

Sécurité de l'information



MANUEL D'UTILISATION DE L'ANNEXE CCTP SECURITE DES SYSTEMES D'INFORMATION

Sommaire

1. Identification du document	3
2. Objet du document	5
3. Domaine d'applicabilité.....	5
4. Politique de sécurité.....	5
5. Périmètres et exigences.....	6
5.1. Périmètres d'application	6
5.2. Niveau d'exigences selon le périmètre	7
5.3. Adaptation de la présente annexe	7
5.4. Adaptations minimales avant envoi aux candidats.....	8
5.5. Autres pièces utiles pour les candidats.....	8
6. Notes sur les domaines d'exigences de la « Grille d'évaluation CCTP SSI ».....	9
6.1. Gestion des identités et de l'authentification.....	9
6.2. Journaux et traçabilité.....	9
6.3. Protection des données sensibles.....	9
6.4. Services hébergés hors SI du CHU (SaaS)	9
6.5. Services hébergés au sein du SI du CHU et administrés en autonomie par le soumissionnaire	9
7. Glossaire des termes employés.....	10

1. Identification du document

Identification	
Pôle	Sujet
Ressources Financières et Transformation Numérique	Manuel d'utilisation de l'annexe CCTP SSI

Classification de l'information			
Public	Restreint	Confidentiel	Secret

Droits	
Modification	RSSI
Lecture	CHU, GHT

Versions				
Versions	Date d'approbation	Rédacteur	Approbateur	Intervention
1.0	01/03/2018	Thierry Veauvy, Laurent Colonges	Olivier PONTIES (DSI)	Document initial : référentiel de l'APHM Auteur : Philippe Tourron - RSSI (18/01/2017)
1.1	11/08/2020	Thierry Veauvy, Laurent Colonges	Nicolas DELAPORTE (DSI)	Adaptation aux besoins CHU Toulouse Auteurs : Thierry Veauvy, Laurent Colonges
1.2	09/10/2021	Thierry Veauvy, Laurent Colonges	Nicolas DELAPORTE (DSI)	Modifications diverses
2	08/12/2021	Thierry Veauvy, Laurent Colonges	Nicolas DELAPORTE (DSI)	Modification de la colonne SaaS
3	14/03/2023	Laurent COLONGES (RSSI)	Nicolas DELAPORTE (DSI)	Remplacement DSIO par DSN, modification cartouches, élargissement au GHT

Mode de licence du document

Ce document est sous licence Creative Commons BY-NC-SA, c'est-à-dire que vous pouvez reproduire cette création, la diffuser ou encore la modifier sous les conditions suivantes :

- Paternité : vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le soumissionnaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre)
- Pas d'utilisation commerciale : vous n'avez pas le droit d'utiliser cette création à des fins commerciales
- Partage des conditions initiales à l'identique : si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.



[Licence Creative Commons BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/)

2. Objet du document

Les solutions informatiques déployées au sein du Système d'Information du CHU Toulouse doivent satisfaire les exigences de sécurité informatique définies dans la Politique de Sécurité des Systèmes d'Information du CHU Toulouse et du GHT HGTO.

Il convient donc de communiquer et contractualiser les engagements des fournisseurs du CHU Toulouse et du GHT HGTO nécessaires en termes de sécurité des systèmes d'information.

Ce document énonce les obligations (pré requis) et recommandations SSI auxquelles sont soumis les fournisseurs du CHU Toulouse et du GHT HGTO. Il a vocation à être intégré dans appels d'offres de marchés publics en tant que Cahier des Clauses Techniques Particulières et également lors de l'analyse SSI dans le cadre du processus d'homologation Projet.

3. Domaine d'applicabilité

La présente politique est applicable sur le SI du CHU Toulouse, du GHT Haute Garonne Tarn Ouest (GHT HGTO) et ses établissements membres : CH Comminges-Pyrénées, CH Lavaur, CH Muret et CH Marchant.

4. Politique de sécurité

La Politique de Sécurité des Systèmes d'Information du CHU Toulouse et du GHT Haute Garonne Tarn Ouest (PSSI GHT HGTO) est applicable.

Les Politiques Techniques de Sécurité sont applicables.

5. Périmètres et exigences

5.1. Périmètres d'application

Le SI du CHU Toulouse et du GHT HGTO est segmenté en niveaux d'exigences différents :

- Le niveau 27001 recouvre les services applicatifs visant à la certification ISO 27001 avec des exigences élevées.
- Le niveau CHU/GHT comprend tous les autres équipements et services hors 27001.

Afin de pouvoir compléter correctement l'annexe CCTP SSI, il sera indiqué dans quel périmètre devra se situer l'application objet du marché, en utilisant le filtre du tableur prévu à cet effet.

5.2. Niveau d'exigences selon le périmètre

Les **exigences de sécurité prérequis** : Leur non-respect est éliminatoire et elles sont notées **P comme Prérequis** dans le document « Grille d'évaluation CCTP SSI ».

Les **exigences de sécurité évaluées** : Ce sont des orientations techniques fortement souhaitées en matière de sécurité pour apporter une cohérence avec les bonnes pratiques et recommandations du secteur santé. Elles sont décrites au soumissionnaire dans le document « Grille d'évaluation CCTP SSI » et sont à prendre en compte dans le cadre de sa réponse, elles sont notées **E comme Evalué** et le niveau de réponse à ces recommandations sera pris en compte dans l'évaluation technique de l'offre.

Le soumissionnaire précisera si sa solution prend en compte ces recommandations. Dans la négative, les solutions palliatives qu'il propose ou le plan produit intégrant ces recommandations seront présentées.

5.3. Adaptation de la présente annexe

Les chefs de projet ou responsables applicatifs en charge de l'appel d'offre peuvent s'appuyer sur une « Grille d'évaluation CCTP SSI » adaptée selon les spécificités du projet :

- Il est possible de modifier les niveaux d'exigence de Evalué à Prérequis
- Il est possible de modifier les poids respectifs de chaque exigence.

Il n'est pas possible de dégrader le niveau d'exigence de Prérequis à Evalué.

5.4. Adaptations minimales avant envoi aux candidats

Le document [Annexe CCTP SSI.xlsx](#) peut être modifié afin de simplifier sa saisie par le candidat.

Afin de limiter les échanges de questions avec les candidats, il convient de retirer les lignes inutiles en fonction du projet :

- **Type d'hébergement :**
 - S'il s'agit d'une application SaaS, retirer toutes les lignes avec « DC CHU / PaaS » dans la colonne D
 - S'il ne s'agit pas d'une application SaaS, retirer les lignes avec « Services hébergés hors SI du CHU (SaaS) » dans la colonne A
- **Niveau de sécurité attendu (application 27001 ou application standard CHU) :**
 - Selon le périmètre cible de l'application, retirer la colonne B ou C afin de clarifier les attendus du document
- **Équipement de type « boîte noire » :**
 - S'il ne s'agit pas d'une application ou d'un système totalement fermé (certains équipements GBM par exemple), retirer les lignes avec « Services hébergés au sein du SI du CHU et administrés en autonomie par le titulaire » dans la colonne A
- **Objets connectés :**
 - Si aucun objet connecté n'est utilisé, retirer les lignes avec « Objets connectés (IoT) »

5.5. Autres pièces utiles pour les candidats

Annexes de sécurité infrastructure :

<https://sharepoint.chu-toulouse.fr/sites/DSIO/Documents%20partages/Forms/AllItems.aspx?RootFolder=%2Fsites%2FDSIO%2FDocuments%20partages%2FDocuments%20de%20r%C3%A9f%C3%A9rence%20Achat%2C%20Projet%2C%20RH%2C%20S%C3%A9curit%C3%A9%2FMarch%C3%A9s%20%28documents%20types%2C%20recommandations%29&FolderCTID=0x0120000E999C13AEFECA4E8937896C7A821008&View=%7BED13A7DC%2DB3AD%2D4403%2D8B2A%2DF76DC4E55AE5%7D>

6. Notes sur les domaines d'exigences de la « Grille d'évaluation CCTP SSI »

6.1. Gestion des identités et de l'authentification

Le CHU Toulouse utilise le service d'annuaire AD (Active Directory) de la société Microsoft en référentiel technique d'identité garant de l'unicité des comptes utilisateurs et n'envisage l'authentification unique (SSO / Single Sign On) qu'au travers de l'identité de domaine portée par les protocoles communément utilisés en environnement Windows.

6.2. Journaux et traçabilité

Le CHU Toulouse met en œuvre la centralisation de ses traces applicatives et systèmes au sein d'un dispositif unique afin d'en garantir l'intégrité, la conservation et la bonne exploitation.

6.3. Protection des données sensibles

Rappel : Article L1110-4 du Code de la Santé Publique

*....Excepté dans les cas de dérogation expressément prévus par la loi, ce secret (secret médical) couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. **Il s'impose à tout professionnel de santé ainsi qu'à tous les professionnels intervenant dans le système de santé.***

6.4. Services hébergés hors SI du CHU (SaaS)

Les exigences du domaine lié aux applications en mode SaaS complètent les exigences des autres domaines et ne se substituent pas.

6.5. Services hébergés au sein du SI du CHU et administrés en autonomie par le soumissionnaire

La totalité des exigences de la présente annexe sont applicables au système mis en œuvre par le soumissionnaire. Les exigences ci-dessous précisent le contexte particulier du système administré en autonomie par le soumissionnaire.

7. Glossaire des termes employés

AD (Active Directory) : Service d'annuaire de la société Microsoft

Application Web : Architecture applicative reposant sur la mise à disposition par HTTP de contenus HTML dynamiques

HTTP (Hypertext Transfer Protocol) : protocole de communication client/serveur reposant sur le principe de requête/réponse vis-à-vis de ressources identifiées par une adresse réticulaire

IAM (Identity and Authorization Manager) : Service de gestion et de synchronisation des identités et autorisations entre les différents composants du système d'information

Kerberos : Protocole d'authentification reposant sur un chiffrement symétrique

LDAP (Lightweight Directory Access Protocol) : protocole standard de communication avec un service d'annuaire

NTLM : Protocole d'authentification reposant sur un mécanisme de challenge

PAM (Privileged account management) : En français, système de gestion des comptes à privilèges. Gestion de comptes administrateur et à pouvoir, avec journalisation, traçabilité et enregistrement des actions.

PKI (Public Key Infrastructure) : Dispositif de gestion des clefs publiques. Permet l'édition des bi-clefs nécessaires au cryptage asymétrique.

SGBD : Dispositif de dépôt et d'indexation de données permettant l'adressage de grands volumes

SOAP : Protocole applicatif mis en œuvre dans le cadre de web services reposant sur l'échange de flux XML par le biais d'un serveur HTTP.

Web Service : Service applicatif exposé sous forme d'API selon le protocole SOAP.

XML (Extended Markup Language) : « langage de balisage extensible » en français) est un métalangage informatique de balisage générique.