Titre du document / Title of the document

CONTRAINTES DU TEXTE 21 CFR PART 11 SUR LE DEVELOPPEMENT DE LOGICIEL APPLICATIF

Rédigé par / Written by :	Fonction / Function :	Date :
Steve CANAS	**Responsable Qualité et Validation**	03/01/2008
Vérifié par / Reviewed by :	Fonction / Function :	Date :
François TRONCHON	**Responsable Contrôle Qualité**	04/01/2008
Approuvé par / Approved by :	Fonction / Function :	Date :
William GESLOT	**Gérant et Directeur des Projets**	08/01/2008

SOMMAIRE / TABLE OF CONTENT

1 EXIGENCES FONCTIONNELLES NECESSAIRES A LA CONFORMITE AVEC LE TEXTE 21 CFR PART 11 POUR CE QUI CONCERNE LES ENREGISTREMENTS ELECTRONIQUES

- 21 CFR 11.10 (d) L'application doit permettre de restreindre l'accès aux données aux seules personnes autorisées
- 21 CFR 11.10 (d) Le code d'identification (UID) attribué à chaque utilisateur doit être unique
- 21 CFR 11.10 (d) Le code d'authentification (PASSWORD) doit être déterminé par l'utilisateur
- 21 CFR 11.10 (d) L'application doit obliger l'utilisateur à fixer un mot de passe d'une longueur minimum (chez nous 6 caractères)
- 21 CFR 11.10 (d) L'application doit obliger l'utilisateur à changer son mot de passe à la première connexion
- 21 CFR 11.10 (d) L'application doit verrouiller la session d'un utilisateur après une période d'inactivité définie sur une session ouverte (chez nous 30 minutes)
- 21 CFR 11.10 (d) L'application doit verrouiller le compte d'un utilisateur après une période définie sans ouverture de session (chez nous 12 semaines)
- 21 CFR 11.10 (d) L'application doit forcer l'utilisateur à changer son mot de passe régulièrement (chez nous tous les 6 mois)
- 21 CFR 11.10 (d) L'application doit obliger l'utilisateur à saisir son UID et son PASSWORD pour ouvrir une session
- 21 CFR 11.10 (d) Après verrouillage d'une session l'utilisateur doit avoir à saisir son UID et son PASSWORD pour accéder de nouveau à sa session.
- 21 CFR 11.10 (d) L'application doit verrouiller le compte d'un utilisateur après 3 tentatives d'accès infructueuses.
- 21 CFR 11.10 (d) L'application doit interdire que deux utilisateurs puissent avoir le même UID
- 21 CFR 11.10 (d) L'application doit disposer de son propre module de sécurité
- 21 CFR 11.300 (d) Le module de sécurité doit reporter de manière automatique les incidents de sécurité survenus lors des sessions. (tentatives d'accès infructueuses, accès en dehors des heures de travail, etc…)
- 21 CFR 11.10 (e) L'application doit générer automatiquement un fichier de pistage, renseigné au fil de l'eau, qui enregistre les actions des utilisateurs relatives à la création, modification, suppression des enregistrements.
- 21 CFR 11.10 (e) Le fichier de pistage doit enregistrer qui à accédé à quoi, à quelle heure, l'action réalisée, l'identité de la personne effectuant l'action.
- 21 CFR 11.10 (e) Le fichier de pistage doit être horodaté (heure/minutes/secondes) de manière non ambiguë et doit préciser le fuseau horaire utilisé.
- 21 CFR 11.10 (e) Les informations enregistrées dans le fichier de pistage ne doivent pas pouvoir être modifiées par les utilisateurs ou par les administrateurs de l'application

- 21 CFR 11.10 (e) Lorsqu'une information concernant la modification d'une donnée est enregistrée dans le fichier de pistage, la nouvelle donnée ne doit pas venir masquer la donnée initiale (on doit pouvoir lire l'ancienne valeur et la nouvelle valeur).
- 21 CFR 11.10 (e) Le fichier de pistage doit être sauvegardé en même temps que les données.
- 21 CFR 11.10 (e) Le fichier de pistage doit pouvoir être rapidement consulté et/ou imprimé
- 21 CFR 11.10 (e) Le fichier de pistage doit pouvoir être exporté dans un format électronique pour transmission aux autorités.
- 21 CFR 11.10 (g) Les données (statiques ou dynamiques) ne doivent pouvoir être accessibles qu'a travers l'application.
- 21 CFR 11.10 (g) L'application doit pouvoir générer une liste des utilisateurs avec leurs droits d'accès et privilèges sur les enregistrements

2 EXIGENCES FONCTIONNELLES NECESSAIRES A LA CONFORMITE AVEC LE TEXTE 21 CFR PART 11 POUR CE QUI CONCERNE LES SIGNATURES ELECTRONIQUES

- 21 CFR 11.50 Les utilisateurs doivent être informés de l'équivalence légale de leur signature électronique avec leur signature manuscrite et doivent formellement reconnaître en voir été informé et l'accepter.
- 21 CFR 11.50 La signature électronique doit faire apparaître le nom complet de la personne ayant réalisé la signature.
- 21 CFR 11.50 L'enregistrement de signature électronique doit faire apparaître la date et l'heure de la signature.
- 21 CFR 11.50 L'enregistrement de la signature électronique doit faire apparaître la décision du signataire (accord, refus, retour, etc…).
- 21 CFR 11.50 Une action de signature électronique ne doit pas proposer une décision par défaut.
- 21 CFR 11.50 L'application doit utiliser une méthodologie de signature électronique qui lie de manière indéfectible la signature à l'enregistrement pour lequel elle a été générée.
- 21 CFR 11.100 Le code de signature de chaque personne habilitée à signer doit être unique.
- 21 CFR 11.100 L'application doit identifier un utilisateur avant que celui-ci ne puisse entrer son code de signature.
- 21 CFR 11.200 Le processus de signature, s'il est réalisé de manière non biométrique doit faire appel à deux composants distincts (UID et PASSWORD) ou mieux le PASSWORD et un SIGN CODE qui ne change jamais.
- 21 CFR 11.200 Si le processus de signature lorsqu'il est réalisé de manière non biométrique fait appel à un seul composant, celui-ci doit être le password.
- 21 CFR 11.200 L'écran de signature doit se verrouiller après 30 secondes.

Et bien sur l'application (*ou le système*) doit être installé, validé, maintenu en conformité avec les exigences des cGxP. Ceci implique un gros travail de rédaction de procédures (*installation, sécurité,*

utilisation, règles de saisies) un effort de validation conséquent mais variable selon la criticité de l'application et son origine (*logiciel commercial utilisé tel quel sans aucune modification ni adaptation, logiciel configurable, logiciel développé spécifiquement*) et dans la phase d'exploitation un travail récurent de gestion de configuration qui peut n'être pas négligeable