et privés à intégrer la sécurité numérique dans un projet Agile, particulièrement dans le cadre d'une démarche d'homologation de sécurité. Il propose une approche simple et pratique, adaptée au mode de développement Agile, d'analyse et de traitements des risques numériques. Le guide est utilisable par toute organisation, quelles que soient sa nature et sa taille. Il s'accompagne d'un guide annexe qui contient des outils méthodologiques et des bases de connaissances permettant à une équipe de développement de mener les activités de sécurité et d'homologation présentées dans le présent document.
Cadre législatif	Sans objet.
url présentation	https://cyber.gouv.fr/publications/agilite-et-securite-numeriques-methode-et-outils-lusage-des-equipes-projet
Propriétaire	 https://cyber.gouv.fr/
Commentaire	Sans objet.



2.11. REFERENTIEL GENERAL D'INTEROPERABILITE (RGI)

RÉFÉRENTIEL GÉNÉRAL D'INTEROPÉRABILITÉ (RGI)		
Présentation	Le RGI est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration. Ces recommandations constituent les objectifs à atteindre pour favoriser l'interopérabilité. Elles permettent aux acteurs cherchant à interagir et donc à favoriser l'interopérabilité de leur système d'information, d'aller au-delà de simples arrangements bilatéraux. Le RGI est défini dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Dans l'article 11 de cette ordonnance, le "RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publications de ce référentiel sont fixées par décret". La version 2.0 du RGI est officialisée par l'arrêté en date du 20 avril 2016. C'est la version "En vigueur" du Référentiel Général d'Interopérabilité.	
Cadre législatif	Ordonnance n° 2005-1516 du 8 décembre 2005	
	Décret n° 2007-284 du 2 mars 2007 Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité	
url présentation	https://www.numerique.gouv.fr/publications/interopabilite/	
Propriétaire		https://www.numerique.gouv.fr/dinum/
Commentaire	Sans objet.	



2.12. SOCLE INTERMINISTÉRIEL DES LOGICIELS LIBRES (SILL)

SOCLE INTERMINISTÉRIEL DES LOGICIELS LIBRES (SILL)	
Présentation 	La modernisation des systèmes d'information de l'État passe notamment par le développement des usages et technologies innovantes et créatrices de valeur pour les utilisateurs, et par la maîtrise des coûts, ce qui implique en particulier de développer la réutilisation et la mutualisation, et d'ajuster au mieux les dépenses d'acquisition. L'approche de l'État privilégie l'efficacité globale, en dehors de tout dogmatisme, pour lui permettre de choisir entre les différentes solutions, libres, éditeurs ou mixtes. C'est l'objet de la circulaire du 19 septembre 2012, signée par le Premier ministre, qui recommande les voies du bon usage du logiciel libre dans l'Administration. Pour dégager le maximum d'efficacité aussi bien économique qu'en termes de qualité, il convient d'utiliser le logiciel libre de manière concertée et coordonnée. Un cadre de convergence des logiciels à privilégier dans le développement des systèmes d'information de l'État, défini en 2012, est maintenu en concertation interministérielle. Il touche en priorité les systèmes les plus déployés, sur les serveurs comme sur les postes de travail. Ce cadre ne fait pas obstacle à l'innovation par essai de nouvelles souches, qui pourront aider à l'évolution du cadre. Ce cadre ne rend pas non plus obligatoire l'évolution adaptative des applications existantes non conformes. Par contre il définit des versions de référence à privilégier et indique les solutions à abandonner, avec des réserves éventuelles pour des contextes d'usage particuliers. Il participe ainsi à la convergence progressive des contextes d'exploitation et à la mutualisation de certains moyens. A ce titre il doit être intégré dans tous les cadres technologiques des ministères et pris en compte à l'occasion de nouveaux développements et de refontes majeures.
Cadre législatif	Circulaire n° 5608-SG du 19 septembre 2012
url présentation	https://www.data.gouv.fr/fr/datasets/socle-interministeriel-de-logiciels-libres/
Propriétaire	 https://www.numerique.gouv.fr/dinum/
Commentaire	Sans objet.



2.13. REFERENTIEL GENERAL D'AMELIORATION DE L'ACCESSIBILITE (RGAA)

RÉFÉRENTIEL GÉNÉRAL D'AMÉLIORATION DE L'ACCESSIBILITÉ (RGAA)	
Présentation	Le handicap est défini comme : « toute limitation d'activité ou restriction de participation à la vie en société subie dans son environnement par une personne en raison d'une altération substantielle, durable ou définitive d'une ou plusieurs fonctions physiques, sensorielles, mentales, cognitives ou psychiques, d'un polyhandicap ou d'un trouble de santé invalidant » (article L. 114 du code de l'action sociale et des familles). L'accessibilité numérique consiste à rendre les services de communication au public en ligne accessibles aux personnes handicapées, c'est-à-dire : • perceptibles : par exemple, faciliter la perception visuelle et auditive du contenu par l'utilisateur ; proposer des équivalents textuels à tout contenu non textuel ; créer un contenu qui puisse être présenté de différentes manières sans perte d'information ni de structure (par exemple avec une mise en page simplifiée) ; • utilisables : par exemple, fournir à l'utilisateur des éléments d'orientation pour naviguer, trouver le contenu ; rendre toutes les fonctionnalités accessibles au clavier ; laisser à l'utilisateur suffisamment de temps pour lire et utiliser le contenu ; ne pas concevoir de contenu susceptible de provoquer des crises d'épilepsie ; • compréhensibles : par exemple, faire en sorte que les pages fonctionnent de manière prévisible ; aider l'utilisateur à corriger les erreurs de saisie. • et robustes : par exemple, optimiser la compatibilité avec les utilisations actuelles et futures, y compris avec les technologies d'assistance.
Cadre législatif	L'article 47 de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées fait de l'accessibilité une exigence pour tous les services de communication publique en ligne de l'État, les collectivités territoriales et les établissements publics qui en dépendent. Il stipule que les informations diffusées par ces services doivent être accessibles à tous. Le Référentiel général d'Accessibilité pour les Administrations (RGAA) rendra progressivement accessible l'ensemble des informations fournies par ces services. Et l'article 47-1 de la loi n° 2005-102 du 11 février 2005 (créé par l'ordonnance n°2023-859 du 6 septembre 2023) » ; Le décret n°2009-546 du 14 mai 2009 (pris en application de l'article 47 de la loi n° 2005-102 du 11 février 2005 sur l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées) impose une mise en œuvre de l'accessibilité dans un délai de deux ans (à partir de la publication du décret) pour les services de communication publique en ligne de l'Etat et des établissements publics qui en dépendent, et de trois ans pour les services de communication publique en ligne des collectivités territoriales et des établissements publics qui en dépendent. Décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne veut un accès équitable des services de communication au public en ligne. Cette initiative veut que tout le monde puisse accéder facilement aux informations numériques, en particulier les personnes souffrant de déficience physique, sensorielle ou cognitive ainsi que les seniors.



	l'arrêté du 20 septembre 2019 portant référentiel général d'amélioration de l'accessibilité (RGAA). Une version 5 du RGAA est en cours de rédaction avec une publication prévue fin 2026. Décret n° 2023-931 du 9 octobre 2023 relatif à l'accessibilité aux personnes handicapées des produits et services a pour objet de transposer en droit français la directive de l'UE relative à l'harmonisation des législations des Etats membres concernant les exigences en matière d'accessibilité aux produits et services (European Accessibility Act).	
url présentation	https://accessibilite.numerique.gouv.fr/	
Propriétaire		https://www.numerique.gouv.fr/dinum/
Commentaire	Sans objet.	



2.14. CONTRAINTES LEGALES « INFORMATIQUE ET LIBERTES » (IL) INSCRITES OU DECOULANT DU REGLEMENT EUROPEEN GENERAL POUR LA PROTECTION DES DONNEES (RGPD)

CONTRAINTES LEGALES INFORMATIQUE ET LIBERTES (IL)	
Présentation	Le règlement européen général pour la protection des données (RGPD) est la pierre angulaire d'un corpus de contraintes légales dotées d'une force obligatoire instituées afin que soient respectés les droits fondamentaux des personnes lors de la mise en œuvre de traitements de données à caractère personnel. Ce corpus comporte ces dispositions législatives et réglementaires ainsi que d'autres normes à <i>valeur contraignante</i> (au sens juridique du terme). Quelques grands principes résument, sans les épuiser, les principales <i>contraintes</i> à respecter : 1. Finalité déterminée, explicite et légitime a. Finalité déterminée Recueillir des données pour un usage précis et bien défini. b. Finalité explicite Enoncer les finalités à l'avance et de manière compréhensible par les personnes dont les données vont être traitées. c. Finalité légitime Ne jamais aller à l'encontre de la loi, ni des droits ou des libertés fondamentales des personnes. 2. Données ajustées/proportionnées aux finalités Veiller à ce que les données collectées (ou à collecter) soient pertinentes, adéquates et non excessives c'est-à-dire strictement nécessaires à la finalité déclarée. 3. Durée de conservation limitée Ne pas conserver les informations concernant les personnes au-delà de la réalisation de la finalité annoncée. S'agissant de concevoir un traitement, déterminer les paramètres/durée par défaut et le mécanisme permettant de basculer les données de leur archive active à leur archive intermédiaire. Prévoir la possibilité d'appliquer à cette occasion les restrictions d'accès ou d'habilitation qui s'imposeront, ainsi que la possibilité de transférer ces archives intermédiaires aux personnes/services chargés de leur destruction ou de leur archivage définitif. 4. Accès aux données limité Traiter les données à caractère personnel en toute confidentialité. S'agissant de concevoir un traitement, rendre les données personnelles manipulables de manière confidentielle et accessibles uniquement aux personnes habilitées à en prendre connaissance dans le cadre de leurs missions. 5. Sécurité physique et logique Prendre (ou, s'agissant de concevoir un traitement, permettre que soient prisent) toutes les précautions utiles, au regard de la nature des données et des risques induits par le traitement, pour préserver la sécurité des données et, notamment, éviter qu'elles ne soient déformées, endommagées, ou que des tiers non autorisés n'y aient accès. 6. Information et droits des personnes dont on traite les données Informar (ou, s'agissant de concevoir un traitement, permettre que puissent être informées) les personnes de l'existence de collecte de données effectuée en identifiant bien le responsable de traitement et en indiquant la finalité poursuivie ainsi que le caractère obligatoire ou facultatif des réponses attendues lors de cette collecte et, le cas échéant, indiquer également les conséquences d'un défaut de réponse. Rappeler aux



	personnes leurs droits ainsi que les canaux et circuits leur permettant de les exercer : les personnes concernées par un traitement doivent toujours pouvoir, si elles le souhaitent, accéder à leurs données personnelles, les faire rectifier, exercer leur droit d'opposition - dès lors qu'une obligation contractuelle ou légale n'impose pas ce traitement auquel cas il faut expliciter cette obligation - ou tout autre droit entrant dans le cadre des articles 12 à 23 du RGPD : effacement (droit à l'oubli), limitation du traitement, portabilité et gestion post mortem. Lorsqu'il y en a, signaler les partenaires destinataires de données à caractère personnel. 7. En cas de sous-traitance S'assurer de l'existence d'un contrat de sous-traitance comportant des clauses « Informatique et Libertés » à respecter (ou faire respecter), et adaptées au traitement effectué ou à effectuer.
Cadre législatif	<u>Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) – Entrée en vigueur le 4 mai 2016 et pleinement applicable à partir du 25 mai 2018.</u>
url présentation	https://www.cnil.fr/fr/professionnel
Propriétaire	 https://www.cnil.fr
Commentaire	Le Règlement européen voté le 14 avril et publié le 4 mai 2016 est pleinement applicable à partir du 25 mai 2018.

2.15. POLITIQUE ET GOUVERNANCE « INFORMATIQUE ET LIBERTES » (RGPG) DE L'AMUE

POLITIQUE INFORMATIQUE ET LIBERTÉS (IL)	
Présentation	L'agence de mutualisation des universités et établissements d'enseignement supérieur et de recherche (Amue) organise la coopération et sert de support aux actions communes de ses adhérents en vue d'améliorer la qualité de leur gestion notamment en contribuant à l'élaboration de leur système d'information à partir d'une offre logicielle plurielle répondant à leur diversité. Bien qu'elle ne soit pas <i>responsable des traitements</i> mis en œuvre par ses adhérents, l'Amue a adopté en 2015 le référentiel de gouvernance « Informatique et Libertés » de la CNIL et a notamment initié dans ce cadre le respect du principe de <i>Privacy By Design/Default</i> c'est-à-dire la prise en compte de la protection des données à caractère personnel dès la conception des traitements. Le respect de ce principe, à titre anticipé de l'entrée en vigueur en 2016 et de l'application à partir du 25 mai 2018 du Règlement Européen, implique en particulier la systématisation des études d'impact sur la vie privée (EIVP/PIA) à l'amont de la mise en œuvre des traitements. Cette systématisation vise à construire des solutions logicielles déjà conformes aux contraintes légales I&L à la livraison, et qui évitent, de par leur conception même, la rupture de la chaîne de conformité en phase d'exploitation.



	Afin que cette politique soit connue de ses adhérents et respectée par ses fournisseurs et sous-traitants, l'Amue publie sa politique externe de protection de données à caractère personnel sur son site Internet institutionnel.	
Cadre législatif	<u>Délibération n°2017-219 du 13 juillet 2017 portant modification du référentiel pour la délivrance de labels en matière de procédures de gouvernance tendant à assurer la protection des données</u>	
url présentation	<u>https://www.amue.fr/informations-legales/politique-externe-amue</u>	
Propriétaire		<u>http://www.amue.fr</u>
Commentaire	Notre politique externe de protection de la vie privée et des données à caractère personnel s'impose à tout agent de l'Amue amené à manipuler ce type de données ainsi qu'à toute personne physique ou morale externe intervenant pour notre compte dans la chaîne (de conception) des traitements, que ces derniers soient à usage interne ou externe (destinés à être exécutés par nos adhérents au moyen de notre offre applicative/SI).	



2.16. NOTATION BPMN

NOTATION BUSINESS PROCESS MODEL AND NOTATION (BPMN)		
Présentation	Business Process Model and Notation a été développée par la Business Process Management Initiative (BPMI), et est maintenant maintenue par l'Object Management Group (OMG) depuis leur fusion en 2005. Le but principal de BPMN est de fournir une notation qui soit réellement compréhensible par tous les utilisateurs de l'entreprise, depuis les analystes métier qui créent les ébauches initiales des procédures, jusqu'aux développeurs responsables de mettre en place la technologie qui va exécuter ces processus, et finalement, jusqu'aux utilisateurs de l'entreprise qui vont gérer et monitorer ces processus.	
Cadre législatif	Norme ISO ISO/IEC 19510:2013 - Technologies de l'information - Modèle de procédé d'affaire et notation de l'OMG	
url présentation	www.bpmn.org	
Propriétaire		www.bpmn.org
Commentaire	Sans objet.	