

NUMÉRO DU PROJET : PROJ-0001

TITRE DU PROJET : ÉLABORATION DE L'AE

AESSSS-001

ARCHITECTURE D'ENTREPRISE DU RSSS

PRINCIPES DIRECTEURS [A200S]

UNITÉ RESPONSABLE

Service des orientations stratégiques et architecture (SOSA)

Version : V1,0

Date de dernière mise à jour : 18 mai 2010

Code de documentation : 00000

Le présent document a été préparé par le Service des orientations stratégiques et architecture (SOSA) sous la Direction générale des technologies de l'information du ministère de la Santé et des Services sociaux du Québec, sous la direction de :

Marc Vézina, Directeur générale des technologies de l'information par intérim

RÉDACTION

Équipe de l'architecture d'entreprise du secteur de la santé et des services sociaux (AESSSS)

COLLABORATION

Architectes du SOSA

Personnel de la DGTI

Membres de la Table d'architecture du RSSS

Partenaires du réseau

REMERCIEMENTS

La Direction générale des technologies de l'information tient à remercier toutes les personnes ayant participé à la production de ce document.

Édition produite par :

La Direction générale des technologies de l'information du ministère de la Santé et des Services sociaux du Québec

Ce document n'est disponible qu'en version électronique :

<http://msss.gouv.qc.ca/extranet/index.html>

Le genre masculin utilisé dans ce document désigne aussi bien les femmes que les hommes.

Toute reproduction totale ou partielle de ce document est autorisée conditionnellement à la mention de la source.

© GOUVERNEMENT DU QUÉBEC, 2010

HISTORIQUE DU BIEN LIVRABLE

Version	Date	Commentaires	Intervenants
0,0	6 mai 2009	Création initiale du gabarit	Alain Perras
0,4	24 mai	Révision des principes des volets information, généraux et affaires. Ajout des volets sécurité et des services applicatifs	Robert Baril, Taha Chaabouni, Marc Beudet, André Langevin, Alain Perras
0,8	30 Juin 2009	Mise à jour des différents volets	Taha Chaabouni André Langevin Alain Perras
1,0	18 mai 2010	Prise en compte des commentaires de Simon Bégin sur l'ensemble des volets couverts	Robert Baril

TABLE DES MATIÈRES

1	PRÉAMBULE	4
2	PRINCIPES GÉNÉRAUX ET DE GESTION.....	5
3	PRINCIPES D’AFFAIRES.....	7
4	PRINCIPES D’INTÉGRATION.....	9
5	PRINCIPES D’INFORMATION	11
6	PRINCIPES DES SERVICES APPLICATIFS	12
7	PRINCIPES DE SÉCURITÉ.....	14
8	PRINCIPES TECHNOLOGIQUES.....	17

1 PRÉAMBULE

Dans l'univers des technologies de l'information, un principe directeur est une règle de l'architecture d'entreprise qui s'applique à un ensemble d'entités organisationnelles du secteur de la santé et des services sociaux (SSSS).

Il peut traiter de tous les aspects de l'architecture, et inclus, mais non exclusivement, les processus d'entreprise, les produits et services, les contrôles de gestion, les ressources humaines, financières, physiques et intellectuelles de l'entreprise.

Les principes directeurs peuvent être regroupés par volet, et chaque volet peut comprendre un ou plusieurs principes.

Les volets qui ont été élaborés dans le cadre du présent document sont :

- principes généraux et de gestion;
- principes d'affaires;
- principes d'intégration;
- principes d'information;
- principes des services applicatifs;
- principes de sécurité;
- principes technologiques.

2 PRINCIPES GÉNÉRAUX ET DE GESTION

Les principes généraux et de gestion concernent la réalisation, l'évolution et la gestion de l'architecture d'entreprise.

No	Principes	Description
Pr.GEG.01	Le MSSS a établi un cadre de gouvernance des ressources informationnelles auquel doit adhérer l'ensemble du SSSS.	<ul style="list-style-type: none"> • Énoncé : Les autorités ministérielles sont responsables de développer et de faire appliquer un cadre de gouvernance des ressources informationnelles pour l'ensemble du SSSS. L'ensemble des acteurs du SSSS doit donc y adhérer. • Justification : Une gouvernance forte permet d'assurer une utilisation optimale des investissements en matière de ressources informationnelles au sein du SSSS.
Pr.GEG.02	L'ensemble des constituantes du SSSS doit s'inscrire dans la mise en œuvre du plan d'informatisation des TI.	<ul style="list-style-type: none"> • Énoncé : Le MSSS est responsable de la définition du plan d'informatisation du SSSS. Ce plan a pour but de définir et de guider les projets d'investissements en TI en lien avec les plans d'affaires des directions générales du MSSS. Les acteurs du SSSS doivent donc s'y inscrire. • Justification : Le respect du plan d'informatisation permet à l'organisation d'augmenter l'efficacité et la rentabilité des investissements en TI.
Pr.GEG.03	L'ensemble des constituantes du SSSS doit respecter les normes adoptées par le MSSS.	<ul style="list-style-type: none"> • Énoncé : Toutes les nouvelles solutions informatiques du SSSS doivent respecter les orientations technologiques du MSSS et être en concordance avec les architectures, les principes directeurs, les normes et standards du MSSS et, le cas échéant, du gouvernement du Québec. Les acteurs du SSSS doivent donc respecter ces normes. • Justification : Les architectures, les principes directeurs, les normes et les standards permettent l'interopérabilité et l'échange d'information entre des systèmes hétérogènes. Cela favorise donc l'arrimage des actifs informationnels déjà en place et à venir.
Pr.GEG.04	Les solutions d'affaires doivent s'inscrire dans une démarche transformationnelle des processus.	<ul style="list-style-type: none"> • Énoncé : Toutes les nouvelles solutions TI du SSSS doivent s'inscrire dans une perspective transformationnelle des processus d'affaires. Cette perspective transformationnelle vise l'efficacité et l'efficacé, mais vise également l'optimisation dans l'utilisation des ressources (humaines, matérielles, financières et informationnelles).

		<ul style="list-style-type: none">• Justification : Le SSSS est en constante mouvance et se voit dans l'obligation d'assurer une transformation constante de ses processus d'affaires. Par conséquent, les solutions d'affaires doivent être offrir l'ouverture souhaitée pour se doter de toute l'agilité nécessaire afin s'adapter rapidement aux changements qui s'imposent.
--	--	--

3 PRINCIPES D'AFFAIRES

No	Principes	Description
Pr.AFF.01	<p>Toutes les décisions d'investissement du MSSS s'appuient sur les plans d'affaires des directions générales.</p>	<ul style="list-style-type: none"> • Énoncé : Les solutions d'affaires à favoriser doivent répondre aux besoins prioritaires des directions générales lesquels sont alignés avec le plan stratégique ministériel. Principalement, elles doivent contribuer à l'amélioration des soins et services des usagers et s'appuieront sur ces derniers. • Justification : Dans un contexte de rareté de ressources, il est nécessaire de s'appuyer sur une vision cohérente des besoins et des priorités d'affaires afin de prendre des décisions optimales d'investissement pour l'ensemble des projets. Ce sont les plans d'affaires qui fournissent la vision requise.
Pr.AFF.02	<p>La vision inter programmes et services doit être intégrée dans la conception des solutions TI.</p>	<ul style="list-style-type: none"> • Énoncé : Lors de la conception de solutions, il est nécessaire d'assurer une cohérence d'ensemble inter programmes et services. Les solutions doivent donc tenir compte du contexte de l'organisation qui dispense les services dans une perspective de continuum de soins de santé et de services sociaux. • Justification : Cette approche permettra d'éviter la conception de solutions en silo qui amènent des redondances dans le développement des solutions TI.
Pr.AFF.03	<p>Se doter d'une vision commune et suffisamment flexible pour tenir compte du contexte des constituantes du SSSS.</p>	<ul style="list-style-type: none"> • Énoncé : L'utilisation d'une vision commune sur les modèles TI doit nécessairement intégrer la possibilité de s'adapter aux contextes différents des constituantes du SSSS. • Justification : L'implantation de solutions non paramétrables dans le cadre du continuum de services donne des résultats contre-productifs.
Pr.AFF.04	<p>Toute solution doit respecter le cadre légal qui prévaut.</p>	<ul style="list-style-type: none"> • Énoncé : La dispensation des services au sein du SSSS se réalise à partir des ententes établies entre les organismes publics et les organismes privés. Les différentes lois qui encadrent la constitution et le fonctionnement de ces organisations doivent être respectées. • Justification : La protection de la confidentialité des informations et la garantie d'offrir un niveau de confiance à l'utilisateur en termes de protection de la vie

		privée sont des pré-requis dans les décisions d'investissements.
Pr.AFF.05	Rendre disponible l'information sur le lieu de l'action au moment de l'action.	<ul style="list-style-type: none"> • Énoncé : Ce principe sous-entend que les systèmes d'information doivent être en mesure de supporter une pluralité de technologies de manière à rendre disponible l'information au moment où l'action se passe et sur le lieu même de l'action. • Justification : En fait, ce principe vise essentiellement à décloisonner l'accessibilité de nos systèmes d'information pour supporter différentes technologies conventionnelles ou non, par exemple, téléphone intelligent, tablet PC, etc.. Ce principe tire son fondement de l'approche « Anytime, Any device, Anywhere ».

4 PRINCIPES D'INTÉGRATION

No	Principes	Description
Pr.INT.01	<p>Les registres des usagers, des intervenants, des organismes et des lieux dispensateurs de services doivent être considérés comme étant la source unique des données.</p>	<ul style="list-style-type: none"> • Énoncé : Le MSSS assure la mise en place des registres d'identification unique des usagers, intervenants, lieux et organismes dispensateurs de services. Les informations de ces registres doivent être utilisées par tous les systèmes d'information du SSSS qui ont besoin de ces données. • Justification : L'architecture de l'information du MSSS est basée sur l'utilisation de ces trois axes d'identification unique fondamentaux. Leur utilisation dans les systèmes d'information favorise les échanges, le partage et une centralisation de l'information.
Pr.INT.02	<p>Toutes les applications du SSSS doivent pouvoir s'arrimer à une gestion fédérée de l'authentification des intervenants.</p>	<ul style="list-style-type: none"> • Énoncé : L'intervenant ne doit s'authentifier qu'une seule fois. L'arrimage des applications à un service commun d'authentification de l'intervenant minimise le nombre d'identifiants et mots de passe que doivent posséder les intervenants. • Justification : Compte tenu du nombre important d'applications, de fonctions et/ou modules communs qui seront mis à contribution dans le SSSS, il n'est pas raisonnable d'imposer aux intervenants de s'authentifier auprès de chacun d'eux.
Pr.INT.03	<p>Minimiser le nombre de connexions point à point en utilisant des services d'intégration locaux, régionaux ou nationaux.</p>	<ul style="list-style-type: none"> • Énoncé : Plusieurs applications doivent être mises à contribution dans le SSSS pour supporter la prestation de soins de santé et de services sociaux. Souvent, ces systèmes doivent s'échanger des informations et, pour ce faire, utiliser des interfaces. Afin de minimiser le nombre d'interfaces à concevoir et à maintenir, on recommande l'utilisation de services d'intégration qui feront le pont entre les diverses applications, les diverses opérations et conversions nécessaires. • Justification : Sans agent d'intégration, le nombre d'interfaces croît selon l'expression : $(n \times (n-1))/2$ (où n est le nombre d'applications). Sans agent d'intégration, 5 systèmes qui voudraient s'échanger de l'information nécessiteraient 10 interfaces distinctes. Comme les interfaces sont dispendieuses à développer et à maintenir, la réduction de leur nombre est plus que souhaitable. L'utilisation de services d'intégration facilite également grandement la gestion de la sécurité des échanges d'information.
Pr.INT.04	<p>L'échange d'information entre</p>	<ul style="list-style-type: none"> • Énoncé : L'échange d'informations entre les

No	Principes	Description
	<p>les solutions au sein du SSSS doit respecter les normes et les standards édictés par le MSSS.</p>	<p>solutions informatiques doit s'effectuer au moyen de messages normalisés. Le contenu (ex. LOINC, SNOMED CT, etc) et le contenant de ces messages seront basés sur des normes ouvertes telles que HL7, XML et SOAP et les processus IHE.</p> <ul style="list-style-type: none"> • Justification : Les données des messages sont plus facilement accessibles et réutilisables lorsque des protocoles d'échanges communs et des standards sont établis et maintenus. L'échange via des messages normalisés assure une plus grande interopérabilité entre les applications, une réduction des coûts globaux de développement, d'entretien des systèmes et facilite l'évolution des applications.

5 PRINCIPES D'INFORMATION

No	Principes	Description
Pr.INF.01	La circulation de l'information doit se faire par l'utilisation des TIC.	<p>Énoncé : La circulation de l'information dans le SSSS doit s'effectuer en priorité par voie électronique.</p> <p>Justification : L'efficacité des communications électroniques devra améliorer l'efficacité et l'efficience du SSSS.</p>
Pr.INF.02	Chaque donnée d'un projet ou d'une solution doit être définie conformément à l'architecture d'information.	<p>Énoncé : Les solutions informatiques (informationnelles ou opérationnelles) déployées dans le SSSS ont l'obligation de produire des modèles de données qui respectent, lorsqu'existantes, les définitions standardisées des éléments de données contenues dans l'architecture d'information (modèle conceptuel corporatif de données et les cadres normatifs). De plus, chaque système ou solution devra démontrer sa conformité face à ces définitions tant du point de vue de la sémantique que du format utilisé.</p> <p>Justification : Dans un contexte où il existe plusieurs solutions hétérogènes ayant des données définies en silo, et en l'absence d'une référence commune, l'échange ou l'exploitation des données devient problématique. Pour pallier à cette difficulté, il est donc essentiel de partager la définition de la donnée et ce, tant sur le plan sémantique, que sur le plan des liens entre les données.</p>
Pr.INF.03	Chaque donnée opérationnelle devrait faire l'objet d'une saisie unique de façon à assurer la qualité des données.	<p>Énoncé 1 : Il est de la responsabilité du SSSS de s'assurer que la donnée doit être saisie une et une seule fois et ce, tant pour des fins opérationnelles et informationnelles.</p> <p>Justification : Éviter les saisies multiples et les collectes ad hoc. Cette approche permettra de rehausser la qualité de l'information traitée à partir des données saisies.</p>
Pr.INF.04	La définition des données opérationnelles doit être complétée par l'identification de ses différents usages informationnels le cas échéant.	<p>Énoncé 1 : Le modèle de données d'un système d'information doit tenir compte à la fois des besoins opérationnels et des besoins informationnels.</p> <p>Énoncé 2 : La donnée doit être utilisée pour répondre à la fois aux besoins opérationnels et informationnels. Dans ce cas, le modèle d'exploitation des données (modèle en étoile ou les cubes) doit compléter le modèle de sauvegarde des données (modèle de données normalisé).</p> <p>Justification : En accord avec le principe de la saisie unique, ce principe permet, d'une part, d'éviter les modifications coûteuses aux TI a posteriori et, d'autre part, de limiter les collectes de données ad hoc (à travers des interfaces web qui sont coûteuses). Il permet également d'améliorer la qualité des données dans les banques de données communes (BDC) ainsi que la qualité des indicateurs. Pour ce faire, il faut faire la différence entre les données calculées, agrégées et les données primaires.</p>

6 PRINCIPES DES SERVICES APPLICATIFS

No	Principes	Description
Pr.APP.01	<p>Le SSSS doit se doter d'une vision de l'utilisateur au cœur même des services d'affaires et systèmes de manière à favoriser l'accessibilité aux informations.</p>	<ul style="list-style-type: none"> • Énoncé : Adopter une approche de développement des solutions qui soit centrée sur l'information sur l'utilisateur. • Justification : Dans le passé, les systèmes d'information déployés dans le SSSS ont été développés en silos, avec une interopérabilité difficile, et concernent habituellement un ou des services d'affaires sans tenir compte d'une vision intégrale de l'utilisateur dans l'ensemble de ses soins de santé ou de services sociaux. En d'autres mots, il n'existe pas de trame de fond qui met l'utilisateur au cœur même de l'ensemble de ses soins de santé ou de services sociaux et ce, tant à un niveau local, régional que provincial. Cette problématique ne permet également pas à l'utilisateur ou à l'intervenant d'avoir une vision intégrée des soins de santé et de services sociaux qui leur sont propres.
Pr.APP.02	<p>Le SSSS doit se doter d'une vision de l'intervenant au cœur même de l'utilisation des services d'affaires et systèmes de manière à en garantir l'accessibilité</p>	<ul style="list-style-type: none"> • Énoncé : Mettre l'intervenant au cœur de l'action des services d'affaires et/ou systèmes d'information du réseau socio-sanitaire afin de lui en assurer l'accessibilité. • Justification : Les systèmes d'information déployés dans le SSSS ont été développés en silos et adressent habituellement un ou des services d'affaires sans tenir compte d'une vision intégrale de l'intervenant dans l'ensemble des services qu'il est susceptible d'utiliser. Il est également difficile pour l'intervenant d'avoir accès de manière intégrée à l'ensemble des services d'affaires ou systèmes d'information qui lui sont rendus disponibles dans l'exécution des tâches qui sont sous sa responsabilité. De plus, la mobilité des intervenants permet difficilement d'avoir un accès facile et intégré aux services et dossiers intégraux des usagers et ce, peu importe où ils se situent.
Pr.APP.03	<p>Favoriser, dans l'ordre suivant, la réutilisation, la mise en commun et l'acquisition de solutions de TI.</p>	<ul style="list-style-type: none"> • Énoncé : Il apparaît clairement pour le MSSS que la mission première des constituantes du réseau socio-sanitaire n'est pas le développement de solutions de TI, mais qu'elles ont plutôt pour rôle d'en assurer le déploiement, l'expertise, le support et le maintien. • Justification : S'assurer du respect de la politique du faire faire édictée par le MSSS en matière de dotation en solutions en TI.

No	Principes	Description
Pr.APP.04	<p>Les applications doivent respecter les règles d'intégrité, d'intégralité, de pertinence et les conditions de disponibilité des données définies dans l'architecture d'information.</p>	<ul style="list-style-type: none"> • Énoncé : Les règles de validation, de saisie, de transmission et d'accès aux données par les applications doivent être conformes aux règles d'intégrité et les conditions de disponibilité des données définies dans l'architecture d'information. Ces dernières seront arrimées au volet de sécurité de l'architecture d'entreprise. • Justification : Pour assurer l'intégrité des données, une standardisation des règles qui encadrent ces considérations permet d'harmoniser les mécanismes de sécurité sur les données et atteindre l'objectif ciblé.
Pr.APP.05	<p>Les données, règles d'affaires et modes de présentation doivent être vus de manière indépendante des traitements.</p>	<ul style="list-style-type: none"> • Énoncé : De manière à assurer une réutilisation optimale, la mise en commun, le développement modulaire, l'agilité de l'AE et de ses RI, il est essentiel que la conception des systèmes d'information s'assure de l'indépendance des données, règles d'affaires, modes de présentation par rapport aux traitements. • Justification : Renforcer l'importance au découplage des systèmes d'information développé au sein du SSSS et assurer une réutilisation optimale des composantes des TI.

7 PRINCIPES DE SÉCURITÉ

No	Principes	Description
Pr.SEC.01	<p>La portée de l'architecture d'entreprise volet sécurité assure la couverture complète du SSSS.</p>	<ul style="list-style-type: none"> • Énoncé : Le volet sécurité de l'architecture d'entreprise du MSSS s'applique sur toute information saisie et emmagasinée sur un actif informationnel du SSSS. Par effet transitif, tout poste de travail, périphérique, serveur, lieux de travail, processus de gestion est couvert par le volet sécurité de l'architecture d'entreprise. Le volet sécurité de l'architecture d'entreprise est responsable d'émettre des orientations dont la mise en œuvre relève du réseau. « Le ministre définit les orientations et les standards en matière d'actifs informationnels en soutien à la gestion du réseau de la santé et des services sociaux et les agences sont responsables de leur mise en œuvre dans le réseau de la santé et des services sociaux. <p>Le ministre détermine les règles et les modalités de gestion relatives aux services de certification et aux services de répertoire offerts dans le secteur de la santé et des services sociaux que tout prestataire de services de certification désigné conformément au paragraphe 1 du premier alinéa de l'article 520.3.3 et que tout prestataire de services de répertoire visé par la présente loi doivent respecter.</p> • Justification : L'information emmagasinée dans le RSSS est propriété soit des usagers soit des intervenants et à ce titre, le volet sécurité de l'architecture d'entreprise doit assurer son maintien selon les règles et conditions du DICA (source « Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale »,) <ol style="list-style-type: none"> a) la « disponibilité », laquelle est la propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée; b) l'« intégrité », laquelle est la propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation ; c) la « confidentialité », laquelle est la propriété d'une information de n'être accessible qu'aux personnes autorisées ; d) l'« authentification », laquelle est un acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif ; e) l'« irrévocabilité », laquelle est la propriété

No	Principes	Description
		d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.
Pr.SEC.02	Les approches et solutions en sécurité doivent respecter la législation, les sources de droit, et les énoncés de politique	<ul style="list-style-type: none"> • Énoncé : Le volet sécurité de l'architecture d'entreprise du MSSS repose sur la législation en vigueur et énoncés de politiques actifs. Le respect de la vie privée et le droit à la confidentialité des informations découlent du Code civil du Québec et les solutions et approches de sécurité au niveau des intervenants et des utilisateurs doivent respecter les lois. De plus, le volet sécurité s'inspire des travaux précédents soit (liste non exhaustive) " Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale ", AGSIN et autres... • Justification : Plusieurs orientations importantes en sécurité ont été amenées par les lois et directives et l'architecture de sécurité doit en tenir compte pour assurer la cohérence dans l'ensemble du réseau.
Pr.SEC.03	Assurer à l'intervenant habilité, un accès à l'information de santé et services sociaux requis à sa pratique, en tout temps, tout lieu et sur une variété de périphériques - utilisant une seule identité numérique globale supportée par l'ensemble des actifs informationnels du RSSS et respectant leur catégorisation pour répondre aux lois et règlements en vigueur .	<ul style="list-style-type: none"> • Énoncé : La sécurité s'applique sur les données, les objets (postes de travail, équipements ou autre) ainsi que les lieux. A terme il n'y a pas d'accès générique et des règles d'accès devront exister pour l'ensemble des éléments appartenant au SSSS. Pour l'ensemble des intervenants du réseau de la santé et/ou pour les usagers du réseau, à terme, une seule et unique identité électronique doit exister pour assurer les accès aux informations/données. Le corollaire de cet énoncé signifie que chaque application doit avoir la capacité intrinsèque de reconnaître l'intervenant ou l'utilisateur. • Justification : Le fait de disposer de plusieurs identités électroniques est contre-productif et diminue le niveau de sécurité de l'ensemble du domaine, car les usagers ne peuvent alors retenir tous les mots de passe et autres mécanismes utilisés. Le changement d'identité successivement pour un même utilisateur entraîne une perte de temps productif dans sa pratique ce qui a un effet sur la productivité globale du réseau de la santé.
Pr.SEC.04	Les mécanismes d'identification et d'authentification en usage dans le SSSS doivent respecter le contexte de travail et les différentes tâches des	<ul style="list-style-type: none"> • Énoncé : Les mécanismes d'identification et authentification utilisés doivent s'insérer de façon transparente dans l'utilisation quotidienne des équipements, des applications, des lieux de travail. Les solutions doivent s'adapter aux intervenants et non l'inverse.

No	Principes	Description
	intervenants.	<ul style="list-style-type: none"> • Justification : Les intervenants du réseau de la santé sont des ressources critiques dont la productivité se reflète directement sur la capacité globale du réseau d'offrir des soins à la population; on doit chercher en tout temps à minimiser les impacts de la technologie et ses contraintes auprès des intervenants.
Pr.SEC.05	Les solutions de sécurité préconisées et en usage doivent s'appuyer sur des standards reconnus et provenir de fournisseurs pouvant garantir leur pérennité.	<ul style="list-style-type: none"> • Énoncé : Assurer l'interopérabilité et la capacité d'évolution de toute solution de sécurité ou choix technologique utilisé pour assurer la sécurité des informations, des lieux ou des personnes. • Justification : Les menaces et risques évoluent et sont alimentés par des conditions internationales. Les fournisseurs de solutions et de technologies suivent ces grands mouvements et répondent, par leur offre de services, à ces problématiques. En conséquence, les pratiques et solutions techniques retenues par l'architecture de sécurité doivent être réévaluées périodiquement afin de tenir compte des changements organisationnels et technologiques ainsi que de l'évolution des menaces et des risques. La seule façon de garantir l'interopérabilité à moindres coûts des solutions est d'utiliser les standards de l'industrie.

8 PRINCIPES TECHNOLOGIQUES

No	Principes	Description
Pr.TEC.01	L'infrastructure technologique d'un établissement doit être gérée et doit évoluer de façon à infléchir le coût total de propriété (CTP).	<ul style="list-style-type: none"> • Énoncé : Le CTP du RSSS est en évolution constante et l'accroissement de la complexité des infrastructures et des progiciels est aussi un facteur aggravant. Chaque organisation doit mesurer son CTP et veiller à l'infléchir en faisant les choix et les acquisitions appropriés. • Justification : Sans un effort constant et une veille attentive de la part de chaque organisation décisionnelle dans les choix techniques, le CTP continuera d'augmenter.
Pr.TEC.02	L'infrastructure technologique du SSSS doit être exploitée selon les meilleures pratiques de l'industrie et les recommandations des manufacturiers.	<ul style="list-style-type: none"> • Énoncé 1 : Les composantes technologiques (Serveurs, postes, logiciels d'exploitation et d'entretien, réseautique, composantes de virtualisation, etc.) nécessitent toutes d'être gérées selon un cadre de gestion propre à leur manufacturier d'origine. En sus des guides d'opération produits par les manufacturiers, il existe aussi des standards de meilleures pratiques (COBIT, ITIL) qui devraient servir de base à la prise en charge de toute composante. • Énoncé 2 : Les composantes technologiques doivent être constamment tenues à jour et des outils et processus doivent être mis en place, lors de l'acquisition d'une composante, pour assurer la capacité d'en gérer l'évolution. • Justification : La gestion opérationnelle des composantes technologiques est l'élément qui contribue le plus aux bénéfices attendus par ces technologies. Le volet gestion est le plus souvent le poste comptable le plus élevé de tous dans l'ensemble du coût total de propriété des TI.
Pr.TEC.03	Le SSSS doit favoriser l'acquisition de solutions commerciales pour les infrastructures matérielles et logicielles lorsque les manufacturiers peuvent démontrer la viabilité de leur entreprise et de leur solution.	<ul style="list-style-type: none"> • Énoncé 1 : Il faut préconiser de réutiliser plutôt que d'acheter et d'acheter plutôt que de développer ou assembler des composantes technologiques pour rencontrer un besoin d'affaires. Cependant si la viabilité d'un fournisseur ou de sa solution peut être remise en cause, alors il peut être justifié si aucune autre solution n'existe, de procéder autrement. • Énoncé 2 : Les logiciels qui suivent le modèle de licence de type GNU GPL (ou ses variantes) – appellation de logiciels libres - peuvent être acquis lorsque soutenus par une entreprise commerciale

		<p>viable et externe au réseau de la santé.</p> <ul style="list-style-type: none"> • Justification : Une application commerciale vendue et supportée par un fournisseur reconnu est plus rapidement utilisable, moins coûteuse à mettre en œuvre et entraîne beaucoup moins de risque que de tenter de créer un logiciel maison pour soutenir les mêmes fonctions. C'est vrai pour les fonctions d'affaires, et encore plus vraies pour les fonctions techniques (technologiques). Le RSSS en recherche d'amélioration du coût total de propriété des TI doit se fier exclusivement sur des fonctions soutenues commercialement pour arriver à réduire ses coûts.
Pr.TEC.04	<p>Les applications développées ou acquises doivent être modulaires et conformes aux environnements d'exploitation du SSSS.</p>	<ul style="list-style-type: none"> • Énoncé 1 : Les applications ciblant une plateforme logicielle doivent avoir été développées en tenant compte des fonctionnalités de la version courante de la plateforme et doivent pouvoir manifester un haut niveau de compatibilité pour cette dernière. • Énoncé 2 : Les applications développées ou acquises de fournisseurs doivent soutenir un modèle de découpage en 2 ou 3 tiers, mais permettre en tout temps de s'installer sur un service de banque de données consolidées déjà acquis et implanté. • Énoncé 3 : Les applications commerciales doivent être accompagnées de leur propre procédure d'installation et fichiers de montages et doivent être accompagnées de documentation pour packaging sur serveur conventionnel, serveur virtuel ou serveur en mode service terminal. • Énoncé 4 : Les applications développées ou acquises doivent pouvoir s'installer par modules séparant les fonctions de présentation, de l'application, et de la base de données. • Justification : Dans un esprit d'efficacité et de simplification des tâches d'administration, assurer aux administrateurs de système le maximum de souplesse dans l'implantation et la mise en œuvre d'un logiciel commercial qui est installé sur la plateforme d'un établissement. Les fournisseurs ne pourront plus demander de configurations spécifiques pour leurs produits ou d'imposer une configuration « boîte noire ».
Pr.TEC.05	<p>Les services de réseautique doivent être configurés, entretenus et mesurés afin de répondre aux besoins des lieux de dispensation de services.</p>	<ul style="list-style-type: none"> • Énoncé : Les services appropriés de réseautique doivent être acquis pour soutenir les besoins d'affaires et doivent être mesurés pour valider l'adéquation avec la qualité de service du réseau. • Justification : Les établissements doivent pouvoir compter sur une infrastructure réseau fiable et performante pour bâtir leurs infrastructures de

		téléphonie IP et de collaboration. Certains établissements ont besoins de l'agilité nécessaire pour déployer leurs propres accès Internet secondaires, liens de relève et accès sans-fil.
--	--	---