Orientations technologiques de la DRI - CHU

À joindre aux appels d'offres du

CHU de Québec

Direction des ressources informationnelles

Septembre 2020

Version 1.25 pour le CHU

TABLE DES MATIÈRES

TABLEAU DE RÉVISION DU DOCUMENT

Version	Date	Révisé par	Sujet/ajout
1.0	25-03-2014	Michel Julien	Document de travail initial
1.1	02-07-2014	Michel Julien	Ajout et ajustement en surbrillance de couleur jaune.
1.2	10-09-2014	Hélène Levasseur/ Chantale Pineault	Ajouts des clauses ISO 27002 concernées. Ajout de l'annexe B.
1.3	12-09-2014	Michel Julien	Ajout des points 7.3.10 et 7.3.11 pour Charles D.T.
1.4	23-12-2014	Michel Julien	Ajout de l'annexe A
1.4a	14-01-2015	Michel Julien	Ajout au point 5.3.7, section sans fil.
1.4b	26-01-2015	Michel Julien	Changement majeur au point 3. Ajout aux points 4.3.1 à 4.3.5 et l'annexe C pour Charles D.T. Révision finale avec les responsables de chaque secteur.
1.5	30-01-2015	Michel Julien Hélène Levasseur	Changement important à l'annexe B et C par Hélène Levasseur. Révision finale avec Mario Trottier et Sylvain Frenette. Apporter les ajustements au texte. Ajout des acronymes, des sigles et du glossaire. Correction du document par Sandra Ovejero
1.6	09-02-2015	Michel Julien et Yvan Fournier	Ajout de trois paragraphes à la fin du point 2.
1.6a	17-02-2015	Michel Julien Yvan Fournier	Ajouter « ou équivalent » aux marques de produits. Ajouter la norme minimale à l'accès utilisateur sans fil de la section « Gestion des accès ». Ajout d'explication à l'annexe A du besoin de liste de matériels et d'équipements.
1.6b	16-03-2015	Michel Julien et Yvan Fournier	Petits ajustements apportés à la demande d'Yvan.
1.7	21-04-2015	Michel Julien	Petits ajustements à la demande de Luc Duval. Ajout d'une section d'information sur le sans-fil à l'annexe A.
1.8	03-08-2015	Pierre-Luc Caseault et Michel Julien	Insertion du point 4, Intégration aux systèmes du CHU de Québec. Ajout d'item dans acronyme et glossaire.

1.9	21-10-2015	Michel Julien	Ajustements apportés aux orientations du tableau 4.
1.10	28-10-2015	Pierre-Luc Caseault et Michel Julien	Ajustements apportés au point 4. Ajout de l'annexe D pour le DPE.
1.11	août 2016 octobre 2016 Janvier 2017	Michel Julien, Serge Larochelle, Guy Verreault, Christian ngor DIENE et Hélène Levasseur.	Mise à jour et révision du document au complet. Mise à jour des tableaux de l'annexe C.
1.12	Février 2017	Michel Julien et Martin Rousseau.	Ajustement apporté au point 4 et ces sous-points. Annexe D enlevée.
1.13	Juin 2017	Christian Ngor DIENE	Plan des locaux d'accès et de distribution. Modèle des antennes sans-fil. Normalisation du câblage et de l'identification.
1.14	Janvier 2018	Mario Trottier Michel Julien	Ajuster texte tableau 3. Enlever toutes informations référant à des marques ou modèles de produits. Remplacer DTI par DRI.
1.15	Janvier 2018	Stéphane Grenier	Plusieurs ajustements, ajouts et corrections.
1.16	Janvier 2018	Neima Mohamed	Ajustement apporté sur le plan des locaux d'accès et de distribution. Normalisation du câblage Ajout d'item dans glossaire
1.17	Janvier 2018	Stéphane Grenier	Modification, Ordinateur portable, retiré les marques et remplacé par « Proposé par le soumissionnaire ou par la DRI. »
1.18	Mars 2018	Christian Ngor DIENE	Respect de conformité avec l'appel d'offres en vigueur au niveau de la DRI.
1.22 CHU	Octobre 2018	Stéphane Grenier	Mise à niveau de versions de produits, protocoles engin, WIFI, ajout des nouveautés du NCH à l'annexe A (intégration des corrections de la version 1.19). **Uniformisation avec la version NCH.** Il faut mettre à jour en parallèle les 2 versions à l'avenir.

1.23 CHU	Décembre 2018	Stéphane Grenier	Mise à jour Windows 10/7, remplacé « le » par « son » dans « encore supportée par son fabricant »
1.24 CHU	Juillet 2019	Christian DIENE	Panneaux de fibre CCH-04U au lieu des 2 U
1.25 CHU	Septembre 2020	Stéphane Grenier	Ajout VMWARE 6.7, MS SQL 2019, MS Serveur 2019, Service F CHU, Version AD. Modifications de spécifications ordinateurs de table, portables et tablettes, retrait IE 11, ajout Edge Chromium, retrait Windows 7, retrait Windows serveur 2008, changement de version infra BVI, ajout protocole de sécurité Web TLS 1.2 et +, Ajout de la version de SAMBA 2 et +

1. INTRODUCTION

L'Organisme public, à titre de membre du réseau de la santé et des services sociaux, s'assure de mettre tous les moyens en place pour se conformer aux différents cadres technologiques émis par le ministère de la Santé et des Services sociaux et aux tendances majeures sur le marché. L'ensemble de l'infrastructure actuelle tend ainsi à orienter ses choix en fonction de ces prérogatives.

Toute l'infrastructure des systèmes d'informations du CHU de Québec est en constante évolution afin de soutenir la mission de l'organisme public.

Ce document d'orientations technologiques est joint à tout appel d'offres du CHU de Québec comprenant des équipements ou des systèmes faisant appel à des composantes informatiques soient : serveur, micro-ordinateur, imprimante ou tout autre système ou périphérique informatiques susceptibles d'être connectées au réseau de télécommunication filaire et/ou sans-fil.

L'adjudicataire sera responsable de la mise en production de sa solution en collaboration avec la Direction des technologies de l'information qui désignera un représentant. De plus, un travail conjoint avec la Direction des technologies de l'information (DRI) sera nécessaire pour l'implantation et la maintenance de la solution afin d'en assurer l'exploitation.

2. RESPECT DES ORIENTATIONS TECHNOLOGIQUES

En lien avec les orientations et les normes du MSSS, la DRI demande au soumissionnaire de respecter et de supporter les orientations technologiques énumérées aux prochains points lorsqu'il propose un nouveau système d'information. Ces orientations couvrent l'ensemble des aspects informatiques pour proposer une solution informatique et/ou du service au CHU de Québec.

Au point 3, nous y retrouvons les équipements technologiques soient : les serveurs, les ordinateurs de bureau, les équipements de télécommunication et de sécurité, les progiciels et les versions supportés, en plus des différentes normes de télécommunication et de sécurité des systèmes d'informations au CHU de Québec. Au point 4, nous y retrouvons les recommandations sur l'intégration aux systèmes du CHU de Québec. Également, veuillez considérer les annexes après le point 5 qui détaille plus précisément les orientations à respecter et à supporter pour certaines technologies.

En tout temps, le soumissionnaire devra proposer une architecture et une infrastructure détaillée à l'aide de document et de schéma exprimant clairement son système d'information.

Pour le contrat de service, le CHU de Québec exige que le soumissionnaire s'engage à rehausser sa solution lorsqu'un produit vient à échéance et à cela ces frais. Ce qui veut dire que lorsque la version du système d'exploitation (du serveur ou du poste de travail), du système de gestion de base de données (SGBD : MSSQL ou Oracle) ou de tout autre produit nécessaire à l'utilisation de sa solution est compromise par la fin d'un produit.

Exemple : Si la solution acquise par le CHU de Québec fonctionne sur Windows serveur 2008 et qu'elle est sous contrat de service, alors que ce produit (Windows 2008) ne sera plus supporté par Microsoft, le fournisseur devra rendre sa solution fonctionnelle sur une version supérieure supportée par Microsoft le plus tôt possible, et ce sans frais supplémentaire.

Toutes les solutions proposées par un soumissionnaire doivent obligatoirement supporter l'environnement Citrix. Ce qui veut dire que ses applications doivent fonctionner adéquatement à partir de Citrix.

3. TABLEAU – DESCRIPTION DES TECHNOLOGIES EN PLACE AU CHU DE QUÉBEC – UNIVERSITÉ LAVAL

Les informations qui se retrouvent dans ce tableau représentent tout ce qui est en place actuellement au CHU de Québec – Université Laval, il sert de guide pour les soumissionnaires afin qu'ils puissent proposer des solutions qui s'y adaptent dans le respect des orientations en place.

Les produits identifiés sont ceux actuellement utilisés au CHU de Québec et sont identifiés afin d'aider les fournisseurs à la compréhension de l'environnement actuel et assurer la compatibilité avec les systèmes et équipements déjà en place.

Item	Type	Orientation	Niveau d'exigence
INFRASTRUCTURE CTI (CENTRE DE TRAITEMENT INFORMATIQUE)			
CABINET D'ÉQUIPEMENT	Matériel	➢ Actuellement utilisé APC *Netshelter* SX 42U. No de modèle AR3100 et R.F.Mote modèle RFM-1948-RB. ➢ Actuellement utilisé 2 unités de distribution d'alimentation de marque APC et Eaton pour cabinet 240 Volts, *Ethernet* 10/100, 42 connecteurs de sortie, No de modèle AP8841(APC) et EMI200-10(Eaton).	
PANNEAUX/PORTE D'ACCÈS	Matériel	➢ Panneaux d'accès actuellement utilisés : Karp, série DSC-214M, Lajoie série RL2001, Acudor série UF-5000, Cendrex, série ADH. ➢ Panneaux d'accès coupe-feu actuellement utilisés: Karp, série KRP150-FR, Lajoie série RL2012-FRN, Acudor série FB-5060, Cendrex, série PFI.	
SERVEUR	Matériel INTEL	➢ Le serveur de type enfichable (rackmount) est exigé dans une salle de serveur avec câbles d'alimentation AC 208v C14. Actuellement, serveur HPE série Proliant DL380 Gen10. ➢ L'ensemble des composantes est redondant. (bloc d'alimentation, cartes réseau 1, et 10 Gbps de type RJ45, disques durs de type entreprise, etc. ➢ Garantie 4 ans et support 8h/5jours ouvrables de base. ➢ Exemple de configuration de base recommandé pour les disques durs : 2 disques durs pour l'O/S configuré en RAID 1 4 disques durs pour les données et l'application configurée en RAID 5 ou RAID 6.	
	Matériel SUN Logique	➢ Actuellement, un SUN équipé minimalement selon l'appel d'offres, ou mieux selon les recommandations du fabricant pour convenir aux besoins du système. ➢ Spécifier les capacités recommandées pour un minimum d'utilisation de 4 ans. (CPU, mémoire vive et l'espace disque nécessaire) pour Sun et Intel. L'espace requis minimal se conforme à l'espace minimal requis par le système + Jeux de sauvegarde + 20% d'espace libre, la valeur la plus haute étant requise.	

PROGICIEL DE SYSTÈME	Serveur Virtuel Serveur Microsoft Serveur SUN/Oracle	➢ Actuellement, le serveur Virtuel sous *VmWare 6*.5 et 6.7 ➢ Microsoft Windows serveur 2016/2019 (64 bits). ➢ Portail Web IIS v10 et plus de Windows. ➢ Intégration au domaine AD Windows privilégié. ➢ Protocole LDAP**S** supporté. ➢ Démarrage en mode service des applications. ➢ Maintenance mensuelle (application des mises à jour et des correctifs de Microsoft), supporter les dernières rustines; Si le système ne peut s'y conformer, les serveurs devront être isolés dans un VLAN dédié. ➢ Actuellement, Solaris. ➢ Actuellement, Serveur Virtuel de préférence sous Solaris. ➢ <u>Pour tous les points énumérés, le logiciel ou système se limite à la version actuelle ou à la version majeure précédente encore supportée par son fabricant.</u>	
SYSTÈME DE GESTION DE BASE DE DONNÉES	Oracle Ms SQL	➢ Oracle 12c ou plus. ➢ Microsoft SQL 2016/2019 (64 bits) et plus ➢ Microsoft SQL Standard privilégié. (L'utilisation d'une version entreprise requiert justificatif) ➢ <u>Pour tous les points énumérés, le logiciel ou système se limite à la version actuelle ou à la version majeure précédente encore supportée par son fabricant.</u>	
SYSTÈME DE HAUTE DISPONIBILITÉ	Serveur	➢ Actuellement, VmWare High Availability (HA); ➢ NLB (balancement de charge réseautique) pour IIS portail Web; ➢ Actuellement, Mise en grappe serveur de fichier (*Cluster* Microsoft); ➢ Actuellement, Mise en grappe Ms SQL (*Cluster* Microsoft).	
SAUVEGARDE DES DONNÉES	Logique	➢ Fournir la documentation technique des données fichiers et des bases de données à sauvegarder; ➢ Les applicatifs dans les serveurs virtuels supportent les instantanés *VmWare Snapshot;* ➢ *Les serveurs de bases de données effectuent quotidiennement une copie de sécurité localement sur les*	

		disques des serveurs, la copie locale est ensuite récupérée par l'engin de sauvegarde du CHU; ➢ *Une copie de sécurité du système d'exploitation est prise sur une base régulière par l'engin de sauvegarde du CHU;* ➢ *Une copie de sécurité des répertoires de fichiers spécifique est prise quotidiennement par l'engin de sauvegarde du CHU.*	
ENVIRONNEMENT DE STOCKAGE	Matériel Logiciel	➢ La technologie *block storage* via *Storage Area Network* (SAN) en *fiber channel* (FC) permet de centraliser et de sécuriser les dépôts de données utilisées au CHU de Québec dans plusieurs de ces CTI. ➢ Spécifier les besoins en espace disques nécessaires pour tous les types des données qui seront requis par le système. L'espace requis minimal se conforme à l'espace minimal requis par le système + Jeux de sauvegarde + 20% d'espace libre, la valeur la plus haute étant requise.	
ENVIRONNEMENT DE TEST ET/OU DE FORMATION	Matériel	➢ Serveur physique ou virtuel dédié à cette tâche. * ➢ Le fournisseur fourni le détail ces environnements. * *Lorsque ce type d'environnement est requis.	
REMISE EN ÉTAT DES SYSTÈMES	Logique	➢ Avec la participation du fournisseur, un plan de reprise après sinistre des systèmes est documenté et éprouvé avant la mise en production dans le CHU de Québec. Le fournisseur remet en fonction le système suite à une panne.	
GESTION DES SERVEURS	Logique	➢ Les administrateurs désignés de la DRI ont les droits de gestion sur tous les serveurs. ➢ La DRI se réserve le droit d'installer les agents nécessaires pour faire la surveillance des serveurs. ➢ Le fournisseur effectue la gestion du système d'information hébergé sur le serveur.	
INFRASTRUCTURE DE TÉLÉCOMMUNICATION TCP/IP (données, voix, vidéo, téléphonie IP) (filaire et sans fil)			
RITM ET CHU DE QUÉBEC	Réseau logique	➢ Les applications qui transigent sur le réseau de la santé doivent obtenir une certification par le CRIM partenaire du MSSS. ➢ Vitesse des liens entre les sites :	

		○ RITM (10, 100, 200 et 300 Mbps) ○ CHU de Québec (1 et 10Gbps)	
COUCHE D'ACCÈS	Matériel	➢ Voir les exigences d'infrastructure de télécommunications au CHU de Québec à l'annexe A.	
COUCHE DE DISTRIBUTION	Matériel	➢ Voir les exigences d'infrastructure de télécommunications au CHU de Québec à l'annexe A.	
COUCHE CŒUR DU RÉSEAU	Matériel	➢ Voir les exigences d'infrastructure de télécommunications au CHU de Québec à l'annexe A.	
FILAIRE FIBRE OPTIQUE	Matériel	➢ Voir les exigences d'infrastructure de télécommunications au CHU de Québec à l'annexe A.	
FILAIRE CUIVRE	Matériel	➢ Voir les exigences d'infrastructure de télécommunications au CHU de Québec à l'annexe A.	
SANS FIL	Matériel	➢ Actuellement utilisé, Cisco Aironet 2800,1600. Voir les exigences d'infrastructure de télécommunications au CHU de Québec à l'annexe A.	
TÉLÉPHONIE IP	Matériel	➢ Tous les systèmes qui s'interfacent avec le système de téléphonie du CHU actuel utilisent la technologie SIP trunck et sont compatibles avec le Call Manager Cisco version 11,5 et supérieur. Voir les exigences d'infrastructure de télécommunications au CHU de Québec à l'annexe A.	
RÉSEAU VIRTUEL (VLAN)	Logique	➢ Protocole TCP/IP. ➢ L'adressage du RITM est utilisé dans tous les sites.	
RÉSEAU VIRTUEL D'EXCEPTION	Logique	➢ Certains équipements se retrouveront dans des réseaux d'exception (isolés) afin de sécuriser l'ensemble des systèmes du CHU de Québec.	
ADRESSAGE IP	Logique	➢ Les adresses IP sont fournies par le responsable de l'infrastructure des télécommunications de la DRI. ➢ Le service DHCP est utilisé, sauf dans quelques cas d'exception. ➢ Le besoin de service *Multicast* pour une application, un serveur, une caméra IP ou autre, doit être clairement défini par le soumissionnaire pour permettre à la DRI d'en faire l'intégration sur l'infrastructure de télécommunication du CHU de Québec.	
CÂBLAGE STRUCTURÉ	Matériel	➢ Actuellement utilisé : Belden, Leviton (câblage General Cable ou Superior Essex), Panduit, Corning.	

INFRASTRUCTURE ET NORME DE SÉCURITÉ			
MUR COUPE-FEU	Matériel	➢ Actuellement, manufacturier : *Fortinet et Cisco* ➢ Fonctions UTM activées dans la plupart des équipements ➢ Capacité de traitement adéquate selon les besoins. ➢ Plusieurs zones démilitarisées afin de séparer les zones de confiance. Les zones à haut risque sont contrôlées par mur coupe-feu, IPS et antivirus réseau. Les zones serveurs sont distinctes des postes de travail, tous les ports sont ouverts de façon granulaire selon les spécifications du fournisseur et les observations de l'équipe sécurité technique. ➢ Les équipements qui ne cadrent pas dans les normes de sécurité du CHU de Québec sont automatiquement placés dans un réseau d'exceptions, derrière un coupe-feu. Un équipement qui n'a pas l'antivirus du CHU, qui n'est pas sur le domaine du CHU de Québec ou qui n'est pas entièrement et mensuellement mis à jour par les engins de mises à jour du CHU de Québec sera automatiquement placé dans un réseau d'exceptions, derrière un coupe-feu. ➢ Le fournisseur fourni la liste précise des ports de communication(UDP/TCP) pour permettre l'utilisation du système d'information. Les communications avec les systèmes déjà en place seront donc permises sous le principe du « privilège minimal requis ».	
ANTIVIRUS TREND MICRO	Serveur Poste	➢ Les logiciels *OfficeScan V 12.x et Deep Security* de *TrendMicro sont* utilisés pour sécuriser sans exception l'ensemble des postes et serveurs Microsoft de l'organisation selon l'entente ministérielle. ➢ Ce logiciel spécifique peut agir à titre de pare-feu ainsi que de service de réputation web. ➢ Le fournisseur fourni la liste précise d'exclusion pour ne pas affecter les performances du logiciel applicatif. ➢ Si le système ne peut s'y conformer, les postes et/ou serveurs sont isolés dans un VLAN dédié.	
SURVEILLANCE SÉCURITÉ / SIEM	Réseau	➢ L'orientation est de configurer le/ les applications pour qu'elles envoient les journaux de sécurité vers le SIEM du CHU de Québec en format *syslog*. Le fournisseur fourni un exemple de journal avant l'implantation et spécifier	

		les types d'évènements considérés anormaux afin de construire les alertes appropriées.	
SURVEILLANCE ZABBIX	Réseau Serveur	➢ Surveillance réseau en temps réel des périphériques (serveur, commutateur, pare-feu, etc.) et des applications et services afin de s'assurer du fonctionnement adéquat selon les barèmes établis par le fournisseur et le client; ➢ Le fournisseur s'assure que le système de surveillance sera en mesure d'interroger ses équipements par le protocole SNMP ou WMI.	
CLASSIFICATION DES DONNÉES	logique	➢ Les données sont classifiées selon leur niveau de **D**isponibilité, d'**I**ntégrité et de **C**onfidentialité et afin d'obtenir une cote **DIC**. **Voir l'annexe C pour la description détaillée de la classification des systèmes d'information.**	
SÉCURITÉ PHYSIQUE	Matériel	➢ **Normes ISO 27002:2013 : voir les exigences en annexe B au chapitre 11 concernant la sécurité physique et environnementale :** o Clause 11.1 : Zones sécurisées o Clause 11.2 : Matériels Les fournisseurs complètent les informations lorsqu'applicables en démontrant comment ils entendent rencontrer ces exigences. (Voir le détail en annexe B). ➢ Tout le matériel de serveurs réseau et de télécommunication est localisé dans les CTI sécurisés. ➢ Tout le matériel de télécommunication de distribution et d'accès est localisé dans des salles sécurisées.	
SÉCURITÉ LOGIQUE	logique	➢ **Normes ISO 27002:2013 : voir les exigences en annexe B au chapitre 9 concernant les contrôles d'accès :** o Clause 9.1 Exigences métiers en matière de contrôle d'accès o Clause 9.2 Gestion de l'accès utilisateur o Clause 9.3 Responsabilités des utilisateurs o Clause 9.4 Contrôle de l'accès au système et à l'information Les fournisseurs doivent compléter les informations lorsqu'applicables en démontrant comment ils entendent rencontrer ces exigences. (voir le détail en annexe B).	
EXPLOITATION DES ACTIFS INFORMATIONNELS	logique	➢ **Normes ISO 27002:2013 : voir les exigences en annexe B au chapitre 12 concernant la sécurité liée à l'exploitation :** o Clause 12.1 Procédures et responsabilités liées à l'exploitation	

		○ Clause 12.2 Protection contre les logiciels malveillants ○ Clause 12.3 Sauvegarde ○ Clause 12.4 Journalisation et surveillance ○ Clause 12.5 Maîtrise des logiciels en exploitation ○ Clause 12.6 Gestion des vulnérabilités techniques ○ Clause 12.7 Considérations sur l'audit des systèmes d'information Les fournisseurs doivent compléter les informations lorsqu'applicables en démontrant comment ils entendent rencontrer ces exigences. (voir le détail en annexe B).	
SÉCURITÉ DES APPLICATIONS	logique	➢ **<u>Normes ISO 27002:2013 : voir les exigences en annexe B au chapitre 14 concernant l'acquisition, le développement et la maintenance des SI :</u>** ○ Clause 14.1 Exigences de sécurités applicables aux SI ○ Clause 14.2 Sécurité des processus de développement et d'assistance technique ○ Clause 14.3. Données de test Les fournisseurs doivent compléter les informations lorsqu'applicables en démontrant comment ils entendent rencontrer ces exigences. (voir le détail en annexe B).	
SÉCURITÉ DES TÉLÉCOMMUNICA-TIONS	Logique	➢ **<u>Normes ISO 27002:2013 : voir les exigences en annexe B au chapitre 13 concernant la sécurité des communications:</u>** ○ Clause 13.1 Gestion de la sécurité des réseaux ○ Clause 13.2 2 Transfert de l'information Les fournisseurs doivent compléter les informations lorsqu'applicables en démontrant comment ils entendent rencontrer ces exigences. (voir le détail en annexe B).	
SÉCURITÉ ET CONTRÔLE D'ACCÈS WIFI (SANS FIL)	Logique	➢ Le type de sécurité minimum requis est WPA2-Entreprise en référence avec la norme IEEE 802.11i. ➢ Les méthodes d'authentification minimum acceptées sont : 802.1x (EAP-TLS, PEAP MSCHAPV2) en référence avec la norme 802.1x. ➢ La méthode de chiffrement minimum requis est : AES (CCMP) en référence à RFC 2759.	
CONNECTIVITÉ WIFI	Logique	➢ Les types de transmissions sans-fil minimum acceptés et supportés sont : 802.11n (2.4 Ghz MIMO), 802.11a (5 Ghz), 802.11n et 802.11ac (5 Ghz MIMO). ➢ L'itinérance supportée est le *Fast Roaming* référence avec la norme 802.11r.	

ENREGISTREMENT DES NOMS DNS – ACTIVE DIRECTORY	Logique	➢ Tous les équipements enregistrés dans le système de nom de domaine *Active Directory* doivent se conformer aux deux standards RFC suivants : RFC 2872 et 1178. ○ RFC 2872 : supporter le caractère de soulignement, dont celui utilisé au CHU de Québec – Université Laval : « domain_chuq.reg03.rtss.qc.ca ». ○ RFC 1178 : ne pas utiliser de caractère non alphanumérique et ne pas débuter par un caractère numérique. ○ RFC 2136, supporter le DDNS (enregistrement et mise à jour dynamique de l'entrée DNS)	
GESTION DES ACCÈS			
ACCÈS UTILISATEURS DISTANTS	Logique	➢ Les utilisateurs doivent respecter les règles d'accès établies par le CHU de Québec soit par : ○ VPN, Authentification OTP et Accès Citrix.	
ACCÈS À DISTANCE DES FOURNISSEURS	Logique	➢ Le soumissionnaire : ○ S'engage à utiliser le service d'accès distant fournisseurs du CHU de Québec Université Laval, pour le soutien à distance. Ce service est sans frais. Si requis : ○ S'engage à acquérir à ses frais un lien de télécommunication sur le RITM ainsi que l'accès au service F via jeton. ○ Dois contacter la DRI et demander l'ouverture de la guérite à chaque intervention. Les modalités d'accès au RITM (Service F) sont disponibles pour les fournisseurs du RSSS. La description de ces modalités est disponible à l'adresse suivante : http://www.ti.msss.gouv.qc.ca/Familles-de-services/Infrastructures/Service-F.aspx	
ACCÈS UTILISATEURS SANS FIL	Logique	➢ L'accès est permis aux utilisateurs du CHU de Québec par le réseau identifié au nom du « CHU ». L'identifiant utilisé est celui du domaine AD lorsqu'il a les droits d'accès. La norme minimale d'authentification est : WPA2 Entreprise.	
ACCÈS UTILISATEUR AD	Logique	➢ Le fournisseur privilégie l'infrastructure actuelle de métarépertoire *Active Directory Windows 2012 R2* et plus. Il supporte plus d'un domaine AD à partir du logiciel applicatif.	

ACCÈS AUX APPLICATIONS	Logique	➢ Le soumissionnaire doit privilégier le protocole LDAPS pour bénéficier du Métarépertoire Active directory 2012 R2 en place pour simplifier le processus d'authentification du code d'accès et du mot de passe. ➢ Dans l'impossibilité de supporter LDAPS, il doit informer la DRI.	
GESTION DES ACCÈS INTERNET UTILISATEUR	logique	➢ Tous les utilisateurs (AD) n'ont pas accès par défaut. ➢ L'accès lui est permis seulement lorsqu'il est autorisé par la DRI.	
TECHNOLOGIE BUREAUTIQUE			
ORDINATEUR DE TABLE	Matériel Logiciel	➢ Proposé par le soumissionnaire ou par la DRI. ➢ Actuellement HP ProDesk I5, I7, 16 Go de mémoire, 512 Go disque SSD. ➢ Création d'images 10, Edge Chromium, etc. ➢ Windows 10 **Entreprise** supporté. La version du système d'exploitation se limite aux versions actuelles encore supportées par son fabricant.	
ORDINATEUR PORTABLE	Matériel Logiciel	➢ Proposé par le soumissionnaire ou par la DRI. ➢ Actuellement HP ProBook 15 pouces et EliteBook 14 pouces, I5, I7, 16 Go de mémoire, 512 Go disque SSD. ➢ Résolution FHD, résolution minimale 1440 X 900 supportée. ➢ Actuellement, Création d'images Windows 10 Entreprise. ➢ Actuellement, Windows 10 Entreprise. La version du système d'exploitation se limite aux versions actuelles encore supportées par son fabricant.	
POSTE VIRTUALISÉ (BVI)	Logique	➢ Virtualisation de postes de travail : ➢ Actuellement, *XenDesktop/XenApp 7 1912 LTSR* ➢ Actuellement, *Windows 10 x64 Entreprise sur Windows 2019 x64.* La version du système d'exploitation se limite aux versions actuelles encore supportées par son fabricant.	
TABLETTE	Matériel Logiciel	➢ Proposé par le soumissionnaire ou par la DRI. ➢ Actuellement HP Elite X2 13 pouces avec clavier détachable, I7, I5, 8/16 Go de mémoire, 256/512 Go disque SSD.	

		➢ Résolution 3000 X 2000, résolution minimale supportée 1440 X 900. ➢ Création d'images Windows 10 Entreprise, Edge Chromium, etc. ➢ Windows 10 Entreprise supporté. La version du système d'exploitation se limite aux versions actuelles encore supportées par son fabricant.	
MONITEUR	Matériel	➢ 21,5 pouces et plus FHD ➢ Résolution minimale supportée 1440 X 900.	
IMPRIMANTE	Matériel	➢ Actuellement, des imprimantes Laser de marque HP standardisées dans le CHU de Québec.	
PROGICIEL			
PROGICIEL	Système d'exploitation Applicatif	➢ Actuellement, Système d'exploitation Windows 10 **Entreprise**. La version du système d'exploitation se limite aux versions actuelles encore supportées par son fabricant. ➢ Actuellement, Suite MS Office 2013 et 2016. ➢ Antivirus Trend Micro OfficeScan V 12.x. et Deep Security Maintenance mensuelle (application des mises à jour et des correctifs de Microsoft), supporter les dernières rustines; Si le système ne peut s'y conformer, les postes devront être isolés dans un VLAN dédié. ➢ Tous disponible en langue française. ➢ Pour tous les points énumérés pour les applicatifs, la version se limite à la version actuelle ou à la version majeure précédente encore supportée par son fabricant.	
SYSTÈME DE MESSAGERIE	Applicatif	➢ *Exchange online (Office 365).* ➢ Client lourd Outlook 2013/2016 et web. ➢ Le logiciel se limite à la version actuelle ou à la version majeure précédente encore supportée par son fabricant. ➢ Tous disponible en langue française.	
NAVIGATEUR/ FURETEUR	Applicatif	➢ Actuellement, Microsoft *Edge Chromium*, Google Chrome dernière version. ➢ Le logiciel se limite à la version actuelle ou à la version majeure précédente encore supportée par son fabricant. ➢ Disponible en langue française.	

APPLICATION WEB	logique	➢ Navigateur supporté : *Microsoft Edge Chromium*, Google Chrome dernière version. ➢ Protocole de sécurité TLS 1.2 et + ➢ Le logiciel se limite à la version actuelle ou à la version majeure précédente encore supportée par son fabricant. ➢ Disponible en langue française.	
APPLICATION CLIENT LOURD	logique	➢ Fournir la source d'installation et la procédure d'installation. ➢ Fournir la source d'installation en format de fichier MSI.	
APPLICATION VIRTUALISÉE	logique	➢ Actuellement, virtualisation d'application sous Microsoft App-V 5.x pour *Terminal Server.*	
DÉPLOIEMENT D'APPLICATION	logique	➢ *Script et/ou logon script, SCCM* et par GPO ➢ Fournir la source d'installation en format de fichier MSI. ➢ L'installation doit être automatisable, incluant la configuration	
GPO	logique	➢ L'AD applique les stratégies et politiques de groupe (GPO) au niveau des postes et utilisateurs.	
PÉRIPHÉRIQUE POSTE	logique	➢ *Des GPO* permettent la gestion des accès des ports USB par poste.	
RETRAIT DES DROITS ADMINISTRATIFS	logique	➢ Les utilisateurs n'ont pas de droits administratifs et leurs accès aux disques locaux sont restreints.	
PORTABLE (DONNÉES)	logique	➢ Chiffrement des disques des portables avec Bitlocker comme protection des données en cas de perte ou de vol d'équipement.	
GESTION DE L'ÉCRAN DE VEILLE	logique	➢ Actuellement, *Screenpass* permet à l'utilisateur de gérer les délais d'inutilisation pour l'activation de l'écran de veille.	
GESTION DE L'IMAGE DE FOND D'ÉCRAN	logique	➢ La gestion du fond d'écran des postes est faite par la direction des communications.	
GESTION DU MOT DE PASSE	logique	➢ *Gestion MDP (mot de passe)* permet de gérer les changements de mot de passe en libre-service à l'aide de questions personnalisées de l'utilisateur. ➢ Mot de passe complexe *:* Il doit être composé au minimum de 8 caractères, une minuscule, une majuscule et un chiffre.	
ENGAGEMENT DE CONFIDENTIALITÉ	logique	➢ L'utilisateur doit lire l'engagement de confidentialité et l'approuver par la signature automatisée lors de l'authentification.	

NORMALISATION DES IDENTIFIANTS	logique	➢ HEJ et HSS utilisent le numéro d'employé et CHUL, HDQ, HSFA et IUCPQ utilisent quelques lettres du prénom et du nom suivi de chiffre. ➢ Certains codes communs sont utilisés pour les postes à multiple utilisateur. ➢ L'identifiant National du MSSS sera utilisé dans un avenir rapproché. La norme est NNPP0001, qui correspond N=Nom de famille et P=Prénom.	
DONNÉES UTILISATEURS	logique	➢ Aucune donnée locale à l'exception des portables et tablettes (Mes documents, etc.). ➢ Toutes les données sont sur le lecteur réseau U : et P :. ➢ Protocoles SAMBA v2 et + supportés	

4. INTÉGRATION AUX SYSTÈMES DU CHU DE QUÉBEC

INTEROPÉRABILITÉ

La communication d'informations entre les applications installées au CHU de Québec est possible à l'aide d'un engin d'interface. Ces services d'interopérabilité s'occupent de la transmission (et de la conversion au besoin) entre les différents systèmes des différentes données médico-administratives, diagnostiques et cliniques.

Dans le cas où un système nécessite la mise en place d'un canal propriétaire entre deux systèmes et que les transmissions de ce canal ne passent pas par l'engin d'interface, la responsabilité du déploiement, du support et de la maintenance de ce canal revient aux fournisseurs concernés.

Le CHU de Québec demande de respecter minimalement la norme au format HL7 v2.X.

Le mode de transmission des messages à privilégier est la connexion directe par socket. Par contre il est possible d'utiliser d'autres modes de transmissions.

- Protocoles supportés : Client / Serveur MLLP, Dépôt / Récupération dans un répertoire, Dépôt / Récupération, FTP (SSL, SSH), Client / Serveur HTTP/HTTPS, Client / Serveur Web Service, Serveur DICOM, Client / Serveur, PeSIT, Client / Serveur AS2, Accès base de données avec la possibilité d'intégrer un flux de travail complet.

  La mise en place d'une couche SSL pour sécuriser les échanges HTTP (HTTPS) est exigée si les données échangées sont de nature sensibles. Si HTTPS doit être mis en place, le choix du nom de domaine et du certificat utilisés devra être discuté avec le CHU de Québec.

- Formats supportés : HL7 version 2.x, HL7 version 3.0, ASTM, HPRIM, XML, JSON, FHIR, Texte, CSV,Document (PDF, RTF, DOC, DOCX, etc.)

- L'échange de fichiers peut être utilisé selon les deux supports suivants :
  - FTP sécurisé (SSL ou SSH)
  - Partage de répertoire sécurisé par code utilisateur et mot de passe (Windows / SAMBA V2 et +), *anonymous* et *guest* n'est pas accepté.

Il est possible de transformer les différents messages pour gérer les diverses variantes de la norme HL7 ou se conformer aux adaptations propriétaires du fournisseur en considérant la disponibilité de l'information à la source.

5. LISTE DES SIGLES ET ACRONYMES

ADT – Admission, départ et transfère des patients du CHU de Québec.

CHU de Québec – Centre hospitalier universitaire de Québec affilié à l'Université Laval de Québec.

CHUL – Centre hospitalier de l'Université Laval

CRIM - Le centre de recherche appliquée en TI, qui développe et transfère des technologies émergentes et du savoir-faire de pointe, pour accélérer leur appropriation par les entreprises et organismes québécois.

DCI – Dossier Clinique Informatisé

DPE – Dossier Patient Électronique

HDQ – L'Hôtel-Dieu de Québec

HEJ – Hôpital de l'Enfant-Jésus

HSFA – Hôpital Saint-François d'Assise

HSS – Hôpital du Saint-Sacrement

IPM – Index Patient Maître

IUCPQ – Institut universitaire de cardiologie et de pneumologie de Québec

MSSS – Ministère de la Santé et des Services sociaux.

DST – Direction des services techniques

DRI – Direction des ressources informationnelles.

RITM - Réseau intégré de télécommunications multimédias. L'infrastructure de communication du réseau de la santé permet l'échange sécuritaire et confidentiel de données entre les différents établissements et professionnels.

RSAI-TI – Responsable de la sécurité des actifs informationnels et technologies de l'information.

CTI – Centre de Traitement Informatique (Centre de traitement de données).

ANNEXE A : INFRASTRUCTURE DE TÉLÉCOMMUNICATIONS AU CHU DE QUÉBEC

DÉFINITION

Certaines appellations sont utilisées à la direction des technologies de l'information du CHU de Québec-Université Laval et il devient important de bien les maîtriser pour une meilleure compréhension commune. Voici la liste:

- **Local de télécommunication d'accès**: ce type de local contient les équipements de télécommunications ainsi que le matériel nécessaire pour desservir les services informatiques et la téléphonie IP. C'est dans ce local que l'inter-connectivité se fait entre le câblage vertical et le câblage horizontal.

- **Local de télécommunication de distribution :** il contient les équipements nécessaires pour l'aiguillage secondaire de plusieurs locaux de télécommunication afin de répartir les charges de communications dans les différents niveaux de notre architecture. Ce type de local est nécessaire lorsqu'il y un besoin de plus de 1000 connexions réseau dans un bâtiment.

- **Le centre de traitement informatique (CTI ou salle satellite) :** Il contient les équipements serveur de l'établissement ainsi que les aiguilleurs principaux du cœur du réseau. Il y a plusieurs CTI dans le CHU de Québec. Dans certains cas ils sont dédiés qu'à des systèmes d'informations et dans d'autres, pour des locaux de télécommunication abritant les cœurs du réseau (aiguilleurs principaux).

- **Câblage horizontal** : câblage de télécommunication entre les locaux de télécommunication d'accès et les prises réseau des équipements informatiques des utilisateurs du CHU de Québec.

- **Câblage vertical** : câblage de fibre optique entre les locaux de télécommunication d'accès aux aiguilleurs de distribution jusqu'au cœur du réseau (aiguilleurs principaux) et les CTI;

Prendre note qu'un local de télécommunication dans certains cas peut avoir les deux rôles, soient : de distribution et d'accès. Dans tout nouveau bâtiment, il devra y avoir deux locaux de télécommunication de

distribution/accès dont un au niveau le plus bas (ex : sous-sol) et l'autre au niveau le plus haut (ex: au dernier étage). Sur les autres étages, il y aura des locaux de télécommunication d'accès.

RECOMMANDATION EN MATIÈRE DE TÉLÉCOMMUNICATION

Le secteur d'infrastructure des télécommunications de la direction des technologies de l'information décrit dans les prochains points, toutes les exigences à respecter en matière de télécommunication, afin d'uniformiser l'ensemble des installations dans ces locaux de télécommunication et dans les CTI. Et cela jusqu'aux exigences matérielles, de l'utilisateur final au sein du CHU de Québec (téléphonie et informatique).

LOCAL DE TÉLÉCOMMUNICATION

Les locaux de télécommunication sont primordiaux, pour offrir une connectivité aux équipements et permettre l'exploitation des services applicatifs et autres pour les utilisateurs. Les prochains points décrivent bien toutes les exigences à respecter pour la mise en place de nouveaux locaux et le réaménagement de ces derniers s'ils sont déjà existants.

LE CÂBLAGE STRUCTURÉ

Le câblage structuré est l'ensemble des techniques, méthodes et normes permettant de réaliser l'interconnexion physique entre les différents locaux d'un établissement comme celui du CHU de Québec qui compte plusieurs sites.

- Le câblage de cuivre est considéré comme solution horizontale qui se limite au niveau des étages.
- Le câblage de fibre optique adapté aux longues distances est considéré comme solution verticale qui relie les locaux de télécommunication d'accès aux locaux de télécommunication de distribution, et ce jusqu'aux CTI ou au cœur du réseau.

CÂBLAGE HORIZONTAL - CUIVRE

Les normes suivantes, pour le câblage de cuivre horizontal : TIA-568-C2 et TIA-606-B (identifications), comprennent un ensemble de standards sur le câblage à paires torsadées et sont utilisés dans les édifices publics. Elles se doivent, donc d'être bien considérées afin de déterminer le meilleur emplacement d'un nouveau local de télécommunication. Les paramètres à considérer sont les suivants:

- Le câblage cuivre de catégorie 6 minimum, composés de 4 paires avec enveloppe FT-4 ou FT-6 ne doit pas avoir plus de 90m de la source à la destination, du local de télécommunication d'accès jusqu'à la prise murale de l'utilisateur final.
- Le chemin de câble horizontal est à considérer dans le calcul des distances. Le plan de l'étage de l'immeuble aidera à mieux visualiser les possibilités d'acheminement du câblage et les distances à couvrir. Ce qui rendra l'emplacement du local de télécommunication plus optimal.
- La salle de télécommunication d'accès, localisée sur l'étage ne devra fournir que de la connectivité aux équipements du même étage. Aucune connexion entre les étages ou inter-bloc (aile ou secteur) n'est acceptée pour les mises en place futures.
- Grâce à ces éléments, le nombre de locaux de télécommunication d'accès nécessaires sera déterminé et localisé sur le plan de l'étage du site.

CÂBLAGE VERTICAL - FIBRE OPTIQUE

Les normes internationales ISO/CEI 11801 et 15018, comprenant un ensemble de standards sur le câblage de fibre optique à utiliser dans les immeubles publics doit être considérées pour en faire une bonne utilisation. Ces normes étant optimisées pour des longueurs s'étendant jusqu'à 3km ou moins.

- Le câblage fibre optique est utilisé entre les locaux de télécommunication d'accès, les locaux de télécommunication de distribution et les CTI. Il traverse régulièrement les étages de façon verticale pour rejoindre les locaux de télécommunication de distribution aiguilleur secondaire et les CTI.
- Ce type de câblage a peu d'incidence sur le choix du local de télécommunication d'accès dans la mesure où il couvre les distances requises.
- Plusieurs types de câblage fibre optique existent et suivant la longueur à couvrir, elle sera adéquatement sélectionnée;

RECOMMANDATION POUR LE LOCAL DE TÉLÉCOMMUNICATION

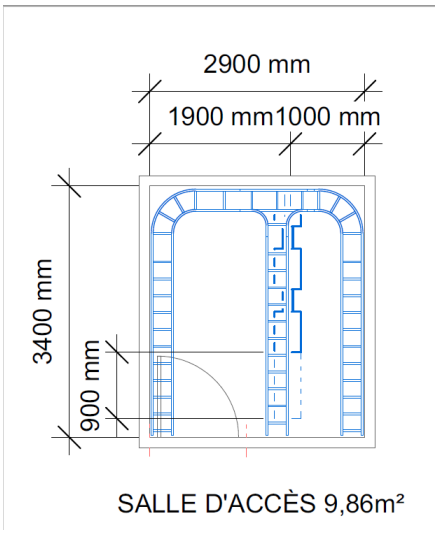
L'AMÉNAGEMENT DU LOCAL

A. Se doit d'être assez grand pour y travailler aisément autant à l'arrière qu'à l'avant des bâtis de métal. Ce qui correspond à un minimum de 9.86 mètres carrés pour les salles d'accès et 14.5 mètres carrés pour les salles de distributions.
B. La porte se doit d'ouvrir vers l'extérieur du local, afin d'exploiter le maximum d'espace intérieur. La porte peut ouvrir vers l'intérieur si l'aménagement, permet d'y travailler aisément autant à l'arrière qu'à l'avant des bâtis de métal.
C. La localisation de l'extincteur ne doit en aucun cas affecter une intervention humaine lors d'urgence ou de simples configurations.
D. Un minimum de deux bâtis de métal de 19''x90'' ou 19''X77''par local est requis. L'un d'entre eux sera pour l'aménagement des panneaux de raccordement et l'autre, pour les équipements de télécommunication informatique;
E. Veuillez noter que ce local doit fournir la connectivité à des prises téléphoniques traditionnelles pour certains sites. Les bâtis de métal ne seront pas utilisés pour ce type de connectivité.
F. Ces deux bâtis permettent la connexion d'environ 600 prises réseau pour des téléphones IP et des équipements informatiques;
G. Pour la téléphonie traditionnelle (analogique), des modules BIX doivent être installés sur le mur lorsqu'il y a un contreplaqué. Dans le cas contraire, un contreplaqué se doit d'y être installé. Les normes de câblage pour la téléphonie analogique sont établies par le département de la téléphonie;
H. Un chemin de câble grillagé de 12''x2'' positionné à horizontal, doit être inclus afin de supporter le câblage au-dessus des bâtis;
I. Le local doit posséder au minimum deux prises électriques d'urgence et deux prises électriques sur le réseau d'alimentation sans interruption (*UPS*) (ce nombre de prises peut être revu à la hausse suivant le nombre d'équipements (commutateurs et autres) à connecter; s'il n'existe pas de réseau d'alimentation sur l'*UPS*, des UPS mobiles seront à prévoir (selon le nombre d'équipements à connecter). Chaque prise doit fournir un voltage de 120 Volts et un courant de 20 ampères. Ainsi, pour une prise double il y aura un circuit de 20 Ampères par prise. À noter que cette configuration permettra l'alimentation de 4 commutateurs avec alimentation électrique Ethernet (*POE*) à pleine capacité;

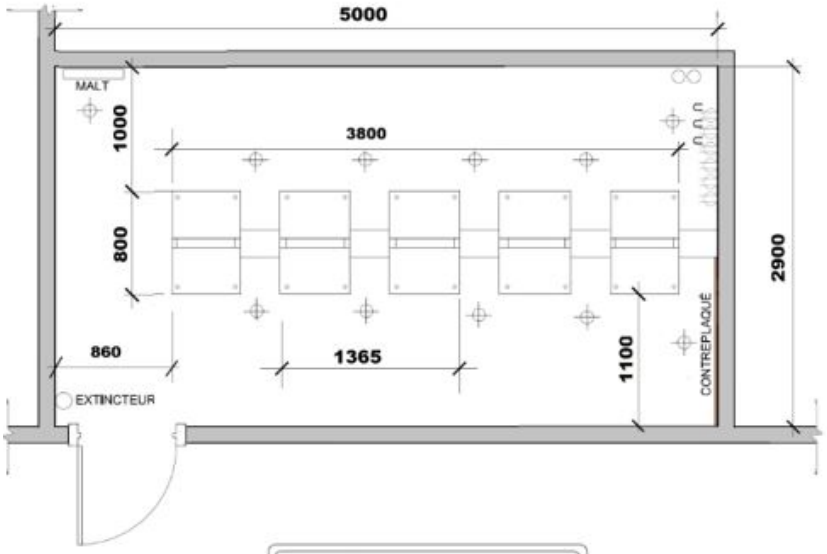
J. L'acheminement du câblage fibre optique entre les étages doit passer par un trou localisé dans un des coins du local;

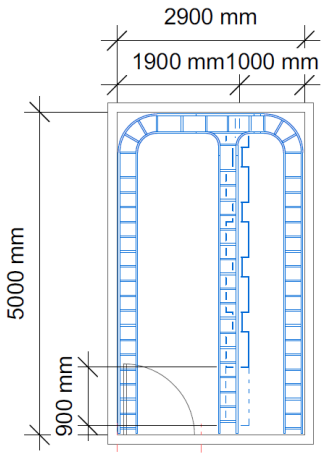
K. Un système d'évacuation de la chaleur doit être mis en place dans le local de télécommunication d'accès et de distribution.
   a. Par un système de ventilation adéquat;
   b. Par des grilles d'évacuation installées sur la porte du local;

PLAN D'AMÉNAGEMENT DU LOCAL D'ACCÈS (2 PLANS UTILISÉS)



PLAN D'AMÉNAGEMENT DU LOCAL DE DISTRIBUTION(2 PLANS UTILISÉS)





SALLE DE DISTRIBUTION 14,5m²

DISPOSITION DES ÉQUIPEMENTS DANS LE LOCAL

A. La disposition des bâtis de métal, des panneaux de raccordement, des modules de type BIX et des prises électriques sera effectuée par la DRI avec le chargé du projet de la DST. Ces informations seront incluses dans les plans et devis de la DST;
B. Les prises électriques seront localisées selon les besoins de la DRI;
C. Les équipements de télécommunications seront installés selon les besoins de la DRI;

D. Tous les locaux de télécommunication requièrent une barre de malt reliée à la terre et installée par les électriciens du chantier ou de la direction des services techniques;

E. La position finale des équipements devra être coordonnée et approuvée par une personne du département de l'infrastructure des télécommunications de la DRI;

F. Dans chaque local d'accès, un bâti 19 pouces est prévu pour les besoins du département Biomédical. Ce bâti doit recevoir leurs câbles cuivre les fibres et leurs équipements. En aucun cas il n'est permis pour eux d'utiliser les deux autres bâtis du département informatique sans l'approbation de la DRI.

G. Pour la DRI un bâti est utilisé pour le câblage et l'autre pour les équipements de communication informatique.

RECOMMANDATION AU NIVEAU DU MATÉRIEL ET DES ÉQUIPEMENTS

CÂBLAGE

LE CÂBLAGE HORIZONTAL

- Catégorie 6 (minimum) type, composés de 4 paires avec enveloppe FT-4 ou FT-6;

LE CÂBLAGE VERTICAL

Le câblage vertical se fera essentiellement avec de la fibre optique, et selon les distances à couvrir, le choix portera soit sur de la multimode ou de la monomode.

- Fibre multimode : 6, 12, 24 brins ou plus en gaine de PVC FT-4 ou FT-6 de 50/125µm OM3 ou OM4 selon la distance du chemin de câble;
- Fibre monomode : 6, 12,24 brins ou plus en gaine de PVC FT-4 ou FT-6 de 9/125µm;
- Quel que soit le modèle proposé, cette fibre devra être amurée;
- Le nombre de brins (6, 12, 24 ou plus) est déterminé par la DRI;
- Des patches de fibre 10G LC/LC de 3 mètres, seront à prévoir selon les besoins de longueur et de connectivité au panneau de raccordement de fibre optique;

CORDON DE RACCORDEMENT

- Des cordons de raccordement, catégorie 6 (minimum) type, composés de 4 paires avec enveloppe FT-4 ou FT-6. La longueur devra être prévue selon les besoins de l'installation;
- Des cordons de raccordement en fibre optique 50µm de type LC, LC selon les besoins pour le raccordement des commutateurs au panneau de raccordement de fibre optique. La longueur devra être prévue selon les besoins de l'installation;

GESTION DU CÂBLE

- Gestion de câble vertical NOIR de 12x77 ou 12X90 pouces, installé entre les deux bâtis;
- Gestion de câble ou grillage au-dessus des bâtis de métal dans le local de télécommunication de 12x2 pouces;

BÂTIS DE MÉTAL (RÂTELIER)

- Deux bâtis NOIRS, avec double filtrage, placés selon les besoins de la DRI. Les bâtis devront être fixés au plancher par la DST.

BOÎTIER FIBRE OPTIQUE ET PANNEAU DE RACCORDEMENT CUIVRE

- Pour le local de télécommunication d'accès, **un boîtier de 1U** (CCH-01U) ou 2U, de raccordement pour fibre optique avec un manchon coupleur de type LC, sera à prévoir;
- Pour le local de télécommunication de distribution, **un boîtier de 4U (**CCH-04U), de raccordement pour fibre optique avec un manchon coupleur de type LC sera à prévoir;
- Le panneau de raccordement de cuivre sera de type RJ45, de 48 ports cat6 (au minimum) et de 2U noir (au minimum).

PLAQUE MURALE POUR PRISE RÉSEAU

- Les plaques murales seront installées à 450 mm du plancher ou à une hauteur comptoir selon les besoins.
- Les plaques murales seront toutes identiques et conformes aux spécifications suivantes :
  - Elles seront installées pour une boîte de sortie électrique de 50 mm de largeur, 90 mm de hauteur et 90 mm de profondeur. Au besoin, le CHU de Québec peut demander l'installation dans un panneau de Placoplatre existant ou en surface avec la mise en place de cache-fils;
  - Elles seront 4 ports MDVO RJ45 catégorie 6 BLANC;
- Les prises murales pour les points d'accès sans-fil devront être de surface et fixées au mur et à l'intérieur du plafond. Elles doivent recevoir les modules MDVO RJ45.

ÉQUIPEMENT D'ALIMENTATION ÉLECTRIQUE DE RELÈVE

Tous les locaux utilisent l'alimentation sans interruption (*UPS*) lorsqu'elle est disponible sur le site, dans le cas contraire, elles doivent utiliser un équipement *UPS* dans le local, pour alimenter les équipements informatiques en cas de panne électrique. Les équipements suivants ou équivalents seront utilisés :

- 2 x *UPS* 1500 VA.

ÉQUIPEMENTS INFORMATIQUES

Les commutateurs d'accès empilables agissant comme un seul commutateur lorsqu'ils sont interconnectés entre eux et ses composantes sont nécessaires dans ce local. Le nombre de commutateurs et de modules est déterminé par la DRI selon les besoins et ils doivent respecter les exigences du devis technique l'appel d'offres en cours (disponible sur demande).

- Actuellement commutateur CISCO de 48 ports SFP+ (ex : WS-C2960XR-48FPD-L)
- Une alimentation de relève selon le modèle sera à prévoir par commutateur;
- Des modules SFP+ et X2 seront à prendre compte. Les modèles dépendront du type de fibre utilisé.

Pour les locaux de télécommunication de distribution :

Les commutateurs de distribution et ses composantes sont nécessaires. Le nombre de commutateurs et de modules est déterminé par la DRI selon les besoins et ils doivent respecter les exigences du devis technique l'appel d'offre en cours (disponible sur demande).

- Actuellement commutateur CISCO de 24 ou de 48 ports SFP+ (ex : WS-C3850-24XS-S)
- Une alimentation de relève selon le modèle sera à prévoir par commutateur;
- Des modules SFP+ et X2 seront à prendre compte. Les modèles dépendront du type de fibre utilisé.

Les points d'accès sans-fil et ses composantes sont les suivants :

- Actuellement, Cisco AIR-AP2802I-A-K9.
- Deux cordons de raccordement doivent en tout temps être fournis (la longueur des câbles dépendra des situations (7 ou 10 pieds).
- Des commutateurs réseau et des contrôleurs de points d'accès seront nécessaires pour les relier au réseau local du CHU. La redondance des équipements contrôleurs est nécessaire en cas de panne. Des licences de point d'accès seront nécessaires sur les contrôleurs.

Les listes qui suivent permettent d'établir clairement les besoins en matériel et en équipements à la direction des services techniques et au soumissionnaire pour les locaux de télécommunication informatique.

LISTE DU MATÉRIEL POUR UN LOCAL DE TÉLÉCOMMUNICATION D'ACCÈS

- 1 x boîtier fibre optique;
- Le choix du nombre et du modèle de réglette sera effectué avec la DRI.;

- Minimum de 2 x Bâtis de 19 pouces de largeur;
- 1 x gestion de câble verticale;
- 1 x gestion de câble horizontale au-dessus des bâtis de 12x2 pouces;
- X cordons de raccordement de catégorie 6 de 4 pieds (au minimum). La quantité sera déterminée par la DRI;
- Les vis permettant de fixer les équipements aux bâtis;
- x panneaux de raccordement de type RJ45 de 48 ports de modèle cat6 (au minimum); La quantité sera déterminée par la DRI;

- Pour certains locaux de télécommunication existants de certains sites, les prises MDVO seront de et de catégorie 6 (au minimum) afin de compléter le panneau de raccordement;

- Une barre de MALT (prise à la terre);

LISTE DES ÉQUIPEMENTS POUR UN LOCAL DE TÉLÉCOMMUNICATION D'ACCÈS

- x commutateurs empilables réseau de 48 ports;
- x modules *stacks*;
- x modules de fibre 10 Gbps;

  N.B. Les quantités seront déterminées par la DRI;
- X UPS 1500 VA; La quantité sera déterminée par la DRI;
- X PDU 15A; La quantité sera déterminée par la DRI;

LISTE DU MATÉRIEL POUR UN LOCAL DE TÉLÉCOMMUNICATION DE DISTRIBUTION

- Fibre optique de 6, 12, 24 brins ou plus en gaine de PVC FT-4 ou FT-6 de 50/125µm multi mode OM3 = 300 Mètres pour une vitesse de 10 Gbits par secondes, OM4 = 500 Mètres Pour une vitesse de 10 Gbits par seconde. Longueur de câble déterminée par la DRI et la DST;
- 1 x boîtier fibre optique;
- x réglettes 24 LC; La quantité sera déterminée par la DRI;
- Minimum de 2 x Bâtis de 19 pouces de largeur;
- 1 x gestion de câble verticale;
- 1 x gestion de câble horizontale au-dessus des bâtis de 12x2 pouces;
- X cordons de raccordement de fibre optique 50µm de type LC, LC (la longueur sera déterminée lors du projet);
- Les vis permettant de fixer les équipements aux bâtis;
- Une barre de MALT (prise à la terre);

LISTE DES ÉQUIPEMENTS POUR UN LOCAL DE TÉLÉCOMMUNICATION DE DISTRIBUTION

- x commutateurs réseau de 24 ou 48 ports de type SFP+;
- x modules de fibre, 10 Gpbs, SR ou LR;

  N.B. Les modèles et les quantités seront déterminés par la DRI;
- x UPS 1500 VA; La quantité sera déterminée par la DRI;
- X PDU 15A; La quantité sera déterminée par la DRI;

***** Tous les équipements de commutation, de routage et de fonctionnalités tierces (modules sans-fil par exemple) devront se conformer à l'appel d'offre en vigueur au niveau de la Direction des Ressources informationnelles et leur acquisition devra aussi se faire par l'intermédiaire de cette dernière (DRI).***

RECOMMANDATION D'INSTALLATION

CERTIFICATION

La certification des installateurs de câble est exigée pour toute installation de câble horizontal et vertical dans le CHU de Québec.

- Valider que les techniciens affectés à l'installation du câble cuivre, possèdent une certification valide de la compagnie choisie, pour l'installation et les essais de system IBDN cuivre;
- Valider que les techniciens affectés à l'installation de la fibre optique possèdent une certification valide de la compagnie choisie;

NORME À RESPECTER LORS D'INSTALLATION

- Le rapport de calibration des appareils d'essais doit être fourni avant le début des travaux.
- Le résultat des tests de câbles doit être fourni par le câbleur de façon électronique;
- Le câbleur doit fournir l'équipement de test afin de se conformer à la norme TIA-568-B;
- Le résultat du test de cuivre doit comprendre la perte en dB le *NEXT* cumulé *Return loss* et la longueur selon la norme applicable TIA-568-B;
- Tout résultat hors norme doit être rapporté au responsable de la télécommunication et sécurité de la DRI;
- Effectuer les tests d'atténuation de "bout en bout avec câble" sur les câbles de fibre optique à 850 nm et à 1300 nm;
- Les résultats des tests ne devront pas dépasser les spécifications du câble de fibre de + 0.5 dB de perte pour chaque joint de connecteur de fibre. Les résultats des tests OTDR seront exigés à la fin des travaux de façon électronique et consultable avant l'approbation des travaux;

- La mise à la terre de la fibre optique est obligatoire afin de nous conformer aux exigences concernant la garantie de 20 ans de la fibre installée.

RECOMMANDATION D'INSTALLATION DU SANS-FIL

- L'installation des points d'accès sans-fil WiFi doit être prévue dans tous les nouveaux projets.
- La disposition des points d'accès (antennes) doit permettre la géolocalisation de toute source WiFi pour localiser les équipements mobiles.
- Une étude de site préliminaire doit être préparée avec les plans d'architecture afin de s'assurer de la couverture du signal.
- La DRI exige qu'un rapport d'étude de site lui soit fourni avant de débuter les travaux.
- Ensuite, la DRI exige une étude de site de sortie afin d'ajuster et d'optimiser la couverture sans fil des points d'accès selon la structure et l'ameublement du bâtiment.
- Le fournisseur qui réalisera les études se doit d'être spécialisé en la matière.

INSTALLATION ET VÉRIFICATION

Il est important de respecter les exigences de la DRI pour l'installation du matériel dans les locaux de télécommunication. La DRI l'exige afin d'uniformiser l'ensemble des installations dans tous ces locaux dans tous ces sites. Il est également important de respecter la disposition des équipements dans le local.

INSTALLATION DANS LE LOCAL DE TÉLÉCOMMUNICATION D'ACCÈS ET DE DISTRIBUTION

- Installer et viser les bâtis de métal au sol (sur demande);
- Fournir et installer les conduits en plus d'installer une corde de tirage même dans les conduits vides;
- Mettre à la terre tout le réseau de conduits et d'étagères à câble;
- Installer et fixer les panneaux de raccordement de cuivre et des boîtiers de fibre optique dans le haut du bâti;
- Installer des supports à câble sur les panneaux de raccordement, lorsque requis;
- Installer le câblage horizontal (cuivre) entre les plaques murales et les panneaux de raccordement;
- Installer le câblage vertical (fibre optique) requis, aucun perçage n'est permis, seul le passage par les puits d'accès est permis;
- Raccorder tous les fils des câbles aux connecteurs MDVO sur les panneaux de raccordement et les plaques murales;
- Identifier toutes les connexions aux deux extrémités soit du côté du connecteur de la plaque murale et du côté du connecteur utilisé sur le panneau de raccordement.

- La mise à la terre de la fibre optique est obligatoire afin de nous conformer aux exigences concernant la garantie de 20 ans de la fibre installée.

INSTALLATION DU CÂBLAGE HORIZONTAL ET VERTICAL DANS LES BÂTIMENTS

Pour le passage des câbles dans les plafonds suspendus des corridors principaux, un chemin de câble doit être prévu dans les plans initiaux, pour supporter les câbles, afin d'éviter qu'ils soient suspendus aux structures existantes. Un tel support sera nécessaire aussi bien pour les câbles informatiques que téléphonique. L'utilisation de crochets suspendus à tout le 1,5 mètre doit aussi être prévue lors de l'installation. Ces chemins ne devront pas être utilisés pour le câblage électrique ou d'autre nature.

Prendre note que l'installation du câblage autre que dans les locaux de télécommunication est sous la responsabilité de la direction des services techniques et de leur norme et standard.

IDENTIFICATION

Il est important de respecter les exigences de la DRI sur l'identification des panneaux de raccordement dans les locaux de télécommunication et des prises murales dans les locaux des utilisateurs d'équipements informatiques / téléphonie IP. Veuillez utiliser un *Ptouch* pour créer les identifications selon les nomenclatures spécifiées ci-dessous et se référer à la norme TIA-606-B.

- Nomenclature utilisée pour l'identification des branchements du câblage informatique et de la téléphonie IP:
  - Identification sur la prise murale : **[BULDING ou AILE]-[LOCAL]. [RÂTELIER]-[POSITION DANS LE RÂTELIER (numéro du U dans le RÂTELIER)] : [PORT]**;
    - Ex.: **H-228B.RAT1-44 :47**
  - **Identifications sur le panneau de raccordement du local de télécommunication : [BLOC DE L'ÉTABLISSEMENT]-[LOCAL DE LA PRISE MURALE DE L'ÉQUIPEMENT DE L'USAGER];
    - Ex. : J-0027

  NB : *en cours de validation pour l'identification au niveau du patch-panel afin de faire référence à la prise dans le local de l'usager.*
- Nomenclature utilisée pour l'identification d'une prise réseau d'un point d'accès sans-fil :
  - La prise au plafond:[LOCAL DE TÉLÉCOMMUNICATION UTILISÉ]-[NUMÉRO DE CONNECTEUR UTILISÉ SUR LE PANNEAU DE RACCORDEMENT];
    - Ex.: J23-98

- Identification sur le panneau de raccordement du local de télécommunication : [BLOC DE L'ÉTABLISSEMENT]- [LOCAL DANS LEQUEL SE RETOUVE LA PRISE DU POINT D'ACCÈS];
  - Ex. : *J-0027

  Notez l'étoile pour signifier que la prise est située au plafond.

- Nomenclature utilisée pour l'Identification du point d'accès sans-fil lui-même :
  - Le point d'accès sans fil : W-[PAVILLION]-[BLOC DE L'ÉTABLISSEMENT]-[L'ÉTAGE]-[4 DERNIER CHIFFRES MAC ADRESSE DU POINT D'ACCÈS];
    - Ex. : W-CHUL-J-00-27C4

TEST ET VÉRIFICATION

La DRI désire recevoir les éléments suivants à la fin de l'installation afin de valider que tout soit conforme.

- Le résultat des tests de câbles horizontal doit être fourni de façon électronique;
- Le résultat des tests OTDR du câblage vertical doit être remis de façon électronique;
- Tout résultat hors norme doit être rapporté au responsable de la télécommunication et sécurité de la DRI;

ANNEXE B : NORMES ISO 27002 : 2013 APPLICABLES AU CHU DE QUÉBEC

Les normes ISO 27 002 : 2013 correspondant au paragraphe 7.3 Infrastructure et normes de sécurité sont :

- Sécurité logique : Chapitre 9 : Contrôles d'accès;
- Sécurité physique : Chapitre 11 Sécurité physique et environnementale;
- Exploitation des actifs informationnels : Chapitre 12 : Sécurité liée à l'exploitation;
- Sécurité des télécommunications : Chapitre 13: Sécurité des communications;
- Sécurité des applications : Chapitre 14 : Acquisition, développement et maintenance des SI.

CHAPITRE 9 D'ISO 27002:2013 : CONTRÔLES D'ACCÈS

Les mesures visent à limiter l'accès à l'information et aux moyens de traitement de l'information. Les objectifs sont de maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information. Rendre les utilisateurs responsables de la protection de leurs informations d'authentification et empêcher les accès non autorisés aux systèmes et aux applications. Tous les accès aux données sont contrôlés au niveau de l'identification, de l'authentification et de l'autorisation. La journalisation des accès de l'utilisateur devrait permettre de reconnaître l'identifiant, l'information accédée, la fonctionnalité utilisée, l'action entreprise et la date et l'heure de l'action posée.

9.1 Exigences métiers en matière de contrôle d'accès	9.1.1. Politique de contrôle d'accès
	9.1.2. Accès aux réseaux et aux services réseau
9.2 Gestion de l'accès utilisateur	9.2.1. Enregistrement et désinscription des utilisateurs
	9.2.2. Distribution des accès aux utilisateurs
	9.2.3. Gestion des droits d'accès et privilèges

	9.2.4. Gestion des informations secrètes d'authentification des utilisateurs
	9.2.5. Revue des droits d'accès utilisateurs
	9.2.6. Suppression ou adaptation des droits d'accès
9.3 Responsabilités des utilisateurs	9.3.1. Utilisation d'informations secrètes d'authentification
9.4 Contrôle de l'accès au système et à l'information	9.4.1. Restriction d'accès à l'information
	9.4.2. Sécuriser les procédures de connexion
	9.4.3. Système de gestion des mots de passe
	9.4.4. Utilisation des programmes utilitaires à privilèges
	9.4.5. Contrôle d'accès au code source des programmes

CHAPITRE 11 D'ISO 27002:2013 : SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

La sécurité physique doit être assurée en respect des normes ISO 27002 présentées ci-après. Les fournisseurs doivent compléter les informations lorsqu'applicables en démontrant comment ils entendent rencontrer ces exigences.

Les mesures visent à empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation et empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.

Deux objectifs sont à prendre en compte lorsque l'on parle de sécurité physique et environnementale : les zones sécurisées et la sécurité des équipements.

Les **zones sécurisées (11.1)** ont pour but de prévenir les accès physiques non autorisés, les dommages et les intrusions dans les bâtiments et informations de l'organisation. Elles hébergeront les équipements qui délivrent ou stockent des données sensibles ou critiques et seront renforcées par des périmètres de sécurité, barrières de sécurité et codes d'accès. Ici on cherche à protéger physiquement les équipements selon les risques identifiés.

L'objectif de contrôle relatif à la **sécurité des équipements (11.2)** cherche à prévenir les pertes, les dommages, les vols ou les compromissions d'actifs, et les interruptions des activités de l'organisation. La protection de l'équipement face aux menaces physiques et environnementales peut nécessiter des contrôles spéciaux (équipements de fourniture d'électricité…) et devra prendre en compte leur disposition et leur localisation pour être efficace.

11.1 Zones sécurisées	11.1.1. Périmètre de sécurité physique
	11.1.2. Contrôle d'accès physique
	11.1.3. Sécurisation des bureaux, des salles et des équipements
	11.1.4. Protection contre les menaces extérieures et environnementales
	11.1.5. Travail dans les zones sécurisées
	11.1.6. Zones de livraison et de chargement
11.2 Matériels	11.2.1. Emplacement et protection des matériels
	11.2.2. Services généraux
	11.2.3. Sécurité du câblage
	11.2.4. Maintenance des matériels
	11.2.5. Sortie des actifs
	11.2.6. Sécurité des matériels et des actifs hors des locaux
	11.2.7. Mise au rebut ou recyclage sécurisé(e) des matériels
	11.2.8. Matériels utilisateurs laissés sans surveillance
	11.2.9. Politique du bureau propre et de l'écran verrouillé

CHAPITRE 12 D'ISO 27002:2013 : SÉCURITÉ LIÉE À L'EXPLOITATION

Les mesures visent à assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information. S'assurer que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants. Se protéger de la perte de données. Empêcher toute exploitation des vulnérabilités techniques. Réduire au minimum l'impact des activités d'audit sur les systèmes en exploitation.

Cet article comporte 7 objectifs de contrôles de sécurité soit :

- Documenter les procédures d'exploitation et de les mettre à disposition de tous les utilisateurs concernés.
- Contrôler les changements apportés à l'organisation.
- Garantir les performances exigées du système.
- Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.
- S'assurer que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.
- Se protéger de la perte de données. Enregistrer les événements et générer des preuves.
- Garantir l'intégrité des systèmes en exploitation

12.1 Procédures et responsabilités liées à l'exploitation	12.1.1. Procédures d'exploitation documentées
	12.1.2. Gestion des changements
	12.1.3. Dimensionnement
	12.1.4. Séparation des équipements de développement, de test et d'exploitation
12.2 Protection contre les logiciels malveillants	12.2.1. Mesures contre les logiciels malveillants
12.3 Sauvegarde	12.3.1. Sauvegarde des informations
12.4 Journalisation et surveillance	12.4.1. Journalisation des événements
	12.4.2. Protection de l'information journalisée
	12.4.3. Journaux administrateur et opérateur
	12.4.4. Synchronisation des horloges

12.5 Maîtrise des logiciels en exploitation	12.5.1. Installation de logiciels sur des systèmes en exploitation
12.6 Gestion des vulnérabilités techniques	12.6.1. Gestion des vulnérabilités techniques
	12.6.2. Restrictions liées à l'installation de logiciels
12.7 Considérations sur l'audit des systèmes d'information	12.7.1. Mesures relatives à l'audit des systèmes d'information

CHAPITRE 13 D'ISO 27002:2013 : SÉCURITÉ DES COMMUNICATIONS

Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie. Maintenir la sécurité de l'information transférée au sein de l'organisme et vers une entité extérieure.

- L'application est certifiée auprès du MSSS avant de la déployer sur le réseau RITM.
- Le CHU de Québec respecte les exigences au raccordement au RITM.
- L'infrastructure réseau sécurisée en place intègre les accès, les protocoles de communication, les systèmes d'exploitation et les équipements.
- L'infrastructure est sous surveillance constante afin d'assurer sa disponibilité et son intégrité.

Les mises à jour se font selon les orientations et les besoins.

13.1 Gestion de la sécurité des réseaux	13.1.1. Contrôle des réseaux
	13.1.2. Sécurité des services de réseau
	13.1.3. Cloisonnement des réseaux
13.2 Transfert de l'information	13.2.1. Politiques et procédures de transfert de l'information
	13.2.2. Accords en matière de transfert d'information
	13.2.3. Messagerie électronique
	13.2.4. Engagements de confidentialité ou de non-divulgation

CHAPITRE 14 D'ISO 27002: 2013 : ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DES SI

Dans un premier temps, ISO 27002 définit un objectif de contrôle relatif aux exigences de sécurité pour les systèmes d'information pour assurer que la sécurité de l'information fait partie intégrante du système d'information.

Veiller à ce que la sécurité fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information. Garantir la protection des données utilisées pour les tests.

- Les logiciels et applications utilisés sont liés aux besoins d'affaire du CHU de Québec et sont acquis légalement selon les lois sur les droits d'auteur;
- Une documentation structurée du logiciel et de l'application informatique doit être fournie;
- Les applications doivent permettre la gestion de profils afin de limiter les accès aux besoins identifiés seulement;
- L'impression des données à partir des applications doit être limitée au niveau du profil utilisateur;
- L'application du libellé du DIC possible à intégrer dans le pied de page.

Le soumissionnaire de solutions logicielles et applicatives doit apporter dans les 18 mois suivant l'adjudication les ajustements nécessaires pour supporter les versions exigées par la DRI.

14.1 Exigences de sécurité applicables aux SI	14.1.1. Analyse et spécification des exigences de sécurité de l'information
	14.1.2. Sécurisation des services d'application sur les réseaux publics
	14.1.3. Protection des transactions liées aux services d'application
14.2 Sécurité des processus de développement et d'assistance technique	14.2.1. Politique de développement sécurisé
	14.2.2. Procédures de contrôle des changements de système
	14.2.3. Revue technique des applications après changement apporté à la plateforme d'exploitation
	14.2.4. Restrictions relatives aux changements apportés aux progiciels
	14.2.5. Principe d'ingénierie de la sécurité des systèmes
	14.2.6. Environnement de développement sécurisé
	14.2.7. Développement externalisé

	14.2.8. Test de la sécurité du système
	14.2.9. Test de conformité du système
14.3. Données de test	14.3.1. Protection des données de test

ANNEXE C : TABLEAUX DU DIC (DISPONIBILITÉ, INTÉGRITÉ ET CONFIDENTIALITÉ) ET NIVEAUX D'IMPACT

Niveaux d'impact	Préjudice	Descriptif	Disponibilité	Intégrité	confidentialité
1. Bas Impact non significatif	Incidences minimales limitées à un secteur administratif de l'organisme sans conséquence pour des tiers	Incidences d'ordre administratif circonscrites et traitées localement sans affecter l'organisme sur le plan global. La mission est réalisée et aucun impact sur l'image, la réputation, le plan médical, etc. Impact négligeable sur le plan financier. Travaux de recouvrement : s'échelonnant sur une période de 48h ou plus, si possible	La perturbation des accès ou de l'utilisation de l'actif informationnel a **un impact négligeable** pour l'organisme.	La modification non autorisée ou la destruction de l'actif informationnel a **un impact négligeable** sur l'organisme.	L'accès non autorisé ou la divulgation de l'actif informationnel a **un impact négligeable** sur l'organisme.
2. Moyen Impact limité ou modéré	Incidences notables, mais limitées à un secteur administratif de l'organisme bien que pouvant avoir des conséquences pour des tiers, au sein même de l'organisme.	Incidences notables, d'une durée limitée, sur le fonctionnement global ou les opérations d'un secteur de l'organisme. À ce niveau, les incidences de l'événement peuvent se résorber facilement et rapidement. Impact mineur sur le plan financier. Aucun dommage important à des tiers ne représente pas un manquement aux obligations médicales ou légales de l'organisme ni une atteinte à l'image ou à la réputation. Travaux de recouvrement : de 4h à 48h.	La perturbation des accès ou de l'utilisation de l'actif informationnel a **un impact modéré** pour l'organisme.	La modification non autorisée ou la destruction de l'actif informationnel a **un impact modéré** sur l'organisme.	L'accès non autorisé ou la divulgation de l'actif informationnel a **un impact modéré** sur l'organisme.

3. Élevé Impact grave	Incidences notables sur l'organisme ou sur des tiers mais ne menaçant pas la continuité des activités de l'organisme ou de ses services, mais pouvant avoir des conséquences toutefois très limitées sur la santé ou sur le bien-être des personnes.	L'événement aurait des incidences sérieuses et pourrait être la cause de dommages sérieux à des tiers ou nuire aux opérations critiques. Impact mineur sur le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée, mais sans porter atteinte à la santé ou au bien-être de ces personnes. Impact moyen sur l'image et la réputation. Impact sérieux sur les plans médical et/ou financier et peut constituer un manquement aux obligations médicales et/ou juridiques. Travaux de recouvrement : inférieur à 4h.	La perturbation des accès ou de l'utilisation de l'actif informationnel a un impact grave pour l'organisme.	La modification non autorisée ou la destruction de l'actif informationnel a un impact grave sur l'organisme.	L'accès non autorisé ou la divulgation de l'actif informationnel a un impact grave sur l'organisme.
4. Très élevé Impact extrêmement grave	Incidences très graves menaçant la continuité des activités de l'organisme. Conséquences très sérieuses pour la santé ou la sécurité de personnes physiques.	Incidences extrêmement sérieuses sur l'organisme ou sur des tiers. La santé ou la sécurité de personnes pourraient être mises en péril. Le fonctionnement et les opérations critiques de l'organisme ou d'autres organismes pourraient être paralysés ou compromis. Les conséquences sur le plan humain ou financier peuvent être désastreuses. Il peut également affecter le respect des droits fondamentaux des personnes à la protection des renseignements personnels qui les concernent et de leur vie privée et mettre en danger la vie, la santé ou le bien-être de ces personnes. Travaux de recouvrement : début des travaux immédiat, ce qui correspond à un taux de disponibilité de moins d'une minute.	La perturbation des accès ou de l'utilisation de l'actif informationnel a un impact très grave pour l'organisme.	La modification non autorisée ou la destruction de l'actif informationnel a un impact très grave sur l'organisme.	L'accès non autorisé ou la divulgation de l'actif informationnel a un impact très grave pour l'organisme.

Disponibilité

Niveau 1	Niveau 2	Niveau 3	Niveau 4
Il est acceptable qu'en cas de problèmes, le système d'information ne soit pas disponible pendant une période prolongée. Aucun impact sur les opérations de l'organisme. **La panne ou l'inaccessibilité de l'information est égale ou supérieure à 48 heures.**	En cas de problèmes, la période de non-disponibilité peut être élevée sans causer de problèmes significatifs aux opérations d'un organisme. Cependant, au-delà d'une certaine période d'indisponibilité, les opérations de l'organisme pourraient être perturbées sans toutefois nuire à sa mission. **La panne ou l'inaccessibilité de l'information est inférieure à 48 heures.**	En cas de problèmes, une courte période d'indisponibilité est permise au-delà de laquelle la mission de l'organisme pourrait être sérieusement affectée. Des mesures doivent être prises pour identifier et corriger les causes du délai. **La panne ou l'inaccessibilité de l'information sont inférieures à 4 heures.**	Le système doit continuellement être disponible. Un effort constant doit être consenti pour s'assurer d'une disponibilité maximale. **La panne ou l'inaccessibilité de l'information sont inférieures à 30 secondes (99.999% de disponibilité).** À la limite, le système ne peut être indisponible que pour quelques minutes seulement.
Exemples:			
Documents à usage interne • Notamment s'ils existent concurremment sous format papier : - Liste d'employés - Catalogues de centres documentaires - Formulaires, documents types • Notamment si leur disponibilité ou leur perte n'a pas de conséquences immédiates : - Statistiques d'utilisation d'un site Internet - Statistiques et données consolidées - Comptes rendus et contenus de présentations de séminaires internes	• Procédures internes, normes et autres documents de référence administrative • Document de travail interne (analyses, études, recherches, etc.) • Procédures opérationnelles, normes • Documents relatifs aux avantages sociaux du personnel • Documents de formation • Comptes à payer et à recevoir • Grand livre	• Dossiers de la clientèle • Ententes avec les fournisseurs de soins et de services • Système d'information et de bases de données qui servent directement la clientèle ex.SIIATH, SIURGIE.	• Documents requis pour la prestation de soins urgents • Systèmes de soins nécessitant une information continue • Documents relatifs aux mesures d'urgence et autres services essentiels • Système d'une infrastructure supportant des services essentiels • Plan de continuité ou de relève d'un service essentiel

Intégrité			
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**
La nature des informations pourrait être compromise sans que les répercussions ne dépassent les activités internes de l'administration.	La nature des informations pourrait être compromise sans que les répercussions ne dépassent les activités administratives ou d'affaires. Des mesures doivent être prises pour identifier les éventuelles pertes d'intégrité.	Des informations critiques pourraient être compromises. Il peut en découler des conséquences médicales et/ou juridiques graves. Des mesures doivent être prises pour identifier et corriger les causes de l'incident.	La nature des informations pouvant affecter la vie ou la santé d'individus est compromise. Il peut en découler des conséquences médicales et/ou juridiques graves. Un effort constant doit être consenti pour s'assurer de l'intégrité maximale de ces systèmes.
Exemples:			
• Informations de nature administrative sans conséquences médicales ou juridiques : - Organigrammes - Inventaires - Listes d'employés	• Documents d'information de gestion, tels que : - Volume et types de demandes de services de la clientèle - Informations médicales et/ou financières nécessaires à la planification - Documents relatifs aux horaires de travail	• Documents relatifs aux plans d'intervention • Systèmes ou documents supportant les services offerts à la population • Normes et procédures médicales et opérationnelles • Tout document ayant une valeur médicale, juridique et/ou financière	• Documents contenant des informations médicales pouvant mettre en péril la santé ou la sécurité des citoyens • Documents ou systèmes contenant des informations médicales : - Dossiers de la clientèle - Diagnostic - Prescriptions - Groupes sanguins • Résultats de tests ou d'examens • Documents contenant des résultats d'inspection ou d'étude sur la qualité des services pouvant mettre en danger la santé ou la sécurité de personnes • Documents ayant une valeur juridique et/ou financière très importante (documents authentiques et actes officiels)

1. Confidentialité

Niveau 1	Niveau 2	Niveau 3	Niveau 4
Les informations sont de nature publique. Aucune barrière à l'accès n'est requise.	Les informations ne sont pas assujetties à une obligation de confidentialité et/ou sont divulguées par l'organisme.	Les informations sont confidentielles en vertu d'un régime juridique. Une barrière à l'accès doit exister pour s'assurer que les accès sont contrôlés.	Les informations sont confidentielles en vertu d'un régime juridique et très sensible à une divulgation éventuelle. Une barrière à l'accès doit exister pour s'assurer que les accès sont contrôlés et journalisés et que les informations sont encryptées.
Exemples:			
• Documents publics (n'étant soumis à aucune restriction d'accès prévue par la loi) • Décisions rendues publiques par l'organisme dans l'exercice de ses fonctions • Renseignements personnels à caractère public (selon l'art. 57 de la Loi sur l'accès) • Documents contenant des données statistiques sur la clientèle	• Documents ayant peu d'incidences sur certaines décisions médicales ou administratives • Dans certaines circonstances, des documents contenant : - Un avis, une analyse - Une décision du Conseil d'administration, etc. - Détails des ententes avec d'autres organismes	• Documents contenant des renseignements personnels et médicaux • Documents contenant des renseignements personnels sur la clientèle et le personnel • Rapports préliminaires d'enquête sur la clientèle et/ou sur le personnel • Certaines communications, recommandations médicales ou administratives internes, telles que recommandations portant sur la Lssss, la Loi sur l'accès • Documents de stratégie de négociation de convention collective	• Documents contenant des renseignements personnels dont la divulgation causerait un tort irréparable à un individu (diagnostic du VIH, etc.) • Documents contenant des renseignements sur des enquêtes en cours, tels que : - Nom et coordonnées d'un informateur à la DPJ - Nom et coordonnées d'une personne bénéficiant d'un régime de protection

GLOSSAIRE INFORMATIQUE

802.11 – Ce standard a été amélioré à plusieurs reprises depuis son approbation par l'IEEEL. Ces améliorations sont définies comme étant des amendements au standard initial. Leur principale application commerciale est la technologie Wi-Fi.

802.11a, 802.11b, 802.11g, 802.11n et 802.11ac sont des techniques de transmission utilisées qui permettent la transmission de données par la liaison sans fil sur les bandes de fréquences 2.4Ghz et 5 Ghz de vitesse allant de 25 à 433 Mbit/s.

802.11r vise à améliorer la mobilité entre les cellules d'un réseau Wi-Fi et permettre à un appareil connecté de basculer plus vite d'un point d'accès à un autre.

802.11i ajoute des mécanismes d'identification et de chiffrement des données (WPA2).

820.1x est un standard lié à la sécurité des réseaux informatiques. Il permet de contrôler l'accès aux équipements d'infrastructures réseau.

AES – *Advanced Encryption Standard,* est un standard de chiffrement avancé approuvé par la NSA (*National Security Agency*).

APC – *American Power Conversion* est une société américaine d'équipements électriques de sûreté appartenant au groupe *Scheider Electric*.

AWG – *American Wired gauge,* est une unité de mesure utilisée permettant de mesurer le diamètre d'un câble électrique. Plus la valeur est élevée, plus le diamètre indiqué est petit.

Belden – *Belden* conçoit, fabrique et vend un portefeuille complet de produits de câble, de connectivité et de réseau pour la transmission de signaux pour des applications de données, audio et vidéo.

BIX – *Building Industry Cross-Connect* fait partie d'un système de téléphonie d'interconnexion (réseau de distribution intégré au bâtiment – IBDN) créer dans les années 1970 par Nortel Networks. Il se compose de différentes tailles de blocs et accessoires de distribution par câble.

CAT6+ - (catégorie 6) Catégorie selon les normes et les standards. Elle est une gradation des performances des éléments utilisés pour les liaisons de type Ethernet. Il permet de transmettre des données à des fréquences jusqu'à 250Mhz et à des débits de 1 Gbit/s sur une longueur de plus de 100 mètres.

CCMP – *Counter-Model/CBC-Mac Protocol* est une méthode de chiffrement définie dans le standard IEEE 802.11i. Il gère l'intégrité des messages.

Cisco – *Cisco Systems* est une entreprise américaine dans le domaine du matériel informatique et de télécommunications.

Citrix – est une entreprise multinationale américaine qui propose des produits de collaboration, de virtualisation et de mise en réseau pour faciliter le travail mobile et l'adoption des services cloud.

Cluster – Un *cluster* est une grappe de serveurs constituée de deux serveurs au minimum (appelés aussi noeud) et partageant une baie de disque commune.

CPU – *Central Processing Unit*, le processeur, unité centrale de traitement est le composant de l'ordinateur qui exécute les programmes informatiques.

Cristal-Net – est un portail d'outils cliniques multi-site qui intègre toute l'information au sujet d'un patient provenant des systèmes sources du CHU de Québec.

dB – Le décibel est une unité de grandeur sans dimension définie comme 10 fois le logarithme décimal du rapport entre deux puissances. Il est couramment utilisé dans le domaine des télécommunications pour mesurer le traitement du signal afin de se concentrer sur les problèmes du moment présent.

DHCP – *Dynamic Host Communication Protocol,* est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station en lui assignant une adresse IP, un masque de sous-réseau, etc..

DNS – *Domaine Name System,* est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

EAP-TLS – *Extensible Authentication Protoco,* est un mécanisme d'identification universel, fréquemment utilisé dans les réseaux sans fil (Wi-Fi) et les liaisons point à point. Et TLS – *Transport Layer Security,* est un protocole de sécurisation des échanges sur internet. Il utilise une infrastructure à clés publiques pour sécuriser les communications d'identification entre les clients et le serveur Radius.

Ethernet – est un protocole de réseau local à commutation de paquets.

Fortinet – est une entreprise américaine qui construit du matériel de télécommunication. Elle est spécialisée dans les solutions de sécurité pour les réseaux et les ordinateurs.

FT4 – *Vertical Flame Test* (test de flamme) la certification de niveau 4 signifie que le câble résiste au feu et aux flammes.

FT6 – *Horizontal Flame & Smoke Test* (test de flamme) –est un câble résiste au feu et aux flammes dans un plénum d'air.

FTP – *File transfert protocol,* protocole de transfert de fichiers entre deux systèmes.

Gbps – *Giga Bits* par seconde, unité de mesure d'un débit de données.

Go – *Giga octet*, unité de mesure basée sur 8 bits pour déterminer une capacité en informatique.

GPO – *Group policy Object,* les stratégies de groupe sont des fonctions de gestion centralisée de la famille Microsoft Windows.

HL7 – *Health Level*, ce standard se réfère à un ensemble de normes internationales pour le transfert de données cliniques et administratives entre les applications logicielles utilisées par divers fournisseurs de soins de santé.

HP – *Hewlett Packard* est une société multinationale dans le domaine du matériel informatique, du logiciel et des services informatiques.

I7 et I5 – Intel *Core* I7 ou I5 d'Intel est utilisé pour ses microprocesseurs haut de gamme depuis novembre 2008.

IBDN – *Integrated Building Distribution Network* est un standard de câblage basé sur l'ingénierie.

IBM – *International Business Machines* est une société multinationale dans le domaine du matériel informatique, du logiciel et des services informatiques.

IEEE 802.11 – est un ensemble de normes concernant les réseaux sans fil locaux (WIFI) qui ont été mis au point par le groupe de travail du comité de normalisation LAN/MAN de l'IEEE *(Institute of Electrical and Electronics Engineers)*

IIS – *Internet Information service*, ce service d'information internet agit comme un serveur WEB permettant ainsi son exploitation par navigateur.

INTEL – *Intel Corporation* est une entreprise américaine cofondée en 1968. Il est le premier fabricant mondial de semi-conducteurs. Cette entreprise fabrique des microprocesseurs.

IPS – *Intrusion Prevention System,* système de prévention d'intrusion est un outil en sécurité des systèmes d'information permettant de prendre des mesures afin de diminuer les impacts d'une attaque.

ISO – Organisation internationale de normalisation.

LC – le connecteur optique LC est un dispositif normalisé permettant de raccorder divers équipements utilisant la fibre optique.

LDAPS **–** *Lightweight Directory Access Protocol* SSL est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP et SSL.

Leviton – La société *Leviton* est le plus grand fabricant de dispositifs de câblage électrique et de solutions de connectivité pour les centres de données informatiques.

Mbps – *Mega Bits* par seconde, unité de mesure d'un débit de données.

MDVO – *Mobile Dynamic Virtual Organizations, est un connecteur mobile basé sur une technologie brevetée.*

Microsoft – *Microsoft* est une société multinationale américaine dans le domaine du développement et la vente des systèmes d'exploitation et de logiciels.

MSCHAPV2 – est la version de Microsoft du protocole CHAP (*Challenge-Handshake Authentification Protocol*)

Ms SQL – *Microsoft* SQL serveur est un système de gestion de bases de données relationnelles (SGBDR) développé par la société Microsoft.

Multicast – est une forme de diffusion d'un émetteur (source unique), vers un groupe de récepteurs. Les termes « diffusion multipoint ou diffusion de groupe » sont également employés.

NLB – la répartition de charge réseau est un ensemble de techniques de distribuer une charge de travail entre différents ordinateurs d'un groupe.

OM3 – Catégorie de fibre optique selon les normes et les standards. Cette catégorie de câble fibre optique multi-mode permet des débits de transmission de l'ordre de 10 Gbits/s sur 300 mètres et de 1 Gbits/s sur 1 kilomètre.

OM4 – Catégorie de fibre optique selon les normes et les standards. Cette catégorie de câble fibre optique multi-mode permet des débits de transmission de l'ordre de 10 Gbits/s sur 500 mètres et de 1 Gbits/s sur 1 kilomètre.

Oracle Database – est un système de gestion de bases de données relationnelles (SGBDR).

OTDR – O*ptical Time Domain Reflectometer.* Cette abréviation désigne un appareil de mesure pour fibres optiques, utilisant le principe de la réflectométrie. Cet appareil sert notamment dans le domaine des télécommunications, afin de caractériser un réseau fibré.

OTP – *One-time password*, solution **d'authentification** utilisant des mots de passe à usage unique.

PDF – *Portable Document Format,* la spécificité du document PDF est de préserver la mise en forme d'un fichier (polices d'écritures, images, objets graphiques, etc.) tel qu'elle a été définie par son auteur, et cela quels que soient le logiciel, le système d'exploitation et l'ordinateur utilisés pour l'imprimer ou le visualiser.

PDU – *Power distribution unit* (barre de distribution électrique) cet équipement consiste à rendre l'énergie électrique disponible, fiable et sécuritaire aux équipements informatiques.

PEAP – *Protected Extensible Authentication Protocol, Protected EAP,* est une méthode de transfert sécurisée d'informations d'authentification pour le réseau sans fil. Cette procédure sert à authentifier un client sur le réseau.

POE – *Power over Ethernet*, qui permet d'alimenter électriquement un appareil via le câblage réseau.

P-TLS *Extensible Authentication Protocol,* le protocole EAP est utilisé pour l'authentification.

PVC – Polychlorure de vinyle, un polymère thermoplastique utilisé pour envelopper les paires de câbles pour en résulter en un seul câble et offrir une protection sécuritaire contre le feu. Il est couramment utilisé dans les télécommunications.

RAID – *Redundant Array of Independent,* désigne les techniques permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit la tolérance aux pannes, soit la sécurité, soit les performances de l'ensemble, ou une répartition de tout cela. Les niveaux mentionnés sont: 1 pour disques en miroir et 5 pour volume agrégé par bande à parité répartie.

RJ45 – *Registered Jack*, prise jack enregistrée est un connecteur 8P8C (8 positions et 8 contacts électriques) qui est couramment utilisé comme interface physique pour terminer le câble de type paire torsadée. Il est surtout utilisé pour les connexions Ethernet entre autres.

SAMBA – est un logiciel d'interopérabilité qui permet à des ordinateurs Windows d'accéder aux fichiers des ordinateurs Unix et Linux.

SAN – *Storage Area Network,* le réseau de stockage est un réseau spécialisé permettant de mettre en commun des ressources de stockage.

SFP – *Small form-Factor Pluggable*, contient un circuit imprimé qui s'enfiche dans le connecteur électrique d'une fente SFP d'un système hôte.

SIEM – *Security information and event management,* il permet de gérer et corréler les logs. On parle de corrélation, car ces solutions sont munies de moteurs de corrélation qui permettent de relier plusieurs évènements à une même cause.

SNMP – *Simple Network Management Protocol,* est un protocole simple de gestion de réseau qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseau et matériels à distance.

Solaris – *Solaris* est le nom du système d'exploitation multitâche et multiutilisateur de *Sun Microsystems* utilisé sur le matériel informatique.

Sonde IPS – *Intrusion Detection System,* est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (réseau ou hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

SSD – *Solid Stade Drive,* aussi appelé disque électronique, est un matériel informatique permettant le stockage de données sur de la mémoire flash.

SSH – *Secure Shell,* est un programme informatique et aussi un protocole de communication sécurisé.

SSL – *Secure socket layer,* protocole de sécurisation d'échange de données sur Internet.

Sun (Oracle) – *Standford University Network* est un constructeur de matériel informatique et éditeur de logiciels américain. Cette entreprise appartient à Oracle depuis 2010.

Syslog – est un protocole définissant un service de journaux d'événements d'un système ou périphérique informatique.

TCP – *Transmission Control Protocol,* est le protocole de contrôle de transmission fiable en mode connecté. TCP est situé au-dessus d'IP et il correspond à la couche de transport.

TCP/IP – *Transmission Control Protocol et Internet Protocol, e*st l'ensemble des protocoles utilisés pour le transfert des données sur Internet.

Trend Micro – est une société japonaise qui développe des logiciels de sécurité informatique (antivirus).

U - (pour unité) est une unité de mesure employée pour décrire la hauteur d'un serveur ou équipement informatique afin de le localiser dans un cabinet de métal dans une salle informatique. 1U correspond à 1 ¾ pouce ou 44.45 millimètres.

UDP – *User Datagram Protocol,* protocole de datagramme utilisateur est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche de transport de la pile de protocoles TCP/IP.

µm - (symbole pour le micromètre), est une unité de longueur de système international d'unités. Il un un sous-multiple du mètre, qui vaut 0,000 001 mètre ou 0,001 millimètre.

UPS – *Uninterruptible Power Supply* (**alimentation sans interruption)** est un dispositif électronique de puissance qui permet de fournir à un système électrique ou électronique une alimentation électrique stable et dépourvue de coupure ou de microcoupure.

URL – *Uniform Resource Locator,* (Localisateur uniforme de ressource), désigne une chaîne de caractères utilisée pour adresser les ressources du Web *(World Wide Web).*

USB – *Universal Serial Bus*, Bus universel en série, est une norme relative à un bus informatique en transmission série qui sert à connecter des périphériques informatiques à un ordinateur.

UTM – *Unified threat management,* gestion unifiée des menaces informatiques, un terme utilisé pour décrire des pare-feu réseaux qui possèdent de nombreuses fonctionnalités supplémentaires qui ne sont pas disponibles dans les pare-feu traditionnels.

UTP – *Unshielded Twisted Pair* (paire torsadée non blindée) Une **paire torsadée** est une ligne de transmission formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre. Cette configuration a pour but de maintenir précisément la distance entre les fils et de diminuer l'interférence du signal entre eux.

VLAN – *Virtual Lan,* Un réseau local virtuel, communément appelé VLAN est un réseau informatique logique indépendant. De nombreux Vlan peuvent coexister sur un même commutateur réseau.

VmWare – est une société informatique américaine fondée en 1998, filiale d'EMC corporation depuis 2004, qui propose plusieurs produits propriétaires liés à la virtualisation d'architectures x86.

VPN – *Virtual Private Network,* réseau privé virtuel est une connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel.

WEB – *World Wide Web (WWW)* ou communément appelé le WEB, et parfois la toile est un système hypertexte public fonctionnant sur internet. Il est aussi exploité en mode privé fonctionnant seulement en établissement. Le web est consultable par l'entremise d'un navigateur.

Wi-Fi – *Wireless Fidelity,* réseau local sans fil, Le Wi-Fi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11. Un réseau Wi-Fi permet de relier sans fil plusieurs appareils informatiques au sein d'un réseau informatique afin de permettre la transmission de données entre eux.

Windows – *Windows* est le nom du système d'exploitation multitâche et multiutilisateur de Microsoft utilisé sur le matériel informatique.

Windows Active Directory ou AD– Il permet la mise en œuvre des services d'annuaire pour les systèmes d'exploitation Windows. Il fournit des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il est communément appelé Domaine AD.

VBScript – *Microsoft Visual Basic Scripting Edition* est un sous-ensemble de Visual Basic utilisé en tant que langage de script d'usage général.

VMI – *Windows Management Instrumentation* est un système de gestion interne de Windows qui prend en charge la surveillance et le contrôle de ressource système via un ensemble d'interfaces.

VMware – *Vmware* est une société informatique américaine qui propose plusieurs produits liés à la virtualisation d'architectures x86.

WPA2-Entreprise – comprends tous les éléments obligatoires de la norme 802.11i. La norme WPA2 impose de prendre en charge le mécanisme CCMP, lequel s'appuie sur AES. WPA est conçu pour les réseaux d'entreprise et demande à ce que l'on installe un serveur d'authentification RADIUS.

XenApp – est un logiciel de la société *Citrix systems* permettant d'accéder à distance à des applications à partir de clients légers. Il s'agit d'un logiciel serveur permettant de distribuer des applications ou des services sur un réseau et d'y accéder.

XenDesktop – est un logiciel de la société *Citrix systems* permettant d'accéder à distance à un bureau virtuel de Windows à partir différents périphériques le permettant.