



**Unité
des technologies
de l'information et
des communications**

Centres hospitaliers
de soins de courte durée

27 mai 2015

Répertoire
des
guides
de
planification
immobilière

Québec 

ÉDITION

La Direction des communications du ministère de la Santé et des Services sociaux

Le présent document s'adresse spécifiquement aux intervenants du réseau québécois de la santé et des services sociaux et n'est accessible qu'en version électronique à l'adresse :

<http://intranetreseau.rtss.qc.ca> ou www.msss.gouv.qc.ca section **Documentation, rubrique **Publications****

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

Dépôt légal

Bibliothèque et Archives nationales du Québec, 2015

Bibliothèque et Archives Canada, 2015

ISBN : 978-2-550-73524-3 (version PDF)

Tous droits réservés pour tous pays. La reproduction, par quelque procédé que ce soit, la traduction ou la diffusion de ce document, même partielles, sont interdites sans l'autorisation préalable des Publications du Québec. Cependant, la reproduction de ce document ou son utilisation à des fins personnelles, d'étude privée ou de recherche scientifique, mais non commerciales, sont permises à condition d'en mentionner la source.



Unité des technologies de l'information et des communications

Coordination et rédaction générale

Céline Drolet, architecte
Direction de l'expertise et de la normalisation
Ministère de la Santé et des Services sociaux (Ministère)

Esther Rinfret, ingénieure, M.B.A.
Direction de l'expertise et de la normalisation
Ministère

Remerciements

Le présent guide a été réalisé grâce à la collaboration des personnes et organismes suivants :

Collaborateurs

Sylvie Bouffard, architecte
Direction de l'expertise et de la normalisation
Ministère

André Matte, ingénieur
Direction de l'expertise et de la normalisation
Ministère

Daniel Pelletier, ingénieur
DGTI – Direction des orientations et de l'architecture
Ministère

Anne Pelletier, ingénieure,
Direction de l'expertise et de la normalisation
Ministère

Comité de lecture

Daniel Pelletier, ingénieur
DGTI – Direction des orientations et de l'architecture
Ministère

Michel Beaudoin, B.A.A.
Responsable – Secteur TI
Groupe Biomédical Montérégie
Agence de la Montérégie

Jocelyn Hamel, PMP
Chargé de projet et architecte technologique
DGTI – Direction des orientations et de l'architecture
Ministère

Claude Pérusse, M.Sc., MAP, PMP
Directeur adjoint des services-conseils en technologies
Groupe Biomédical Montérégie
Agence de la Montérégie

Martin Kirouac, Ph. D.
Conseiller en planification d'équipement
Groupe Biomédical Montérégie,
Agence de la santé et des services sociaux(Agence) de la Montérégie

Denis Vallière, ingénieur
Coordonnateur en électricité
Direction Expertise technique et Estimation
SQI

François St-Yves, ingénieur, M. Sc.
Direction Expertise technique et Estimation
Société québécoise des infrastructures (SQI)

André Bélisle, ingénieur, PMP, CDCDP
DGTI – Direction des orientations et de l'architecture
Ministère

Jason White
Consultant
Direction Opérations en technologies de l'information
SQI

Les lecteurs suivants ont été désignés par l'Association québécoise d'établissements de santé et de services sociaux :

Mario Houle, ingénieur, directeur
Direction des ressources informationnelles et services techniques
CSSS d'Antoine-Labelle

Riadh Benziane
Responsable de l'informatique
CSSS Cavendish

Marc Bélisle, M. Sc.
Directeur des ressources informationnelles et du biomédical
CSSS d'Ahuntsic et Montréal-Nord

Bertrand Carrier, M. Sc., CPA, CMA,
Chef du service des ressources financières et
informationnelles – adjoint à la DSA
CSSS de la MRC-de-Coaticook

Julie Whissel, directrice adjointe
Soutien technique et informationnel
Direction des services financiers et techniques
Centre de santé et de services sociaux (CSSS) de Gatineau

Stéphane Landry,
Chef de service – Technocentre de Québec
Technocentre de la région de la Capitale-Nationale

Le lecteur suivant a été désigné par le Regroupement des directeurs des services techniques associés :

Carl Therrien, ingénieur
Conseiller en bâtiment – GBE
Institut universitaire en santé mentale de Montréal

Visites

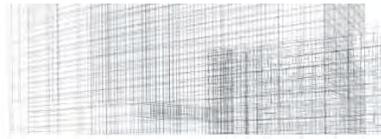
Finalement, nous remercions Daniel Pelletier, André Bélisle et Jocelyn Hamel, de l'équipe de la Direction générale des technologies de l'information, ainsi que Michel Beaudoin, Claude Pérusse et Martin Kirouac, de l'équipe du Groupe biomédical Montérégie. Leur contribution a été grandement appréciée.

Nous remercions également l'équipe du Centre hospitalier affilié universitaire de Québec, Hôpital de l'Enfant-Jésus, qui nous a reçus et nous a permis de partager ses expériences en vue de faire progresser le présent guide, ainsi que l'équipe du Centre hospitalier de l'Université Laval qui nous a fait visiter ses installations. Leur contribution a aussi été grandement appréciée.



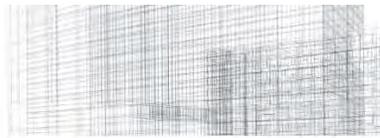
Table des matières

DOMAINE D'APPLICATION	1
1. Contexte.....	1
1.1 Définition	1
1.2 Description des activités	1
1.3 Description des usagers.....	4
1.4 Logistique.....	4
1.5 Risques	5
1.5.1 Emplacement des locaux	5
1.5.2 Maintien des activités	6
1.5.3 Adaptabilité et flexibilité des infrastructures	6
1.6 Tendances.....	6
1.7 Encadrement légal	8
2. Éléments de programmation.....	9
2.1 Critères de conception	9
2.1.1 Fonctionnalité	9
2.1.2 Confort et ambiance	9
2.1.3 Sécurité	10
2.1.4 Opération et entretien.....	10
2.2 Organisation spatiale	10
2.2.1 Description des secteurs d'activité de l'Unité des technologies de l'information	10
2.2.2 Liaisons fonctionnelles	11
2.2.3 Schéma organisationnel.....	12
2.2.4 Sous-composantes, locaux et espaces.....	13
2.3 Locaux spécifiques.....	14
2.4 Calcul des superficies	16
3 Objectifs de performance technique	17
3.1 Généralités.....	17
3.2 Unifomat II.....	18
Annexe	30
Références.....	32



Liste des abréviations

ASSC	Alimentation statique sans coupure
CCQ	Code de construction du Québec
CH	Centre hospitalier
CHA	Centre hospitalier affilié
CSSS	Centre de santé et de services sociaux
CTI	Centre de traitement informatique
CVCA	Chauffage, ventilation et conditionnement d'air
DGTI	Direction générale des technologies de l'information
DPE	Dossier patient électronique
DSQ	Dossier Santé Québec
ITS	Indice de transmission sonore
MALT	Mise à la terre
RAMQ	Régie de l'assurance maladie du Québec
RDM	Retraitement des dispositifs médicaux
RITM	Réseau intégré des télécommunications multimédia
RSSS	Réseau de la santé et des services sociaux
TIC	Technologies de l'information et des communications
UTIC	Unité des technologies de l'information et des communications



Domaine d'application

Le présent guide expose les objectifs relatifs aux performances fonctionnelles et techniques applicables pour la programmation, la conception et la construction de l'Unité des technologies de l'information et des communications (UTIC), incluant les centres de traitement informatique (CTI) de données, de soutien et d'expertise, ainsi que les centres de développement, que l'on retrouve dans tous les types de bâtiments du réseau de la santé et des services sociaux (RSSS). Ajoutons qu'il sera également question dans ce guide de la salle des serveurs, des salles réservées aux technologies de l'information et des communications (salles des TIC satellites¹) et du local d'entrée des services.

Les recommandations contenues dans ce guide de planification immobilière sont applicables à toutes les installations du RSSS, aux UTIC faisant partie de structures indépendantes, ainsi qu'aux projets de location et aux projets en impartition. La mise en application de ces recommandations n'a pas force de loi mais se veut une invitation à utiliser les meilleures pratiques qui soient dans ce milieu. Elle vise la qualité des services, la sécurité des personnes qui circulent dans l'UTIC ainsi que la sécurité des actifs informationnels.

1. Contexte

1.1 Définition

La fonction principale de l'UTIC consiste à assurer l'utilisation optimale des installations et systèmes relatifs aux technologies de l'information et des communications, afin que ceux-ci répondent efficacement aux besoins des usagers (patients), des médecins et du personnel du RSSS.

L'UTIC offre l'ensemble des services associés à l'hébergement et au bon fonctionnement des actifs informationnels. Physiquement, outre les espaces ou postes de travail nécessaires aux activités effectuées par le personnel, cette unité inclut l'ensemble des locaux hébergeant les équipements, les installations et les systèmes nécessaires à la prestation des services en matière de TIC. D'autre part, les espaces, les locaux et les composantes qui constituent l'UTIC peuvent être regroupés dans un seul bâtiment, à usage unique ou multiple, ou encore être répartis sur plusieurs sites ou bâtiments.

1.2 Description des activités

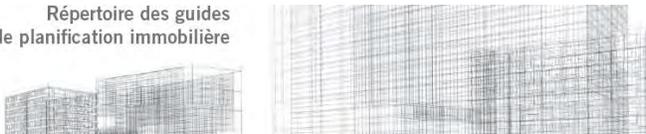
La description qui suit reste sommaire. Elle a pour principal objectif d'informer le lecteur, plus particulièrement celui occupant des fonctions essentielles dans le domaine immobilier (ex. : architecte, ingénieur, administrateur), et dont les préoccupations ont pour objet la planification des activités liées au bon fonctionnement de l'UTIC.

Fonctionnement

L'UTIC assure des services de jour et de nuit, fournissant soutien et assistance en tout temps (24 heures sur 24, 7 jours sur 7). Outre le fait que cette unité doit assurer un accès quotidien aux services électroniques du réseau intégré des télécommunications multimédia (RITM) à ses utilisateurs, elle doit également gérer de façon sécuritaire des systèmes qui traitent et acheminent des données jugées essentielles et confidentielles. Le RITM², un réseau rapide et hautement sécurisé, permet l'échange de données tout en assurant la confidentialité de l'information.

1. Les salles des TIC satellites sont réparties sur différents étages, de façon superposée, à l'intérieur d'un même bâtiment.

2. Une description plus complète du RITM est donnée sur le site du Centre de services partagés Québec : [\[http://www.cspq.gouv.qc.ca/faire-affaire-avec-le-cspq/famille-de-services/sous-famille-de-services/services/service/reseau-integre-de-telecommunications-multimedia-ritm/?no_cache=1\]](http://www.cspq.gouv.qc.ca/faire-affaire-avec-le-cspq/famille-de-services/sous-famille-de-services/services/service/reseau-integre-de-telecommunications-multimedia-ritm/?no_cache=1)



Le RITM sert également à la circulation de l'information entre le Dossier Santé Québec (DSQ) et le Dossier patient électronique (DPE). Ce réseau permet le téléaccès (télétravail), la visioconférence et la télésanté tout en facilitant les échanges spécialisés en cardiologie, en radiologie, en pathologie et en oncologie, entre autres, ainsi qu'en ce qui a trait à la formation médicale.

Voici quelques exemples d'activités de l'UTIC :

- l'opération, le maintien et l'amélioration des systèmes informatiques et téléphoniques, ainsi que des services de télécommunication;
- la gestion et l'amélioration de l'infrastructure de réseau;
- l'achat des divers équipements, logiciels et câbles;
- le support aux usagers (dépannage, documentation, formation, etc.);
- la réparation et l'entretien d'équipements relatifs aux technologies de l'information.

Compte tenu de son rôle dans le maintien des services destinés à la population ainsi qu'aux différents intervenants du RSSS (établissements, professionnels, médecins, etc.), et compte tenu des informations et des équipements qu'elle héberge, l'UTIC est un secteur hautement sécurisé dont l'accès est restreint, en particulier en ce qui concerne la salle des serveurs dans une installation donnée ou un CTI de données servant exclusivement aux besoins d'un bâtiment donné. La **sécurité** et la **redondance** des systèmes sont deux notions de première importance dont il faut absolument tenir compte en tout temps, tout en considérant que l'UTIC peut agir également comme centre de relève.

L'intégration des TIC dans les infrastructures de parcs immobiliers en grande partie déjà existants a eu pour conséquence que l'on retrouve aujourd'hui dans ces parcs immobiliers des UTIC dont la topologie organisationnelle et les dimensions sont très variées. La variation de cette topologie organisationnelle peut aussi être observée dans les parcs immobiliers neufs du fait que les standards, les normes, les technologies et les besoins évoluent rapidement.

Orientations DGTI-Ministère

La classification Tier II, telle que définie par l'Uptime Institute, correspond au niveau minimum de performances techniques que l'UTIC doit respecter (salle des serveurs et salles des TIC satellites). Toutefois, les exigences en matière de performances techniques décrites dans la section D du guide de l'UTIC devront permettre de se rapprocher de la classification Tier III, lorsque la criticité des enjeux relatifs aux services offerts l'exige.

Il est à noter que plusieurs organismes ne répondent qu'à la classification Tier II. Il faut donc considérer ce fait lors du choix de la classification Tier, qui doit être définie en fonction des critères mentionnés dans le document suivant :

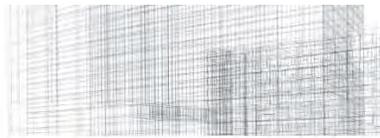
UPTIME INSTITUTE – Data Center Site Infrastructure Tier Standard: Topology

Note :

Voici quelques brèves descriptions des principales classifications Tier selon le type de fonctionnement d'un bâtiment ou d'une installation. Toutefois, afin de tenir compte de toutes les exigences à respecter, il importe de se référer aux normes de l'Uptime Institute.

À titre d'exemple, la norme *Data Center Site Infrastructure Tier Standard: Topology*, définit, de façon générale, les différentes classifications comme suit :

- **Tier I – Infrastructure de base** : aucune redondance en ce qui a trait à la capacité des équipements et des réseaux de distribution mécanique et électrique.
- **Tier II – Infrastructure avec composantes redondantes** : redondance (minimalement N+1*) des équipements électromécaniques, à l'exception des réseaux de distribution mécanique et électrique, qui sont simples.
- **Tier III – Infrastructure parallèle** : redondance (minimalement N+1*) des équipements électromécaniques et des réseaux de distribution mécanique et électrique parallèles (un réseau de distribution en service et l'autre en attente) permettant l'entretien planifié de n'importe quelle composante électromécanique sans affecter le fonctionnement des installations.



- **Tier IV – Infrastructure insensible aux défaillances :** installations électromécaniques multiples, indépendantes et isolées, fonctionnant parallèlement et simultanément, de façon à garantir le service sans interruption, peu importe la défaillance.

De plus, pour aider à la compréhension des différentes classifications, la norme ANSI/TIA-942 – *Telecommunications Infrastructure Standard for Data Centers* comporte des informations utiles permettant l'interprétation et la compréhension des différentes classifications.

* Dans l'expression « N+1 », « N » représente le nombre d'équipements requis pour satisfaire à la demande normale et « +1 » indique le nombre d'équipements additionnels nécessaires pour répondre à cette demande.

Recommandations soutenant les orientations ministérielles

Les orientations ministérielles contenues dans le *Plan stratégique 2010-2015 du ministère de la Santé et des Services sociaux (Ministère)* recommandent le regroupement des enjeux 4 (« La qualité des services de l'innovation ») et 6 (« Une gestion performante et imputable ») définis dans ce document. Ceux-ci visent à assurer la circulation de l'information clinique et l'intégrité de celle-ci, et à améliorer la performance du système de santé et des services sociaux. Quant aux utilisateurs, ils comptent sur la disponibilité en tout temps des applications et des systèmes de même que sur leur performance. Toujours dans le même esprit, le Ministère accorde la priorité à la mise en place d'un volet technologique performant de nature à soutenir les orientations suivantes :

- informer la population sur son état de santé et de bien-être et sur les moyens de le maintenir ou de l'améliorer;
- optimiser l'utilisation des ressources informationnelles et la circulation de l'information clinique en vue de favoriser l'intégration des services;
- soutenir l'organisation des activités universitaires dans le secteur de la santé;
- rendre accessible des installations robustes, performantes et ayant une disponibilité en tout temps pour répondre aux besoins de la population et des utilisateurs.

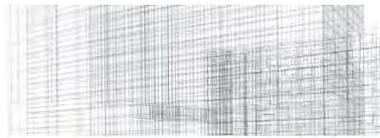
Optimisation

Quand il s'agit d'optimiser l'utilisation des ressources et la circulation de l'information doit-on parler de consolidation ou de décentralisation ? Lorsque l'on parle d'un CTI de données exclusif, on parle de consolidation (centralisation). Lorsque l'on parle de la salle des serveurs dans un établissement donné, on parle de décentralisation. Le présent guide vise actuellement les bâtiments dont les besoins sont assurés par leur propre salle des serveurs et leurs propres salles des TIC satellites. Toutefois, les recommandations et orientations ministérielles doivent se refléter dans les CTI de données. Il faut donc considérer que bon nombre d'installations ont leur propre salle des serveurs. De plus, même si une centralisation peut être considérée, on doit pouvoir avoir accès en tout temps à certains équipements essentiels (ex. : ASSC) sur le site même d'un bâtiment, cela afin d'assurer un dépannage plus rapide en cas de besoin et d'agir sans délai si un problème de groupe électrogène survient.

Politique de sécurité

Le Ministère, en collaboration avec ses partenaires du RSSS, la Régie de l'assurance maladie du Québec (RAMQ) et la Direction générale des technologies de l'information (DGTI), a mis au point une politique de sécurité relative aux informations nominatives informatisées (ex. : dossier patient électronique³). Cette politique met en œuvre un ensemble de mesures de sécurité logique, physique, humaine et organisationnelle visant à assurer la confidentialité, l'intégrité et la disponibilité de l'information, et à prévenir les risques associés à une opération ou à une autre au moment de sa collecte, de son entreposage, de son traitement ou de sa transmission.

3. Se référer au glossaire pour de plus amples informations au niveau du dossier patient électronique.



Sécurité des actifs informationnels

La sécurité physique concerne tant les équipements, les fournitures, les serveurs, le matériel de télécommunication et autres actifs informationnels du même genre. Pour assurer la sécurité physique des actifs informationnels appartenant aux organismes faisant partie du RSSS, des mesures concernant l'emplacement des installations et du matériel, le contrôle de l'accès aux locaux et, pour l'inventaire, l'entretien et la disposition du matériel informatique, doivent être appliquées.

Le document : « Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité » regroupe l'ensemble des textes encadrant la sécurité des actifs informationnels, soit la « Politique nationale sur la sécurité des actifs informationnels », les « Rôles et responsabilités des acteurs en matière de sécurité », les « Mesures en matière de sécurité des actifs informationnels » et le « Répertoire des procédures optionnelles en cette matière de sécurité des actifs informationnels » (voir en annexe quelques-uns des éléments de ce cadre de gestion).

Les mesures en matière de sécurité des actifs informationnels (sécurité physique, logique, de l'exploitation des actifs, des applications, des télécommunications, etc.) doivent être mises en place par les organismes faisant partie du RSSS, de même que par les utilisateurs des actifs informationnels de ces organismes, afin d'assurer la sécurité des actifs en question. Ces mesures constituent le minimum auquel les organismes et les utilisateurs sont astreints. Elles s'appliquent au Ministère et aux différents partenaires du RSSS. Elles servent de base aux responsables de la gestion de la sécurité des actifs informationnels pour définir les mesures propres à l'organisme pour lequel ils travaillent.

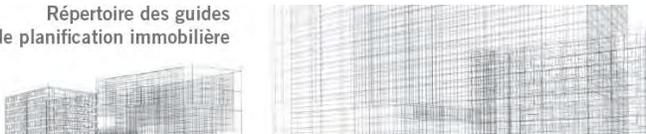
1.3 Description des usagers

En ce qui concerne l'utilisation des actifs informationnels du RSSS, deux groupes d'utilisateurs se distinguent : 1) le personnel et 2) les visiteurs.

1. **Personnel :** Ce groupe est composé du personnel administratif et du personnel attribué aux technologies de l'information et des communications. Selon leur fonction, on doit réserver aux membres du personnel un espace de travail qui leur est propre (ex. : bureau ouvert, atelier, bureau fermé ou autre) et, en vertu du protocole de sécurité adopté, certains d'entre eux seront autorisés à accéder aux aires sécurisées dans lesquelles sont logés les ordinateurs, les serveurs des réseaux locaux, le matériel de télécommunication ainsi que les autres actifs informationnels.
2. **Visiteurs :** Ce groupe est composé du personnel externe à l'UTIC (personnes s'occupant de l'hygiène et de la salubrité, de l'entretien des installations, etc.) ainsi que des visiteurs tels que les fournisseurs, les consultants et les spécialistes chargés de l'entretien et de la réparation des équipements ou offrant des types de services qui ne sont pas du ressort du personnel de l'UTIC. Selon les politiques de l'établissement, ces derniers seront accompagnés par une personne autorisée pour accéder à l'aire sécurisée. De plus, selon l'endroit physique auquel les visiteurs auront accès, on restreindra leur accès logique aux équipements (serveurs, logiciels, etc.) selon le type d'intervention qu'ils effectueront.

1.4 Logistique

Les enjeux associés à la logistique sont principalement reliés à l'organisation du travail, aux divers niveaux de **sécurité** qui régissent les déplacements des personnes et des équipements ainsi qu'au traitement des données. Lors de la programmation de l'unité, l'établissement doit élaborer des politiques et des procédures pour gérer ces enjeux. Il doit entre autres considérer les points qui suivent.



1. Flux des personnes

L'accès des membres du **personnel** à l'UTIC est généralement régi en fonction de leur appartenance ou non à l'unité. Concernant le personnel interne, les niveaux d'accessibilité sont fonction des responsabilités attribuées à chacun au sein de l'UTIC, les déplacements du personnel pour certains secteurs et locaux particuliers étant gérés par un système de contrôle des accès.

Quant aux **visiteurs**, ils ont un accès limité à l'UTIC. Ils devraient idéalement utiliser les aires de circulations publiques pour s'y rendre et être accompagnés d'un représentant de l'UTIC en tout temps.

Évidemment, l'usager (patient) n'a aucunement besoin d'accéder à cette unité fonctionnelle.

2. Flux des équipements, du matériel et des fournitures

Dans un centre hospitalier (CH), par exemple, la **livraison** se fait au quai de réception de l'établissement. De là, les équipements et autres fournitures sont, soit expédiés temporairement à l'entrepôt central et acheminés à l'UTIC en temps opportun, soit acheminés directement aux espaces d'entreposage de l'UTIC, pour être traités par la suite dans les ateliers d'assemblage et de configuration.

Les équipements sont directement transportés vers leurs utilisateurs si ceux-ci font partie du personnel interne de l'établissement. Par contre, ils passent par le quai de livraison, si nécessaire, lorsqu'ils sont destinés à des utilisateurs externes. Un établissement comportant plusieurs bâtiments aura aussi son quai de livraison, même si toutes les personnes concernées sont des utilisateurs internes. Le technicien pourra par ailleurs emporter lui-même l'équipement à son point d'utilisation pour en effectuer l'installation et la configuration.

Quant au matériel et aux équipements actifs nécessitant **réparation** ou **entretien**, ils sont généralement acheminés directement aux ateliers de l'UTIC.

3. Flux de l'information et des communications

L'ensemble de ces flux relève de l'UTIC. Quant aux aspects immobiliers qui y sont liés, ils touchent notamment :

- la répartition des salles des TIC satellites, qui est fonction des normes en vigueur quant à la distribution de celles-ci dans un bâtiment;
- l'emplacement des conduits de filage informatique dans les infrastructures, établi en fonction des risques reliés, entre autres, à la sécurité et à la prévention des infections (voir la section suivante).

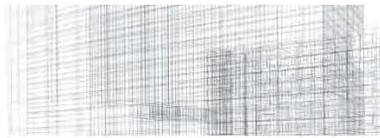
1.5 Risques

Les principaux objectifs en matière de prévention des risques potentiels reposent sur un principe essentiel, à savoir que la sécurité des installations doit être adéquate, afin que l'on puisse fournir à la population des services de santé en toute sécurité et assurer la poursuite des activités en matière de soins (réf. : Plan des mesures d'urgence de l'établissement).

Les principaux facteurs de risque à considérer sont reliés à l'**emplacement des locaux** qui hébergent les actifs informatiques, au **maintien des activités** ainsi qu'à l'**adaptabilité** et à la **flexibilité des infrastructures**, compte tenu de l'évolution rapide des TIC.

1.5.1 Emplacement des locaux

La salle des serveurs et les salles des TIC satellites constituent un des secteurs les plus vulnérables. Afin de protéger les actifs informatiques, ces salles doivent être à l'abri des **aléas d'origine naturelle** engendrés par l'environnement tels : les inondations, les tremblements de



terre, le verglas, etc.), et des **aléas d'origine anthropique**, qui regroupent les sinistres technologiques (ex. : explosion d'une fournaise) et les sinistres reliés à l'activité humaine (ex. : émeute, incendie criminel, explosion d'une bombe ou autre explosion, etc.).

L'endroit où l'on décide d'installer l'UTIC à l'intérieur du bâtiment doit faire l'objet de certaines précautions. Il faut notamment :

- éviter le rez-de-chaussée (risque d'effraction);
- éviter le sous-sol (risque d'inondation);
- éviter les espaces sous les toitures ainsi que les espaces situés sous les locaux où il y a une grande utilisation d'eau et, par conséquent, risque de fuites (ex. : salle de toilette, salle de retraitement des dispositifs médicaux (RDM), etc.);
- éviter les endroits où passent directement des conduites d'eau ou de gicleurs (au-dessus de la salle ou au plafond);
- l'installer à l'écart des espaces où il y a une circulation publique importante;
- l'installer à l'écart des salles électriques, des salles mécaniques si celles-ci n'ont pas un lien direct avec la fonctionnalité de la salle des serveurs, et des ascenseurs;
- éviter le bruit électrique, les interférences, etc. ;
- l'installer dans un bâtiment dont la structure répond aux exigences du Code de construction du Québec (CCQ) en matière de protection civile (ex. : risque de séisme).

1.5.2 Maintien des activités

La salle des serveurs et les salles des TIC satellites d'étage doivent rester opérationnelles en tout temps pour assurer la continuité des services dans les installations. Pour ce faire, on doit :

- planifier des plans de contingence et de relève pour assurer la continuité des soins et des services;
- éviter d'installer ces salles à proximité de locaux pouvant contenir des matières inflammables;
- planifier adéquatement l'emplacement de la salle des serveurs;
- ajouter des mesures permettant de réduire les risques.

1.5.3 Adaptabilité et flexibilité des infrastructures

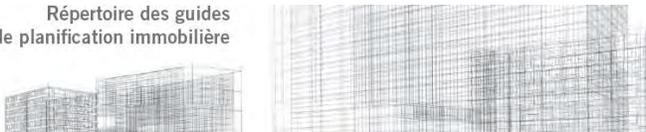
La salle des serveurs et les salles des TIC satellites doivent être conçues de façon à pouvoir évoluer dans les années à venir. Pour permettre cette évolution, on doit :

- éviter des localisations ne permettant pas d'expansion éventuelle de la salle des serveurs;
- s'assurer que les locaux contigus soient des locaux dont la fonction est moins essentielle et qu'ils puissent être déplacés pour permettre une expansion éventuelle;
- éviter les salles qui ne répondent pas aux normes les plus récentes en matière de sécurité incendie, de sécurité physique, de risque de surchauffe de la salle des serveurs, etc.

1.6 Tendances

Évolution technologique

Le développement des technologies est en plein essor et ses applications dans le domaine de la santé sont de plus en plus nombreuses et diversifiées. Les technologies d'imagerie médicale, l'implantation accrue de nouveaux systèmes d'information générant un grand nombre de données, la mise en place d'entrepôts de données et de systèmes de gestion de la reconnaissance ainsi que l'accroissement des activités de téléaccès (télétravail) font en sorte que les besoins en ce qui a trait à l'échange et au partage de l'information sont sans cesse croissants. Il faut également considérer les enjeux, en matière de sécurité, liés à l'arrivée des assistants numériques personnels : tablettes portables (ex. : Android), téléphones mobiles (ex. : iPhone), ordinateurs portables, etc. De plus, le



partage d'information (dossier patient électronique avec transfert de données) par le DSQ, la RAMQ, etc., permet d'avoir accès facilement à un dossier et de le modifier pour le tenir à jour et en faire le suivi. Encore ici, toutefois, des enjeux en matière de sécurité sont à considérer, étant donné l'augmentation du nombre d'utilisateurs d'appareils mobiles et de technologies sans fil et le partage d'information associés à toutes ces nouvelles tendances (VPN⁴, LAN⁵, MAN⁶, WAN⁷, etc.).

On constate également que tout ce qui a trait au BYOD « *Bring your own device* » : (« Apportez vos appareils personnels ») aura un impact sur la sécurité de l'information, le partage de données ainsi que la protection adéquate de celles-ci. En fait, tous les services techniques à distance et sur la route auront à être sécurisés (ex. : ANP – assistant numérique personnel).

On devra donc tenir compte, sur le plan de la sécurité, de l'évolution technologique et des nouvelles réglementations associées.

On observe enfin que l'organisation des soins de santé sans papiers ou sans films, l'accès des patients à l'information qui les concerne, ainsi que la recherche et l'enseignement, devront de plus en plus être pris en considération dans l'aménagement des établissements, lesquels devront alors disposer de l'infrastructure, des locaux et des éléments opérationnels appropriés (ex. : travail à plusieurs écrans). De plus, l'UTIC devra prévoir une capacité de stockage de l'information appropriée et s'assurer de pouvoir répondre aux requêtes qui lui seront faites (ex.: éviter les délais pour accéder aux données et s'assurer que le système puisse afficher les données rapidement).

Sécurité

En matière de sécurité, de nouvelles pratiques de gestion sont en cours de développement, qu'il s'agisse de la création de répertoires d'entreprise ou de l'application de mécanismes de sécurisation s'appliquant jusqu'aux données. Ces pratiques prévoient également le cryptage des données et la transmission d'information, le recours à des mécanismes d'identification forts ne pouvant être falsifiés, tels que la carte à microprocesseur ou le jeton électronique, et la création d'infrastructures à clés publiques.

Quant à la gestion des infrastructures technologiques, de plus en plus de modèles et de protocoles normalisés visant à assurer la continuité des services et à éviter les coupures de courant sont en cours de développement.

Flexibilité et adaptabilité

L'environnement physique doit permettre une certaine flexibilité et être adaptable pour faire face aux changements futurs des actifs informationnels. Pour assurer cette flexibilité et cette adaptabilité, il est nécessaire de préciser quels sont les changements anticipés et quels seront leurs impacts (ex. : augmentation des surfaces).

Sur le plan de l'environnement physique, on doit en outre considérer l'aménagement des bureaux pour le travail à plusieurs écrans et l'ajout de serveurs dans les salles réservées à cet effet (salles des TIC satellites), cela afin de répondre aux besoins grandissants d'informatisation de données.

-
4. VPN : Virtual Private Network ou RPV : réseau privé virtuel. Ce réseau permet de créer un lien direct entre des ordinateurs distants.
 5. LAN (Local Area Network) : ensemble d'ordinateurs reliés entre eux par un réseau (ex. : Ethernet) d'un même établissement.
 6. MAN (Metropolitan Area Network) : ensemble de LAN géographiquement proches (environ quelques dizaines de kilomètres) et interconnectés.
 7. WAN (Wide Area Network) : ensemble de LAN interconnectés couvrant de grandes distances (ex. : Internet).



1.7 Encadrement légal

Certification

La certification des applications du réseau est obligatoire et doit être faite en fonction du type de parc informatique retenu. Au minimum, il est nécessaire d'obtenir une certification en ce qui concerne le partage de l'information (application certifiée dans un tel environnement).

Note :

Aucun mécanisme officiel de certification n'est prévu et aucune certification de l'*Uptime Institute* n'est requise pour les salles de serveurs.

- Les applications sont uniquement certifiées en vertu du processus d'homologation du Ministère, selon certaines consignes administratives (réf. : Circulaire 2013-026 : 04-02-18-02).
- L'encadrement légal fait référence au respect des règles particulières applicables à l'utilisation de ces applications dans les UTIC.
- Les exigences portent sur les points suivants : la sécurité et la protection des renseignements personnels, l'interopérabilité, l'intégration des données, les performances, la technologie, etc.



2. Éléments de programmation

2.1 Critères de conception

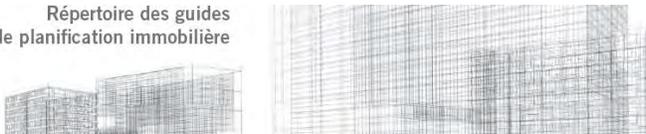
Les critères de conception qui suivent sont applicables dans une perspective d'ensemble. Cependant, la section consacrée aux locaux spécifiques de l'UTIC (section 2.2.3) complète ces informations en présentant des critères d'aménagement propres à chaque local. Les critères sont classés en fonction des catégories suivantes : fonctionnalité, confort et ambiance et sécurité.

2.1.1 Fonctionnalité

1. Privilégier le regroupement des secteurs d'activités afin d'éviter la multiplication des sites et de permettre le partage des ressources.
2. Tenir compte de l'impact d'une utilisation de plus en plus grande des outils informatiques dans le domaine de la santé sur les superficies, de façon à obtenir une marge de manœuvre pour accueillir les projets à venir :
 - Installer la salle des serveurs de façon à ce qu'elle soit contiguë à des espaces dits « *soft* », pour faciliter l'expansion éventuelle de celle-ci.
3. Concevoir des espaces polyvalents, flexibles et adaptables, en adoptant, entre autres, des dimensions uniformes ou des multiples et en combinant certaines activités.
4. Considérer, dans la planification, que la zone sécurisée, une fois aménagée, sera très difficile à déplacer, étant donné les enjeux techniques et l'infrastructure coûteuse associée à celui-ci.
5. Tenir compte, lorsque l'emplacement des câbles nécessaires au bon fonctionnement de l'UTIC sera déterminé, des risques liés à la prévention des infections en ce qui a trait aux systèmes des TIC.
6. Aménager les locaux selon leur fonction propre et faire en sorte qu'il n'y ait aucun partage d'espace dans le secteur sécurisé. À titre d'exemple :
 - réserver la salle des serveurs exclusivement à l'hébergement de l'équipement informatique.
7. Calculer la distance maximale entre deux salles de télécommunication satellites en respectant la norme voulant que la longueur d'un câble soit d'au plus 90 mètres depuis une sortie murale jusqu'à une salle de télécommunication

2.1.2 Confort et ambiance

1. Signaler efficacement les lieux qui doivent l'être.
2. Aménager et concevoir les espaces de façon à réduire le bruit et à favoriser la concentration.
3. Optimiser l'apport d'éclairage naturel dans les aires de travail.



2.1.3 Sécurité

1. Considérer les risques potentiels, incluant les catastrophes naturelles, les bris accidentels, les conditions environnementales, de même que l'accessibilité restreinte de certains espaces, lors du choix de l'emplacement de l'UTIC dans un établissement (salle des serveurs décentralisée ou CTI de données principal centralisé) :
 - éviter d'aménager la salle des serveurs le long d'un mur extérieur ou à un endroit facilement accessible à partir du niveau du sol;
installer toutes les salles de serveurs dans des endroits à l'abri des risques d'inondation, de fuite d'eau et d'effraction, ainsi qu'à l'écart des ascenseurs, de toutes les salles électromécaniques et des espaces où il y a une importante circulation de personnes.
2. Sécuriser les accès et les limiter aux personnes autorisées (circulation restreinte), selon les politiques de l'établissement.
3. Assurer le fonctionnement de l'UTIC 24 heures sur 24, 7 jours sur 7, selon la criticité de la mission de l'établissement.
4. Protéger le secteur sécurisé de toutes les intrusions (ex. : cloisons périphériques renforcées, systèmes d'alarme, etc.).
5. Considérer que les salles des TIC ne devraient pas comporter de fenêtres, celles-ci favorisant les effractions.
6. Assurer la redondance des systèmes (électrique, mécanique et de sécurité) dans les limites de la classification Tier II.
7. Prévoir des procédures ou des mécanismes de protection contre l'utilisation non autorisée et le vol des équipements.

2.1.4 Opération et entretien

1. Évaluer la largeur des circulations (incluant les portes) situées le long du parcours des pièces et des équipements volumineux qui seront remplacés.

2.2 Organisation spatiale

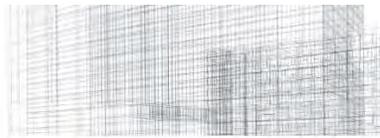
L'UTIC contient un **secteur sécurisé**, dans lequel sont hébergés les équipements d'emmagasinage, de télécommunication, les serveurs et autres équipements centraux. Ce secteur constitue donc le centre névralgique de l'unité. À ce dernier, s'ajoutent les secteurs abritant les activités de soutien essentielles au bon fonctionnement des équipements informatiques précités, les activités reliées aux services aux usagers, ainsi que celles communes à toute unité fonctionnelle, telles que l'administration, le soutien général, le service à la clientèle ainsi que le soutien du personnel. L'enjeu principal à considérer dans l'organisation spatiale d'une telle unité se situe sur le plan de la sécurité des actifs informationnels, soit des mesures à prendre pour se conformer au niveau de sécurité requis (réf. : Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux : Volet sur la sécurité).

D'autre part, l'entrée et l'installation de systèmes des technologies de l'information et des communications dans le bâtiment nécessitent l'aménagement d'un **local d'entrée des services de téléphonie/informatique**, une **salle des serveurs** et des **salles de télécommunication (salles des TIC satellites)**; signalons que ces dernières hébergent physiquement les zones d'interconnexion. Les salles des TIC satellites sont distribuées, selon des règles précises dans le bâtiment afin de rencontrer plusieurs critères, dont celui d'assurer la diversité des parcours. Elles peuvent contenir quelques serveurs en redondance et des zones d'interconnexion.

2.2.1 Description des secteurs d'activité de l'Unité des technologies de l'information

Les secteurs d'activité qui composent l'UTIC sont décrits brièvement dans le présent chapitre. Le schéma 1 précise quelles sont les activités qui sont effectuées dans chaque local composant ces secteurs d'activité.

- **Aire administrative** – Ce secteur peut inclure une aire d'accueil, des espaces et des locaux de travail ainsi que des salles de rencontre.



- **Zone sécurisée** – Zone fermée et contrôlée hébergeant la salle des serveurs ainsi que tous les espaces et locaux nécessaires à son fonctionnement. Elle regroupe donc les espaces et locaux techniques tels que la salle d'entrée des services de téléphonie/informatique, les salles d'électromécanique de la salle des serveurs ainsi qu'une salle de contrôle. Les salles des TIC satellites seront aussi considérées comme des zones sécurisées, mais celles-ci seront réparties sur les étages du bâtiment.
- **Soutien technique et services à la clientèle** – Secteur regroupant les espaces et locaux permettant d'assurer les activités reliées au bon fonctionnement du secteur sécurisé. Regroupe également les locaux où se déroulent les activités permettant d'assurer les services à la population, la centrale téléphonique, l'atelier de préparation ou de réparation des équipements, les bureaux, etc.
- **Soutien général** – Espace réservé à l'entreposage et aux activités d'hygiène et de salubrité (ex. : entreposage des déchets et des matières recyclables). Il est généralement situé à proximité des axes verticaux de circulation principale.
- **Soutien au personnel** – Secteur réservé aux activités de détente. Les espaces et locaux de ce secteur peuvent être situés à l'intérieur de l'unité ou à l'extérieur de celle-ci lorsqu'ils sont partagés par le personnel de plus d'une unité fonctionnelle.

Lorsque l'UTIC est située dans un bâtiment autonome étant considéré comme un bâtiment capable de subvenir à tous les besoins de cette unité en ce qui a trait à sa capacité d'accueil et à la continuité des services, l'organisation spatiale du lieu devra être planifiée en fonction des besoins reliés, notamment, à la livraison et à l'entreposage du matériel et des fournitures. Une évaluation des besoins relative aux espaces et aux équipements servant à l'expédition, à la livraison et à l'entreposage du matériel, des fournitures, etc. (incluant les déchets de toutes catégories) est alors nécessaire.

2.2.2 Liaisons fonctionnelles

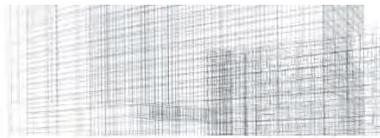
Les liaisons fonctionnelles déterminent la proximité physique requise entre deux secteurs d'activités ou entre deux unités. Le type de proximité souhaité est fonction du niveau de sécurité recherché (situation critique, urgence), de la fréquence des déplacements et du temps que nécessitent ces déplacements (efficacité).

Les liaisons fonctionnelles sont de deux ordres :

1. externes : entre l'UTIC et les autres unités fonctionnelles situées dans le bâtiment;
2. internes : entre les secteurs d'activité d'une unité fonctionnelle donnée soit, dans le cas présent, l'UTIC.

Liens externes

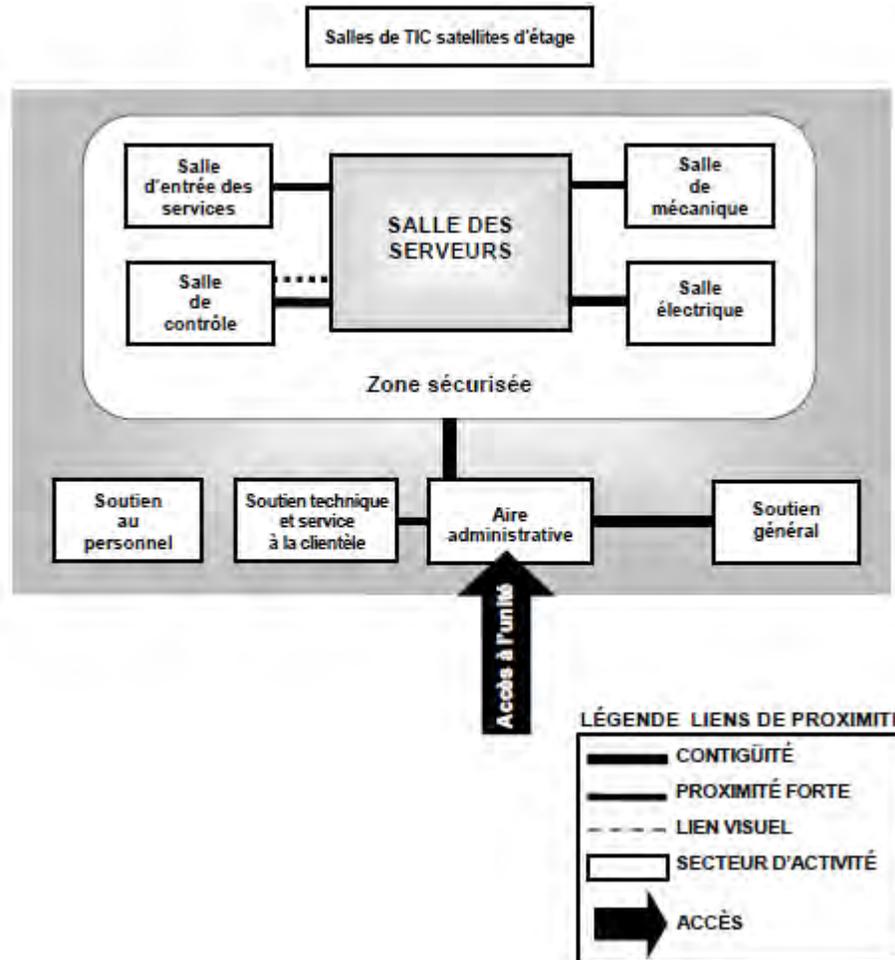
Les activités réalisées dans l'UTIC s'effectuent indépendamment de toutes les autres activités qui se déroulent dans l'établissement à l'intérieur duquel l'UTIC est située, et cela peu importe la mission de l'établissement. Conséquemment, d'un point de vue immobilier, il y a peu de liens fonctionnels à respecter quant à la proximité d'autres secteurs d'activité, l'UTIC étant somme toute relativement indépendante. L'UTIC peut donc être située à l'écart de toute autre unité fonctionnelle nécessaire à la réalisation de la mission de l'établissement, voire être isolée dans un bâtiment distinct du complexe hospitalier, par exemple, ou dans une salle des serveurs se situant en dehors du site hospitalier.



Liens internes

On note que les activités essentielles au bon fonctionnement du secteur sécurisé, ont généralement lieu dans des locaux contigus à ce dernier. Lorsque la salle des serveurs est située dans un établissement et non dans un CTI de données, les salles des TIC satellites de l'établissement doivent être aménagées à des distances précises l'une de l'autre (la longueur d'un câble doit être d'au plus 90 mètres depuis une sortie murale jusqu'à une salle de télécommunication satellite) pour ne pas nuire à la qualité du réseau des TIC. Les salles des TIC satellites doivent aussi être sécurisées.

2.2.3 Schéma organisationnel



Note : voici la hiérarchie utilisée dans les schémas et diagrammes du présent document en ce qui concerne les liens de proximité.

Contigüité : contact direct essentiel entre deux secteurs d'activité.

Proximité forte : les systèmes transporteurs (ex. : ascenseurs, monte-charges et tubes pneumatiques) peuvent diminuer le besoin de proximité physique requis. Dans certains cas, ce sont les systèmes informatiques et de communication qui éliminent la distance.



2.2.4 Sous-composantes, locaux et espaces

Le tableau suivant indique les superficies minimales nettes ou les ratios suggérés pour la programmation des locaux et espaces potentiels (proposés ou possibles). Des informations générales y sont présentées. Concernant certains locaux particuliers vis-à-vis desquels on trouvera l'icône « ► » dans la colonne « Lien », des informations complémentaires sont présentées dans la section qui suit (section 2.3).. La lettre « É », enfin, indique que la superficie minimale nette (ou le ratio) est fonction des besoins ou du mode de fonctionnement de l'établissement.

Tableau 1 – Espaces, locaux, superficies nettes minimales (m²) ou ratios (m²/élément) recommandés

Espaces, locaux, superficies nettes minimales ou ratios		Sup. nette min. (m ²) ou ratio	Lien
1. Aire administrative			
a) Accueil	Poste ou comptoir, servant à l'accueil des usagers. Peut être partagé avec d'autres unités.	5,5 m ² /pers.	
b) Vestiaire des visiteurs	Vestiaire intégré ou mobilier amovible, visible de l'accueil.	100 mm lin./pers.	
c) Salle d'attente	Salle accessible et visible à partir de l'accueil.	2,0 m ² /pers.	
d) Bureau	Espace fermé.	7,5 à 11,0	
e) Aire ouverte	Espace à aire ouverte comportant un poste de travail.	4,5	
f) Salle de réunion	Salle qui peut être adaptée ou non à différents usages. Évaluer la pertinence d'y installer une cloison amovible afin de diviser la salle en deux sections. Cette salle peut être avoir différentes fonctions. Par exemple, on peut s'en servir pour évaluer les produits, les logiciels et le matériel des fournisseurs; dans ce cas, il faut prévoir des prises de courant et des connexions adéquates.	2,0 m ² /pers.	
g) Salle de toilette	Espace comprenant des toilettes et des lavabos. Évaluer la possibilité de partager cet espace avec d'autres unités. Privilégier un des trois types d'aménagements suivants : <ul style="list-style-type: none"> - salle de toilette du personnel : sans accès universel : - salle de toilette universelle sans aidant : - salle de toilette multiple avec deux équipements (wc ou urinoir/wc) et lavabo. 	2,5 3,5 8,0	
2. Zone sécurisée			
a) Salle d'entrée des services	Local hautement sécurisé d'arrivée des services de téléphonie/informatique situé à proximité de la salle des serveurs. Protégé par un contrôle des accès.	É	
b) Salle des serveurs	Local hautement sécurisé, refroidi par un climatiseur à haute performance alimenté en électricité d'urgence et assurant la continuité des services à l'aide d'une ASSC. Généralement situé de façon à réduire les risques liés aux catastrophes naturelles et accidentelles. Protégé par un contrôle des accès.	É	►
c) Salle de contrôle	Local qui doit être adjacent à la salle des serveurs afin d'assurer un lien visuel direct avec celle-ci, (ex. : fenêtrer la salle de contrôle de façon à assurer une supervision de la salle des serveurs). Il faut prévoir un poste informatique et un téléphone dans ce local.	5,5 m ² /pers.	
d) Salle mécanique	Local distinct pour les équipements mécaniques réservés au fonctionnement de la salle des serveurs.	É	
e) Salle électrique	Local distinct pour les équipements électriques réservés au fonctionnement de la salle des serveurs (ex. : ASSC).	É	
f) Salles des TIC satellites	Locaux sécurisés et verrouillés, refroidis par un climatiseur à haute performance alimenté en électricité d'urgence et assurant la continuité des services à l'aide d'une ASSC. Comportent généralement plusieurs salles protégées par un contrôle des accès et réparties de façon à assurer une diversité des parcours afin de mieux gérer les possibles catastrophes.	É	

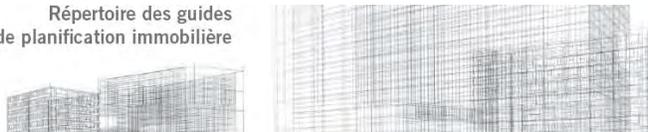


Espaces, locaux, superficies nettes minimales ou ratios		Sup. nette min. (m ²) ou ratio	Lien
3. Soutien technique et services aux usagers			
a) Bureau	Voir « Aire administrative ».	É	
b) Aire ouverte	Aire réservée aux activités reliées à l'assistance téléphonique.	É	
c) Ateliers	Locaux réservés à la préparation et à la réparation des équipements informatiques. Ces locaux devront être équipés d'établis dotés de prises éliminatrices de surtension et de tapis contrôlant l'électricité statique. Des prises réservées aux services techniques seront prévues pour assurer le plus de flexibilité possible.	É	
4. Soutien du personnel			
a) Salle de repos	Pièce aménagée pour la détente et les pauses. Peut être partagée avec une autre unité. Un éclairage naturel est souhaitable. Évaluer la pertinence d'ajouter : <ul style="list-style-type: none"> - une cuisinette ou un coin café : prévoir l'espace suffisant pour un four à micro-ondes, un réfrigérateur et une machine à café; - des espaces pour des machines distributrices; - des salles de toilette à proximité. 	2,0 m ² /pers. 2,5 2,0 m ² /machine	
b) Espace vestiaire du personnel	Le vestiaire du personnel peut être centralisé ou décentralisé selon le fonctionnement de l'établissement. Le CH peut aussi réserver à chaque employé un petit casier pour ses objets personnels : <ul style="list-style-type: none"> - casier mi-hauteur; - casier pleine hauteur. 	2,0 m ² /pers. 0,2 m ² /casier 0,4 m ² /casier	
5. Soutien général			
a) Local d'hygiène et de salubrité	Local satellite pour l'entretien ménager. Peut être partagé.	4,0	
b) Local d'entreposage des déchets et du matériel recyclable	Espace réservé à l'entreposage des déchets ordinaires et du matériel recyclable lorsque l'établissement participe à un programme de recyclage. Peut être partagé.	6,0	
c) Dépôt	Local généralement sécurisé pour l'entreposage de l'équipement.	É	
d) Réserve	Local servant à entreposer du matériel et des équipements. Peut être centralisée dans le bâtiment.	É	

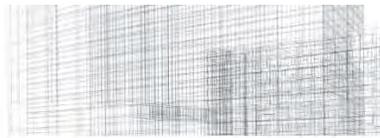
2.3 Locaux spécifiques

Seuls les locaux spécifiques de l'UTIC sont inclus dans la présente section, où ils sont présentés par ordre alphabétique. Les objectifs de performance technique documentés au chapitre 3 du présent document s'appliquent pour toute l'unité et doivent être consultés en parallèle avec les critères d'aménagement des locaux spécifiques.

Attention : les critères qui suivent sont présentés à titre indicatif seulement et doivent être validés dans le cadre de chaque programme en fonction du mobilier choisi, des équipements utilisés et des pratiques mises en place par chaque établissement.



SALLE DES SERVEURS	
Superficie à évaluer par l'établissement	
Critères d'aménagement	
<p>FONCTIONNALITÉ</p> <ol style="list-style-type: none"> Dimensionner la salle des serveurs en fonction des besoins en équipement et considérer les espaces nécessaires pour la réparation et l'entretien de ceux-ci. Aménager la salle de façon sécuritaire, en fonction des risques définis à la section 1.5 Risques. Prévoir un espace suffisant pour l'installation ou le remplacement d'équipements volumineux. À titre d'exemple : <ul style="list-style-type: none"> prévoir une largeur libre adaptée à l'équipement pour toutes les portes situées sur le circuit, opter pour des panneaux amovibles dans la cloison afin de pouvoir agrandir les ouvertures. Situer la salle des serveurs et les salles TIC satellites d'étage à distance de toutes sources dont les vibrations pourraient affecter celles-ci (ex. les cages des ascenseurs, les salles électriques et mécaniques). Plancher surélevé (si requis) : <ul style="list-style-type: none"> évaluer la pertinence de surélever le plancher de la salle notamment pour les besoins électromécaniques et pour limiter des bris en cas de dégât d'eau. porter une attention particulière à l'installation du système de plancher surélevé (finition des coupes et insertion dans la structure) de façon à éviter toute évacuation d'air provenant du vide technique. ayant les propriétés suivantes : <ul style="list-style-type: none"> antistatique capable de supporter les équipements prévus Prévoir une mise à la terre. Prévoir une couleur claire pour les finis intérieurs, de façon à maximiser les effets de l'éclairage. Considérer que le dessus des cabinets doit être libre de tout obstacle (ex. : tête de gicleurs) sauf si les câblages informatiques passent au-dessus des cabinets. 	<p>FONCTIONNALITE (SUITE)</p> <ol style="list-style-type: none"> Faciliter la gestion du câblage en uniformisant les accessoires tels que les râteliers (chemin de câble) afin de faciliter la distribution électrique et celle de la climatisation. <p>SECURITE</p> <ol style="list-style-type: none"> Prévenir le vol d'équipements, de données et le sabotage, en sécurisant les accès, l'enveloppe du local, (murs, plafonds, plancher et leurs composantes) ainsi que les cabinets, à titre d'exemple : <ul style="list-style-type: none"> prévoir un système de surveillance par vidéo, ainsi qu'un système de contrôle des accès et de surveillance visuelle directe à partir d'un local adjacent (ex. : salle de contrôle). sécuriser les fenêtres, par exemple, prévoir un verre laminé d'une pellicule sécuritaire ou une unité en verre broché. prévoir une construction dalle à dalle pour les cloisons de la salle. Prévenir les intrusions : par exemple, <ul style="list-style-type: none"> faire ouvrir les portes d'accès vers l'extérieur. éliminer toute fenestration sur un mur extérieur. Prévoir un revêtement de plancher ou une finition de plancher ayant les caractéristiques suivantes : <ul style="list-style-type: none"> qui ne libère ni n'accumule de la poussière (ex. béton traité avec de l'époxy). ayant des propriétés antistatiques. Prévoir une protection-incendie minimale de deux heures, aux points d'entrée des conduits dans la salle, et ce, même si les exigences du CCQ sont inférieures. Prévoir la même exigence pour les séparations coupe-feu (planchers, cloisons) et les ouvertures. Considérer que seule la documentation relative à l'entretien des actifs informationnels doit être entreposée dans la salle. Aucun autre type d'entreposage de matériaux combustibles ou dangereux n'y est autorisé.
Dimensions	
<ol style="list-style-type: none"> Dimension minimale de salle selon le nombre de cabinet: <ul style="list-style-type: none"> 1 à 10 cabinets : 3m x 10m 11 à 20 cabinets : 5,5m x 10m 21 à 30 cabinets : 5,5 x 13m 31 à 40 cabinets : 5,5m x 17m 41 à 50 cabinets : 10mx 11m 51 à 60 cabinets : 10m x 13m Superficie de la salle TIC satellite de l'étage : <ul style="list-style-type: none"> minimale : 2,5 m² maximale : 5,0 m² 	<ol style="list-style-type: none"> Hauteur minimale des plafonds : 2 600 mm Se coordonner avec les services électromécaniques et tenir compte des exigences des fabricants d'équipement et du type de cabinet prévu (ex. haute densité). Dimension minimale des portes : 1 000 mm X 2 100 mm Plancher surélevé (si requis) : ayant les caractéristiques suivantes : <ul style="list-style-type: none"> Dimension des tuiles : 600 mm x 600 mm Pente minimale recommandée : 2 %
Dégagements	
<ol style="list-style-type: none"> Positionnement minimum des cabinets : <ul style="list-style-type: none"> devant : 1 000 -1 200 mm arrière : 600 - 900 mm sur le dessus des cabinets : 460 mm 	



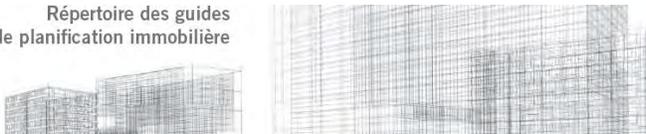
2.4 Calcul des superficies

La **superficie brute de l'unité** est déterminée selon le facteur de conversion **F1**. Les superficies et facteurs sont définis dans le document intitulé Méthode de calcul des superficies, disponible à l'adresse suivante :

<http://msssa4.msss.gouv.qc.ca/fr/document/publication.nsf/4b1768b3f849519c852568fd0061480d/e4cf054c8edaabe485257b41006a8ca0?OpenDocument>

Facteur de conversion F1	1,40
---------------------------------	-------------

Note : circulations internes, densité des murs et des cloisons, similaires à une unité d'administration.



3 Objectifs de performance technique

La présente section traite des objectifs relatifs à la performance technique requise pour l'aménagement de l'UTIC. Les performances techniques pour les composantes et les systèmes de base du bâtiment (*base building*), de même que pour l'aménagement de l'emplacement, seront présentées dans un guide complémentaire.

1. Définition

Bâtiment de base : les systèmes et composantes inclus dans le « bâtiment de base » sont les suivants : infrastructure, structure et enveloppe du bâtiment.

2. Structure de l'information : les objectifs de performance technique sont ordonnancés conformément à la nomenclature de la classification **Uniformat II**.

3. Codes, normes et règlements :

- les spécifications contenues dans les normes, codes et règlements en vigueur ne seront pas répétées dans la présente section lorsqu'elles conviennent aux activités de l'unité;

- lorsque ces spécifications ne sont pas adaptées aux activités de l'unité, les objectifs de performance à considérer seront précisés, toujours dans le respect des spécifications minimales qui font l'objet d'une loi ou d'un règlement dont l'application est obligatoire (ex. : norme CSA 317-2, majorité des articles du CCQ);

- concernant les **articles des normes, codes et règlements dont l'application n'est pas obligatoire** (ex. : article 6.2.1.1 – Règles de l'art du CCQ), nous mentionnerons dans le chapitre quels sont les documents auxquels se référer et préciserons quels sont les objectifs de performance à respecter.

4. Critères : dans chaque section Uniformat, les objectifs de performance sont regroupés selon certains critères : fonctionnalité (efficacité, organisation, interrelation, ergonomie), confort (bien-être, ambiance, autonomie), sécurité (santé, sûreté), exploitation et entretien ainsi que pérennité.

3.1 Généralités

Les recommandations présentées sous cette rubrique s'adressent à l'ensemble des disciplines. De plus, elles sont applicables à toutes les sous-sections de la classification Uniformat II qui suivent. Le dimensionnement, les besoins et les contraintes en ce qui a trait aux nouvelles salles (salle des serveurs, salle de contrôle, salle électrique, salle mécanique, etc.) doivent être abordés en tenant compte des éléments suivants : surface de la salle, puissance désirée, niveau de service et continuité, évolution envisagée et flexibilité, modalités d'exploitation future, etc.

Normes

Noter que les objectifs de performance qui suivent s'appuient sur la notion de « Tier », définie par l'*Uptime Institute* et largement adoptée dans le monde. La norme ANSI/TIA-942 *Telecommunications Infrastructure Standard for Data Centers*, en vigueur au moment de la rédaction du présent guide, peut servir de complément d'information. Il est recommandé de consulter la version la plus récente de la norme précitée au moment de définir les exigences techniques liées au programme fonctionnel et technique.

1. Sécurité

- Concevoir les installations de façon à respecter le niveau de service *Tier II*, tel que défini dans le document de l'*Uptime Institute* intitulé – *Data Center Site Infrastructure Tier Standard : Topology*.



Note :

Principaux critères de performance Tier II, tels que définis par l'*Uptime Institute*, dans le document intitulé – *Data Center Site Infrastructure Tier Standard: Topology*, 2010.

- Redondance des composantes actives de soutien (groupe électrogène, ASSC, refroidisseurs, équipements de rejet de chaleur, pompes, unités de refroidissement, réservoirs de carburant).
- Non redondance des composantes des réseaux de distribution (conduits, tuyauterie, alimentation électrique).
- Maintien du service lors de l'entretien des systèmes de soutien : non.
- Tolérance aux pannes : non.
- Compartimentation : non.
- Refroidissement continu : non.

2. Exploitation et entretien

Faciliter l'accès aux équipements et aux systèmes (mécaniques, électriques et médicaux) de manière à ce que les travaux éventuels de construction, de réparation et d'entretien courant et préventif puissent être exécutés en occasionnant le moins de bruit et de poussière possible, et ce, sans interrompre les activités courantes.

3. Pérennité

Sélectionner des matériaux et des produits durables, reconnus et testés pour leur facilité d'entretien et qui résistent aux impacts pouvant se produire dans les endroits où circulent des chariots.

3.2 Unifomat II

C Aménagement intérieur

C10 Construction intérieure

1. **Sécurité** - Sécuriser les locaux de la « zone sécurisée » par une conception de type anti-intrusion.

Exemple :

- Construire des cloisons dalle à dalle renforcées.

2. **Confort** - Assurer l'intégrité de l'ensemble des systèmes plancher-mur-plafond, de façon à les rendre conformes aux normes ASTM E-336 et à réduire la transmission sonore vers les espaces adjacents au secteur sécurisé, en vue d'assurer le confort des usagers.

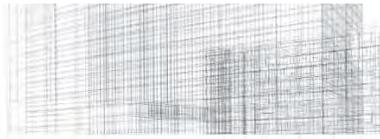
C1010 Cloisons intérieures

1. Confort

- Concevoir les systèmes de cloisons et les plafonds, là où ils sont nécessaires, en respectant l'indice de transmission sonore (ITS) requis.
- Respecter un ITS minimal dans la conception des locaux suivants :
 - aires d'attente et salles de repos du personnel : 45 ITS
 - salles de toilette, bureaux, salles de réunion et de visioconférence : 50 ITS
- Concernant les locaux où sont logés les équipements médicaux qui nécessitent un environnement sonore particulier, se référer aux exigences des fournisseurs des équipements.
- Prévoir un fenêtrage donnant sur les espaces de circulation interne, à défaut d'éclairage naturel, dans les secteurs où le personnel travaille pendant de longues périodes.

2. Pérennité

- Protéger les murs de façon à ce qu'ils résistent aux impacts de chariots lourdement chargés.
- Concevoir des cloisons qui supportent facilement les vibrations produites par l'équipement.



C1020 Portes intérieures

1. Sécurité

- Prévoir une fenestration dans les portes fréquemment utilisées par le personnel et là où une surveillance est requise.
- Tenir compte du fait que le battant des portes ouvrant sur un corridor ne doit pas réduire la largeur de ce dernier en deçà de la largeur requise pour la circulation et pour l'évacuation de l'unité.

2. Exploitation et entretien

- Protéger les portes, les cadres et la quincaillerie contre les chocs occasionnés par les chariots et les autres équipements roulants.
- Réduire au minimum le nombre de largeurs types des portes.
- Quincaillerie : prévoir des plaques de protection d'une hauteur d'au moins 1 100 mm de chaque côté et au bas de chacune des portes par où passent des chariots.

C1030 Accessoires intégrés

1. Exploitation et entretien

- Protéger les portes, les cadres et la quincaillerie contre les chocs occasionnés par les chariots et autres équipements fréquemment déplacés.

Exemples :

- Opter pour des plaques de protection en acier inoxydable sur le bas des portes, des deux côtés.
- Privilégier les protecteurs de portes surélevés afin de protéger les poignées.
- Installer des protecteurs de coins et des protecteurs muraux sur une hauteur d'au moins 1 800 mm dans les endroits où circulent des chariots.

- Opter pour des revêtements de sol uniformes, de manière à simplifier les activités liées au fonctionnement et à l'entretien (hygiène et salubrité).

C30 Finition intérieure

1. Sécurité

- Prévoir des matériaux de finition qui ne produisent pas de poussière pour les murs, les planchers et les plafonds.

Note :

Respecter la norme CAN/CSA-IEC 61000-4-2 pour les propriétés antistatiques du plancher.

C3020 Finition de planchers

1. Confort

- Prévoir des revêtements qui facilitent le maniement du matériel roulant (chariots).
- Prévoir des revêtements insonorisants dans les aires de travail administratif.
- Accorder la priorité aux revêtements souples qui facilitent le maniement des équipements roulants.

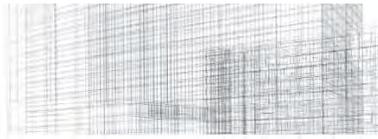
1. Pérennité

- Choisir des matériaux durables qui résistent à l'usure, aux poinçonnements et aux marques faites par les chariots et divers autres équipements.

Exemples :

Revêtements souples en rouleaux :

- **Vinyle hétérogène :**
 - conforme à la norme ASTM F-1303 type I, catégorie I, endos classe B;
 - couche d'usure minimale de 0,5 mm.



- **Vinyle à endos :**
 - conforme à la norme ASTM F-1303, type II, catégorie I, endos classe A;
 - couche d'usure minimale de 1,27 mm.
- **Caoutchouc :**
 - conforme à la norme ASTM F-1859;
 - épaisseur minimale de 2,0 mm;
 - masse de 3,05 kg/m².
- Carreaux de vinyle de composition (en anglais, vinyl composition tile ou VCT) :**
 - conformes à la norme ASTM F-1066, classe 2, motif dans la masse;
 - épaisseur minimale de 3,2 mm.
- Plinthes :**
 - en caoutchouc;
 - hauteur minimale de 150 mm.
- Carreaux de céramique et plinthe en carreaux coupés :**
 - conformes à la norme CAN/CGSB-75;
 - de type 4 RH-1 (minimum d'absorption d'eau extérieure ou RH-2);
 - facteur d'abrasion R-10.
- Adhésif :**
 - conforme aux normes ANSI A118.4 et ANSI A118.11;
 - composé de ciment-colle modifié au polymère.
- Coulis :**
 - conforme à la norme ANSI A118.3;
 - complètement imperméable;
 - résistant aux agents chimiques, aux nettoyages fréquents et aux chocs.

C3030 Finition de plafonds

1. Sécurité

- Renforcer le plafond afin de pouvoir y installer les équipements ou les accessoires requis.

D Services

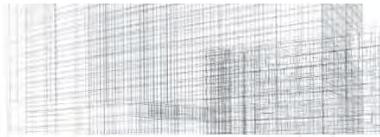
1. Fonctionnalité

- **Classification Tier** – Concevoir les installations électromécaniques de façon à respecter la classification *Tier II*, telle que définie dans le document – *Data Center Site Infrastructure Tier Standard : Topology*, publié par *l'Uptime Institute*. Noter que certaines exigences définies dans la présente section vont au-delà du minimum requis pour respecter la classification Tier II, cela afin d'assurer le respect des orientations ministérielles en fonction de la complexité des services offerts.
- **Capacité et évolution** – Concevoir les installations électromécaniques de façon à permettre, au besoin, leur expansion ou l'ajout de nouveaux équipements sans créer d'interférence induite avec l'exploitation de la salle des serveurs, et ce, pendant toute la période de vie utile de cette salle.
- **Installations non associées** - Éliminer tous les équipements, toute la tuyauterie et tous les conduits non associés aux équipements de la salle des serveurs, à l'intérieur de celle-ci. Cette mesure s'applique également aux espaces où se trouvent des équipements de soutien essentiels à la salle des serveurs.
- **Norme sismique et moyens de fixation des composants** Respecter les exigences de la norme CAN/CSA S832 : diminution des risques sismiques concernant les composants fonctionnels et opérationnels des bâtiments.

D20 Plomberie

1. Fonctionnalité

- **Prévention des dommages causés par l'eau** – Limiter les risques de dommages et d'interruption de service causés par l'eau. À cet effet :
 - bannir de la salle des serveurs tout point d'eau tel que lavabo, évier, fontaine, etc.;
 - éliminer toute tuyauterie d'alimentation en eau et toute tuyauterie de drainage non associées aux équipements de la salle des serveurs, à l'intérieur ou au-dessus de celle-ci;



- assurer une évacuation rapide d'une éventuelle accumulation d'eau dans la salle des serveurs;
- prévenir les débordements et refoulements d'eau de drainage dans la salle des serveurs;
- appliquer les mesures énumérées ci-dessus aux espaces où se trouvent des équipements de soutien essentiels à la salle des serveurs.

D30 Chauffage, ventilation et conditionnement d'air

1. Généralités

- **Normes et guides** – Consulter, entre autres, les documents de référence suivants :
 - les ouvrages de la collection « Datacom » publiés par l'ASHRAE, lesquels comportent des recommandations détaillées en matière de conception des installations de chauffage, de ventilation et de conditionnement d'air (CVCA) des salles de serveurs;
 - la norme CAN/CSA Z317.2, laquelle comporte des recommandations particulières relativement au maintien des fonctions essentielles d'un établissement de santé, dont les salles d'équipement informatique.

2. Exploitation et entretien

- Faciliter la maintenance des équipements à l'aide des mesures suivantes :
 - installer les équipements de conditionnement d'air dans des endroits où il sera facile d'en effectuer la maintenance et, éventuellement, le remplacement complet, en prévoyant le minimum d'interférence possible avec l'exploitation des installations informatiques;
 - assurer des dégagements suffisants pour permettre le plein accès aux composants des équipements de CVCA;
 - considérer d'avoir recours à un local séparé de la salle des serveurs pour les équipements de CVCA.

D3040 Distribution de chauffage, ventilation et conditionnement d'air

1. Fonctionnalité

- **Conditions ambiantes pour les équipements de la salle des serveurs** – Concevoir les installations de CVCA conformément aux recommandations de l'ASHRAE, notamment celles contenues dans le document intitulé *Thermal Guidelines for Data Processing Environments* (collection Datacom). Les conditions ambiantes à l'admission d'air des équipements doivent se situer à l'intérieur de la fourchette des valeurs recommandées (*recommended*). En aucun temps, même en situation de panne ou d'urgence, ces conditions ne doivent se situer hors de la fourchette des valeurs admissibles (*allowable*).

Note :

Résumé des recommandations de l'ASHRAE pour les salles de serveurs avec ambiance bien contrôlée (classe 1), tirées du document *Thermal Guidelines for Data Processing Environments*, 2^e édition, 2009.

Conditions en marche :

Température bulbe sec :

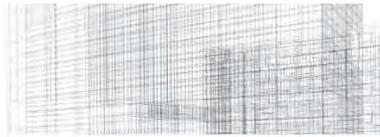
- recommandée : de 18 à 27 °C;
- admissible : de 15 à 32 °C;
- taux de variation maximum : 5 °C/h (bande magnétique); 20 °C/h (disque dur).

Humidité :

- recommandée : température de rosée de 5,5 à 15 °C, sans dépasser 60 % d'humidité relative;
- admissible : de 20 à 80 % d'humidité relative, sans dépasser une température de rosée de 17 °C.

Conditions à l'arrêt :

- température bulbe sec : de 5 à 45 °C;
- humidité : de 8 à 80 % d'humidité relative, sans dépasser une température de rosée de 27 °C.



- **Niveau de propreté de l'air**

- Assurer une qualité de filtration de l'air d'au moins MERV 8 et, préférablement, d'au moins MERV 11.
- Maintenir la salle des serveurs en pression légèrement positive afin de prévenir l'infiltration d'air et de contaminants à travers les cloisons et l'enveloppe du bâtiment.

Note :

Afin de maintenir une pression positive, les points de passage de câbles et tuyaux à travers l'enceinte de la salle devraient être scellés et la porte devrait être bien ajustée.

Il peut aussi être nécessaire de conférer à la salle un degré d'étanchéité suffisant pour assurer le maintien, pendant le temps requis, d'une concentration adéquate de l'agent gazeux « propre » pour l'extinction d'incendies, le cas échéant. Les recommandations du fabricant de l'agent gazeux « propre » concernant le taux de dilution (exfiltration, ventilation) doivent être suivies. Voir D40.

- **Organisation de type « allée froide » et « allée chaude »**

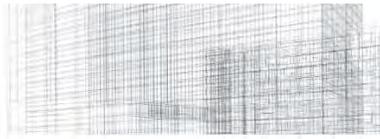
- Optimiser la distribution d'air refroidi aux entrées d'air des équipements informatiques et optimiser le captage de l'air chaud rejeté par ceux-ci en adoptant les concepts d'allée chaude et d'allée froide, lorsque les équipements informatiques sont conçus à cet effet (c'est-à-dire : flux d'air des équipements allant de l'avant vers l'arrière, de l'avant vers le dessus ou de l'avant vers le dessus et vers l'arrière).
- Assurer une bonne différenciation thermique des allées froides et chaudes afin de maximiser le rendement thermique et énergétique. À cet effet :
 - o répartir adéquatement la distribution d'air refroidi dans l'allée froide;
 - o capter l'air chaud aux endroits stratégiques le long de l'allée chaude;
 - o considérer les techniques de confinement de l'allée froide telles que : l'absence d'espace entre les cabinets, l'obturation des espaces inutilisés des cabinets, les rideaux thermiques flexibles, le un cloisonnement thermique rigide, etc.;
 - o éviter les situations où l'air chaud expulsé par les équipements informatiques revient se mélanger avec l'air refroidi, notamment en haut et aux extrémités des allées;
 - o éviter les situations où l'air refroidi est rejeté du côté chaud sans avoir servi au refroidissement des équipements.

- **Organisation de type autre qu'allée froide et allée chaude**

- Faire en sorte que l'air chaud évacué des équipements informatiques non conçus pour fonctionner selon le concept d'allée froide et d'allée chaude ne nuise pas au fonctionnement des équipements voisins. À cet effet :
 - o regrouper ces équipements et les séparer de ceux organisés selon le mode allée froide et allée chaude;
 - o évaluer la pertinence d'un quelconque traitement permettant de capter le flux d'air chaud près de la source ou de le rediriger.
- Évaluer la pertinence d'avoir recours à tout autre dispositif ou méthode permettant d'assurer le refroidissement des équipements informatiques comme, par exemple, le refroidissement par liquide.

Note :

Le présent guide n'exclut pas la possibilité d'utiliser des méthodes innovatrices autres que le refroidissement par air selon la configuration allée froide et allée chaude.



- **Éléments additionnels d'efficacité énergétique**
 - Optimiser la température d'alimentation de l'air de manière à limiter les coûts de refroidissement. Cette optimisation doit se faire sans créer de points de surchauffe localisés.
 - Récupérer la chaleur rejetée par le système de refroidissement lorsque celle-ci peut être économiquement réutilisée.
 - Considérer les différentes options de refroidissement gratuit.

Note :

Il existe plusieurs options de refroidissement gratuit, par exemple : l'apport direct d'air extérieur, l'échangeur de chaleur air-air, le refroidissement par l'eau de la tour de refroidissement, les serpentins au glycol en boucle, etc.

Les installations de refroidissement gratuites doivent offrir le même niveau de fiabilité et de maîtrise des conditions ambiantes que les systèmes de refroidissement mécanique.

- **Vibrations** – Prévenir la transmission des vibrations causées par les équipements de CVCA aux équipements informatiques.
- **Continuité de service** – Respecter les éléments suivants afin de répondre au critère de performance Tier II :
 - redondance N+1 des unités de refroidissement (unité de traitement d'air avec compresseur de refroidissement);
 - redondance N+1 des appareils employés pour le rejet de chaleur (tour de refroidissement, condenseur sec, échangeur de chaleur sur boucle d'eau refroidie, pompes).

Note :

Le dédoublement des réseaux de distribution (conduits et tuyauterie) n'est pas nécessaire pour respecter le critère Tier II.

D3060 Régulation et instrumentation

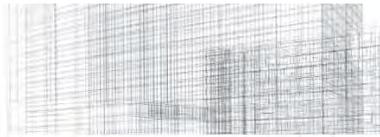
1. Fonctionnalité

- **Adaptabilité** – Assurer un contrôle permettant d'ajuster les paramètres d'alimentation en air refroidi en fonction des besoins exacts et évolutifs des équipements informatiques.
- **Interface de l'utilisateur** – Procurer, au responsable de l'exploitation et de la sécurité des installations, une interface graphique affichant les paramètres de fonctionnement (température, humidité relative, débit, consommation d'énergie, tendances, etc.), afin qu'il puisse assurer une surveillance de la fiabilité des équipements informatiques et leur efficacité énergétique.
- **Disponibilité du service** – Concevoir le système de contrôle de manière à maintenir le niveau de service escompté (Tier II).

D40 Protection incendie

1. Généralités

- **Normes et guides** – Consulter la norme NFPA 75 – *Standard for the Fire Protection of Information Technology Equipment*.



2. Fonctionnalité

– Disponibilité du service

- Évaluer les besoins particuliers de protection contre les incendies de chaque salle de serveurs, en fonction notamment de la vulnérabilité des installations informatiques et des techniques d'extinction qui peuvent être utilisées.
- Considérer l'installation de gicleurs de type pré-action et à brume pour une protection accrue contre les dommages causés par l'eau.
- Considérer l'installation d'un système d'extinction par agent gazeux « propre ».

Note:

Consulter la norme NFPA 2001 – *Standard on Clean Agent Fire Extinguishing Systems*.

Vérifier auprès de l'assureur et de la municipalité les exigences en matière de protection contre les incendies, notamment pour des gicleurs de type pré-action.

D50 Électricité

1. Généralités

Normes et guides

- CAN/CSA Z32 – Sécurité en matière d'électricité et réseaux électriques essentiels des établissements de santé.
- CAN/CSA C282 – Alimentation électrique de secours des bâtiments.
- *Uptime Institute – Data Center Site Infrastructure Tier Standard : Topology*.
- ANSI/TIA-942 – *Telecommunications Infrastructure Standard for Data Center*.
- ANSI/TIA-1179 – *Health Care cabling*.
- Guide d'aménagement du centre hospitalier du Ministère (*Base Building*).

2. Fonctionnalité

Distribution d'électricité dans la salle des serveurs et les salles des TIC satellites.

- Un seul parcours.

Serveurs

- La redondance des serveurs est déterminée selon la cote DIC (cote DIC : étape permettant de déterminer la performance des actifs informationnels en fonction de trois objectifs visant la sécurité de l'information : la disponibilité, l'intégrité et la confidentialité).

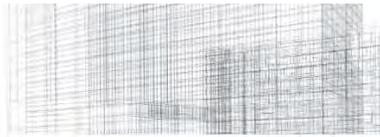
D5010 Service et distribution électrique

1. Fonctionnalité

- Considérer l'installation d'un composant permettant de supprimer les surtensions transitoires, de protéger les installations contre les surtensions transitoires nuisibles et contre les bruits de ligne électrique (*transient voltage surge suppression*) sur le réseau électrique réservé à la salle des serveurs, cela afin d'éliminer ou de réduire les dommages causés par les surtensions aux équipements de traitement de données et aux équipements essentiels.
- Assurer la disponibilité d'une alimentation électrique fiable et stable conforme au standard Tier II.
 - Un réseau de distribution électrique normal et un réseau de distribution électrique d'urgence assureront l'alimentation de la salle des serveurs et des salles des TIC satellites tout en évitant les coupures de courant par l'ajout d'alimentation statique sans coupure (ASSC).

Note :

Certains centres de traitement informatique régionaux seront considérés comme des centres de niveau Tier III. Il faudra alors prévoir plus de redondance dans les réseaux de distribution (câble, matériel et équipement).



2. Sécurité

- Restreindre les risques de défaut électrique dans la salle des serveurs et les salles des TIC satellites, notamment :
 - en les dotant d'une alimentation statique sans coupure (ASSC) pour assurer la continuité de l'alimentation électrique de leurs réseaux et éviter ainsi la perte de données ou l'arrêt d'un système sans une fermeture adéquate (se référer à la section D5090) :
 - en les raccordant au réseau d'alimentation électrique d'urgence et en les reliant à un groupe électrogène (se référer à la section D5090).

Note :

Tous les équipements de la salle des serveurs doivent être alimentés par le réseau d'urgence raccordé par un conducteur lui-même relié à la salle des groupes électrogènes.

Tous les serveurs de la salle des serveurs doivent être raccordés à l'ASSC afin qu'en cas de panne de courant, aucune coupure de courant ne soit possible dans l'attente de la prise en charge des équipements par le groupe électrogène.

- Munir la salle des serveurs d'un système de surveillance de l'environnement électrique.

3. Exploitation et entretien

- Permettre l'évolution de la salle des serveurs et des salles des TIC satellites en réduisant les risques de coupure.

Note :

Les panneaux électriques ne doivent pas être encastrés dans le mur car il est plus difficile de passer le câblage additionnel lorsque nécessaire.

Aucune boîte de jonction ne devrait être installée sous un plancher surélevé afin de limiter les risques opérationnels liés aux inondations.

D5020 Éclairage et distribution secondaire

Éclairage

1. Généralités

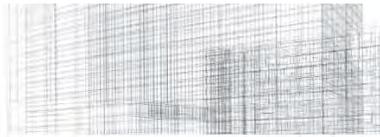
1. **Norme :** CAN/CSA Z317.5 – *Illumination Systems in Health Care Facilities*.

2. Sécurité

- Prévoir un éclairage approprié en utilisant des appareils et des composants capables de fournir un éclairage de qualité.
 - En général, l'éclairage de la salle des serveurs est de 500 lux et l'éclairage pour une tâche particulière de 750 lux.
- Utiliser des **détecteurs de mouvement** équipés d'un interrupteur manuel pour contrôler les luminaires des locaux tels que les salles de réunion, les salles de cours ou de repos et les vestiaires. Ailleurs, utiliser un interrupteur et l'intégrer à un système centralisé de contrôle de l'éclairage permettant la programmation horaire de chaque interrupteur.
- Prévoir des luminaires alimentés par une batterie dans la salle des serveurs et les salles des TIC satellites.

Prises de courant

- De façon générale, il faut prévoir pour l'UTIC des prises de courant sur les réseaux de distribution électrique normal et d'urgence.
- **Réseau d'urgence :** raccorder les prises de courant de la salle des serveurs et des salles des TIC satellites au réseau d'urgence (se référer au guide d'aménagement du centre hospitalier du Ministère pour plus de détails sur le réseau d'urgence).



- **Réseau d'ASSC:** raccorder les prises de courant de la salle des serveurs et des salles des TIC satellites au réseau d'ASSC (se référer au guide d'aménagement du centre hospitalier du Ministère pour plus de détails sur le réseau d'ASSC).

D5030 Communication et sécurité

1. Fonctionnalité

- Maintenir le fonctionnement des systèmes de communication et de sécurité en tout temps (24 heures sur 24, 7 jours sur 7).
- Considérer la possibilité d'une expansion future de 50 %.

2. Sécurité

Détection alarme incendie

- Assurer une protection contre les incendies par des moyens de détection adéquats :
 - a. installer des détecteurs de fumée;
 - b. relier ces détecteurs au système général de l'immeuble;
 - c. transférer les alarmes au poste de sécurité ou à un système central.
- Installer le panneau annonciateur près des bureaux et du poste de sécurité afin qu'une intervention puisse avoir lieu très rapidement en cas de besoin.

Exemple :

L'installation d'un système à alerte rapide pour la détection de fumée dans les zones critiques peut être considérée.

Système de téléphonie/télécommunication

- Relier les circuits au réseau d'urgence pour les armoires de téléphonie.
- Protéger les circuits reliés au réseau d'urgence à l'aide d'une ASSC.
- Prévoir des répartiteurs sur les étages.
- Ventiler adéquatement les armoires de téléphonie.

Note :

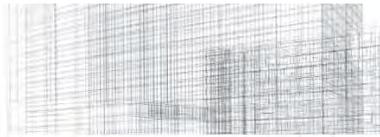
Si l'installation d'un réseau de téléphonie IP est considéré, les armoires de téléphonie ne seront plus nécessaires. Il faudra plutôt considérer l'utilisation d'un serveur de communication central, de téléphones IP, de passerelles VoIP et de commutateurs IP.

Câblage réseau et réseau de fibres optiques

- S'assurer d'avoir deux réseaux de fibres optiques empruntant deux routes totalement distinctes à l'entrée du bâtiment, si la mission de l'établissement nécessite ce type de réseau.
- Protéger le réseau des risques de coupure électrique.
 - Utiliser des connecteurs de type « *twist lock* » pour le câblage alimentant les cabinets des serveurs.
- Assurer la redondance aux points stratégiques (doublement des équipements essentiels : câbles et matériel, lorsque cela est nécessaire);
- Répartir les salles des TIC satellites sur différents étages en respectant les longueurs de câbles requises selon la superficie du bâtiment (effectuer une distribution en étage : salles superposées d'un étage à l'autre).
- Réserver exclusivement les locaux techniques aux équipements de liaison informatique ou de télécommunication.
- Séparer le câblage à l'aide de râteliers (chemins de câbles) pour éviter les croisements de courants forts avec des courants faibles.

Note :

Dans la salle des serveurs, l'installation du réseau de distribution électrique et du câblage peut être effectuée par le haut (au-dessus des cabinets) ou par le bas (sous un plancher



surélevé).

- La tendance actuelle consiste à faire cette installation par le haut. Toutefois, cela dépendra de la solution mécanique retenue.
- Il importe de se coordonner avec les responsables de l'installation mécanique pour effectuer ce choix.

Sécurité et contrôle des accès

- Assurer la sécurité de la salle des serveurs et des salles des TIC satellites et contrôler leur accès.
 - a. Limiter l'accès à ces salles aux principaux intervenants concernés.
- Installer un système de contrôle des accès sécurisé permettant l'enregistrement des accès.

Note :

Le contrôle des accès à la salle des serveurs ou aux salles des TIC satellites peut être effectué à l'aide d'un :

- lecteur magnétique ou biométrique.

Le contrôle des accès peut être effectué par l'enregistrement de différentes données :

- nom de l'utilisateur, local, date, heure, durée de la visite ou de la séance de travail, etc.

- Procéder à la journalisation des accès.
- Implanter un système de surveillance local et à distance des équipements importants (ex. : ASSC, CVCA, extincteurs au gaz, groupe électrogène, etc.).

Exemples :

En vue de protéger l'UTIC contre les intrusions frauduleuses ou le vol de données :

- à l'intérieur : concevoir des salles fermées avec caméra et poste de surveillance vidéo;
- à l'extérieur : installer des systèmes de sécurité et de surveillance avec verrou électronique.

Une salle adjacente vitrée comportant des bureaux peut être installée à proximité de la salle des serveurs pour la surveillance des travaux plus longs (ex. : sous-traitance).

Intrusions et malveillance

- Assurer une surveillance et maintenir le fonctionnement en tout temps (24 heures sur 24, 7 jours sur 7) des systèmes de :
 - a. détection de fumée;
 - b. détection de chaleur;
 - c. détection de température;
 - d. détection d'incendie (feux couvants ou informatiques);
 - e. détection des intrusions (contacts de porte, détecteurs de mouvement);
 - f. contrôle électronique des accès à la salle des serveurs;
 - g. détection de dégât d'eau.
- Procéder à la journalisation des accès.

Exemple :

La surveillance peut être effectuée en tout temps (24 heures sur 24, 7 jours sur 7) avec les équipements suivants :

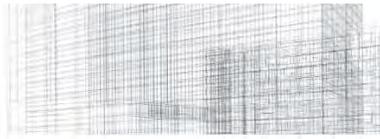
- caméras de surveillance;
- détecteurs de mouvement.

On peut aussi avoir recours à un agent de sécurité, si nécessaire.

- Centraliser les alarmes (techniques, contre les intrusions, de détection des incendies, etc.) et s'assurer que le temps d'intervention est adéquat lorsqu'une alarme est déclenchée.
- Procéder à la journalisation des accès.

Exemple :

Le recours à un système de surveillance signalant l'ouverture prolongée d'une porte peut être considéré pour le contrôle des accès à la salle des serveurs.



D5090 Autres systèmes électriques

Alimentation électrique de secours

1. Fonctionnalité

- Maintenir en tout temps (24 heures sur 24, 7 jours sur 7) le fonctionnement du système d'alimentation électrique.

2. Sécurité

- Prévoir une redondance automatique de l'alimentation de secours (redondance du groupe électrogène).

3. Exploitation et entretien

- Réduire les interruptions de courant, même pour les opérations de maintenance.
 - h. La continuité de l'alimentation électrique doit être assurée lors de la maintenance dans les unités répondant aux normes de la classification Tier III. Pour les installations correspondant à la classification Tier II, les coupures d'électricité « *shut down* » devront être planifiées avant toute opération de maintenance.

Note :

Analyser la capacité nécessaire du groupe électrogène pour la salle des serveurs en considérant la possibilité d'expansion future selon l'option choisie :

- groupe électrogène servant à plusieurs secteurs;
- groupe électrogène réservé à la salle des serveurs.

Le groupe électrogène devrait fonctionner avec une charge de moins de 80 % pour assurer un bon fonctionnement des installations et des équipements.

Doter la salle des serveurs d'une capacité de recouvrement réduisant le risque de failles en cas de désastre.

ASSC : Alimentation statique sans coupure (batterie ayant une autonomie de quinze minutes)

1. Fonctionnalité

- Se prémunir contre les risques de coupure de l'alimentation électrique du fournisseur en utilisant une alimentation électrique autonome.

Note :

L'installation d'une ASSC permet de régulariser la tension et d'arrêter les serveurs de façon adéquate lorsqu'il y a défaillance du groupe électrogène.

2. Sécurité

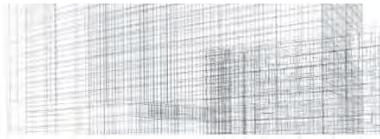
- Prévoir une redondance automatique de l'ASSC.

Note :

Prévoir des prises de courant de la salle des serveurs sur l'ASSC, il faut toutefois en prévoir sur le réseau électrique normal aussi.

3. Exploitation et entretien

- Installer de préférence l'ASSC près de la salle des serveurs afin de :
 - fournir une énergie électrique de qualité réduisant les perturbations sur le réseau de télécommunication;
 - assurer la disponibilité et la continuité des services électriques tout en protégeant les installations et les équipements;
 - permettre l'arrêt des serveurs en cas de défaillance du groupe électrogène.



Note :

L'ASSC devrait fonctionner avec une charge de moins de 80 % pour assurer un bon fonctionnement des installations et des équipements.

Mise à la terre

1. Sécurité

- Effectuer une mise à la terre (MALT) adéquate pour les systèmes informatiques.
 - o effectuer une MALT mécanique et électrique de tous les équipements (cabinets, échelles à câble, etc.);
 - o installer une MALT pour les planchers.

Note

Pour effectuer une bonne MALT, se référer à la norme ANSI/TIA-607-A.

E Équipements et ameublement

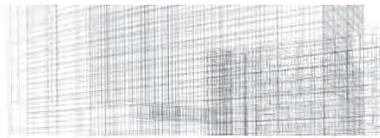
E20 Ameublement et décoration

1. Confort

- Prévoir un mobilier qui peut être ajusté en hauteur, selon les besoins des utilisateurs et lorsque la tâche à accomplir le requiert.
- Prévoir un coup de pied et, lorsque nécessaire, un appuie-pieds pour les meubles qui servent dans les zones de travail en station debout.

2. Sécurité

- Prévoir, sur l'ameublement mobile, des freins qui soient faciles d'accès et d'utilisation.



Annexe

Extrait du *Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité* – chapitre III.

Sécurité physique

Pour l'emplacement des installations et du matériel

Les locaux où se trouvent les ordinateurs centraux, les mini-ordinateurs, les serveurs des réseaux locaux, le matériel de télécommunication et autres actifs informationnels doivent :

- i. être situés dans des endroits protégés contre les catastrophes naturelles (ex. : verglas, inondations) ou accidentelles (ex. : bris d'aqueduc ou de tuyauterie, surchauffe, déclenchement de gicleurs);
- ii. être protégés par des mécanismes de contrôle d'accès;
- iii. être munis de systèmes de chauffage, de ventilation et de climatisation conformes aux normes recommandées par les fournisseurs;
- iv. être munis d'un système d'alimentation électrique sans interruption et d'un système de protection contre les incendies;
- v. permettre de voir les faits et gestes du personnel autorisé présent à l'intérieur du local (aire ouverte).

Les équipements, ce qui comprend les imprimantes, les photocopieurs et les télécopieurs, doivent être placés de façon à éviter toute utilisation et observation non autorisées.

Pour le contrôle de l'accès aux locaux

L'accès aux locaux où se trouvent les ordinateurs centraux, les mini-ordinateurs, les serveurs des réseaux locaux, le matériel de télécommunication et autres actifs informationnels doit être limité au strict minimum et réservé aux personnes autorisées uniquement.

Une liste des personnes autorisées à accéder à ces locaux doit être constituée. Outre le nom de ces personnes, la liste comporte l'énumération des tâches autorisées pour chacune d'entre elles et la durée habituelle de leur intervention. Cette liste doit être mise à jour périodiquement.

Un mécanisme de contrôle de l'entrée et de la sortie des personnes qui accèdent aux locaux sécurisés doit être mis en place.

Le personnel externe (ex. : fournisseurs, consultants, tiers n'étant pas des employés) chargé de l'entretien et de la réparation des équipements ou de tout autre type d'intervention permise doit être accompagné par une personne autorisée.

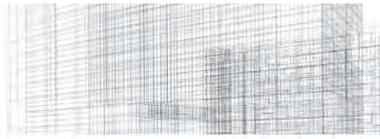
Pour le matériel informatique (incluant les portables)

L'inventaire des équipements, précisant la localisation et l'assignation principale de ces équipements, doit être constitué et tenu à jour.

La configuration de base des équipements installés doit être définie et tenue à jour.

Le registre de l'entretien des équipements doit être constitué et tenu à jour.

Les équipements déclarés en surplus ou mis au rebut doivent être exempts d'information électronique avant leur abandon.



Les renseignements nominatifs ou de nature sensible contenus sur les supports magnétiques (disque dur, disquette, CD-ROM) que l'on désire éliminer doivent être détruits de façon à ce que leur caractère confidentiel soit protégé.

L'information contenue sur tout équipement à déplacer doit, au préalable, être analysée et, le cas échéant, éliminée.

Des procédures ou des mécanismes de protection contre l'utilisation non autorisée et le vol des équipements doivent être mis en place.

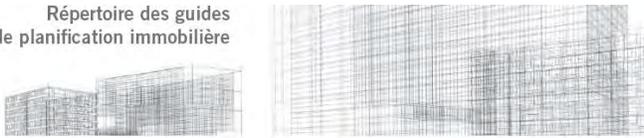
L'organisme doit instaurer une procédure obligatoire pour autoriser la sortie d'équipement hors de ses installations.

Pour plus de détails sur les autres sections sur la sécurité

Voir le Cadre de gestion au :

- [http://Ministère4.Ministère.gouv.qc.ca/extranet/ri.nsf/04bdef86723b0cf8852566de004c8583/9c29ee7e5c5d42058525703b00725379/\\$FILE/Cadre%20global%20de%20gestion-volet%20securite_V2007-03.pdf](http://Ministère4.Ministère.gouv.qc.ca/extranet/ri.nsf/04bdef86723b0cf8852566de004c8583/9c29ee7e5c5d42058525703b00725379/$FILE/Cadre%20global%20de%20gestion-volet%20securite_V2007-03.pdf) :

- 2.4. sécurité logique;
- 2.5. sécurité de l'exploitation de ces actifs;
- 2.6. sécurité des applications;
- 2.7. sécurité des télécommunications.



Références

Sources documentaires

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE). ASHRAE Datacom Series (titres divers). Pour obtenir une liste des publications, consulter le site suivant : [<https://www.ashrae.org/resources--publications/bookstore/datacom-series>].

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE). *Handbook Applications*, chap. 19 : « Data Processing and Telecommunication Facilities », 2011.

AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS (ASHRAE). *Thermal Guidelines for Data Processing Environments*, 2^e édition, 2009, 58 p. (coll. Datacom).

ASSOCIATION CANADIENNE DE NORMALISATION. « CAN/CSA Z317.2-10 – Systèmes de chauffage, de ventilation et de conditionnement d'air (CVCA) dans les établissements de santé : exigences particulières », CAN/CSA, mise à jour n^o 1, février 2011.

MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX (Ministère). *Guide d'élaboration et de mise en œuvre : Cadre de gestion des infrastructures publiques (Inventaire – État des infrastructures – Maintien des actifs – Déficit de maintien des actifs – Valeur de remplacement)*, 2014, 33 p. [En ligne]. [http://www.tresor.gouv.qc.ca/fileadmin/PDF/infrastructures_publiques/cadres/GestionInfrastructures.pdf].

MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX (Ministère). *Plan stratégique 2010-2015 du ministère de la Santé et des Services sociaux*, 2010, 52 p. [En ligne]. [<http://publications.msss.gouv.qc.ca/acrobat/f/documentation/2010/10-717-02.pdf>].

MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX (Ministère). *Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité*, version révisée, 2007, 76 p. [En ligne]. [www.Ministère.gouv.qc.ca] (section « Documentation », rubrique « Publications »).

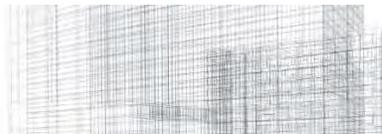
MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX (Ministère). *Plan stratégique 2005-2010 du ministère de la Santé et des Services sociaux*, 2005, 47 p. [En ligne]. [<http://publications.msss.gouv.qc.ca/acrobat/f/documentation/2005/05-717-01.pdf>].

MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX (Ministère), PELLETIER, Lucie (chef de projet), et coll. *Les orientations technologiques du réseau sociosanitaire : Pour un accès intégré et sécurisé de l'information*, 2003, 274 p. [En ligne]. [http://catalogue.iugm.qc.ca/GEIDFile/RTSS.PDF?Archive=192342491052&File=RTSS_PDF].

MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX (Ministère). *Recueil de mesures de sécurité de l'information : Trousse d'outils*, version 2.0, 2003, 103 p. [En ligne]. [[http://msssa4.msss.gouv.qc.ca/extranet/ri.nsf/0/029246b809ea0d158525703c005ef3ab/\\$FILE/recueil de mesures.PDF](http://msssa4.msss.gouv.qc.ca/extranet/ri.nsf/0/029246b809ea0d158525703c005ef3ab/$FILE/recueil%20de%20mesures.PDF)].

MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX (Ministère), PELLETIER, Lucie (chef de projet), et coll. *Les orientations technologiques du réseau sociosanitaire : Pour un accès intégré et sécurisé de l'information – Document synthèse*, 2001, 32 p. [En ligne]. [<http://www.santecom.qc.ca/BibliothequeVirtuelle/MSSS/2550377389.pdf>].

NATIONAL FIRE PROTECTION ASSOCIATION. « NFPA 75: *Standard for the Protection of Information Technology Equipment* », NFPA, 2013.



TELECOMMUNICATIONS INDUSTRY ASSOCIATION. « ANSI/TIA-942-2-2010 – *Telecommunications Infrastructure Standard for Data Centers Addendum 2 – Additional Guidelines for Data Centers* », ANSI/TIA, 2010.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION. « ANSI/TIA-942-2005 – *Telecommunications Infrastructure Standard for Data Centers* », ANSI/TIA, 2005.

TURNER, W. P., et collab. *Tier Classification Define Site Infrastructure Performance*, New York, Uptime Institute, 2008, 19 p. (coll. Uptime Institute White Paper). [En ligne]. [<http://www.greenserverroom.org/Tier-Classifications-Define-Site-Infrastructure.pdf>].

UPTIME INSTITUTE PROFESSIONAL SERVICES, LLC. *Data Center Site Infrastructure Tier Standard: Topology*, New York, Uptime Institute, 2010, 8 p. [En ligne]. [<http://www.gpxglobal.net/wp-content/uploads/2012/08/tierstandardtopology.pdf>].



GLOSSAIRE

Le présent glossaire définit certains termes relatifs aux activités liées aux technologies de l'information et des communications, de même que certains termes plus généraux.

Actif informationnel	Banque d'informations électroniques, système d'information, réseau de télécommunication, technologies de l'information, installations électroniques ou ensemble de ces éléments. Un équipement médical spécialisé ou ultra-spécialisé peut aussi comporter des composantes qui font partie des actifs informationnels, notamment lorsqu'il est relié de façon électronique à des actifs informationnels. (réf. : Loi sur les services de santé et les services sociaux, art. 520.1). S'ajoutent à cette liste les documents imprimés générés par les technologies de l'information (voir le Cadre de gestion des actifs informationnels appartenant aux organismes de réseau de la santé et des services sociaux – Volet sur la sécurité).
Audit	Dans le contexte du présent document, évaluation périodique basée sur des critères définis permettant de vérifier si les normes de l'ensemble ou d'une partie du Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité sont appliquées.
Banque d'informations électroniques	Collection d'informations électroniques relatives à un domaine défini, regroupées et organisées de façon à en permettre l'accès.
Dossier patient électronique	Le dossier patient électronique, ou dossier clinique informatisé, permet un accès rapide au dossier du patient. Ce dossier étant numérisé, on peut y accéder à partir de plusieurs établissements ou organismes, tout en conservant la confidentialité désirée.
Équipement informatique	Ordinateurs, mini-ordinateurs, micro-ordinateurs, postes de travail informatisés, incluant leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de communication, de réception et de traitement de l'information, et tout équipement de télécommunication.
Information électronique	Information sous toute forme (textuelle, symbolique, sonore ou visuelle), dont l'accès et l'utilisation ne sont possibles qu'au moyen des technologies de l'information.
Infrastructure commune	Ensemble des composantes matérielles, logicielles, technologiques et organisationnelles partagées en tout ou en partie par le Ministère et les organismes du RSSS.
Impartition	Entente contractuelle entre une entreprise et un tiers pour la gestion continue et l'amélioration des activités reliées à une partie ou à l'ensemble : 3. d'une infrastructure (ex. : systèmes d'information, systèmes de sécurité, réseaux de télécommunication); 4. des processus opérationnels (ex. : exploitation d'un réseau de télécommunication).
Organisme	Dans le cadre du présent document : le Ministère, les régies régionales et les autres établissements du RSSS.
Politique de sécurité	Énoncé général émanant de la direction d'un organisme et indiquant la ligne de conduite adoptée relativement à la sécurité, à la mise en œuvre des mesures visant à assurer la sécurité et à leur gestion. Mentionnons qu'il importe de faire une utilisation appropriée et sécuritaire des TI dans le respect de toute loi liée au traitement de l'information.
Réseau étendu	Un réseau étendu se dit d'un réseau local qui devient une partie d'un réseau plus large lorsqu'une liaison est établie (par l'intermédiaire de modems, d'aiguilleurs distants, de lignes téléphoniques, de satellites ou d'autres connexions) avec un gros système, un réseau de données public ou un autre réseau local.
Réseau informatique	Ensemble des composantes et des équipements informatiques reliés par voie de télécommunication, soit pour accéder à des ressources ou à des services informatisés, soit pour en partager l'accès.
Réseau local	Réseau informatique de taille réduite limité, le plus souvent, à un seul organisme.
Technologie de l'information	Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer de l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).
Télécommunication	Ensemble des procédés électroniques et informatiques de transmission d'information à distance.
Unité d'exploitation informatique	Unité administrative qui a comme tâche d'assurer le bon fonctionnement, l'amélioration et l'entretien des services informatiques de l'organisme.