

Utilisation du mot de passe dans secuTrial®

Référence	Version	Type	Valable dès le
UIC.SER.DAT.INS.01	2	INS-Instruction	17/12/2013
Rédaction	Vérification	Approbation	
MOSTAGUIR Khaled	CHABERT Jocelyne	DESMEULES Jules	

*Ce document comporte 2 sections identiques, une en français et une en anglais.
This document has two identical sections, one in French, and the other in English.*

(Section française) Se connecter au système secuTrial® : Votre user-ID, votre mot de passe et vos responsabilités

Gardez à l'esprit que votre compte secuTrial® est **strictement personnel et que vos paramètres d'accès doivent rester confidentiels.**

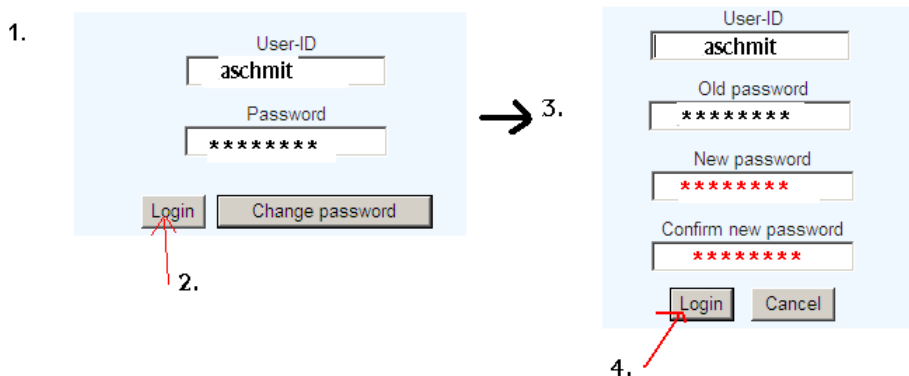
En mode de production, vous êtes tenu **responsable de toute action effectuée dans secuTrial® avec vos paramètres de connexion. Toute action active ou passive est considérée comme étant faite sous votre nom (système Audit Trail).**

Dès votre première connexion au système, vous acceptez implicitement ces termes.

L'accès au système est créé par le Data Manager à la demande du promoteur et/ou de l'investigateur principal de chaque centre. Seules des adresses institutionnelles sont utilisées pour la communication. L'accès est personnel et ne doit en aucun cas être communiqué à une tiers personne. Pour répondre aux exigences de sécurité des HUG, l'accès est bloqué après 4 essais infructueux. Pour réactiver un compte bloqué, contactez le Data Manager:

datamanager.crc@hcuge.ch (CC: Khaled.Mostaguir@hcuge.ch)

A votre première connexion, le système vous demandera de remplacer immédiatement le mot de passe qui vous a été envoyé par un nouveau mot de passe qui vous est personnel:



Le nouveau mot de passe doit contenir au moins *huit caractères* dont au moins *1 chiffre* et ne pas contenir de nom facilement identifiable comme le nom ou le prénom de l'utilisateur, le nom de l'étude, le rôle de l'utilisateur ou le nom du logiciel. Le système vous demandera un changement de votre mot de passe tous les 3 mois.

Tout utilisateur de secuTrial® est responsable de son accès à secuTrial® et de l'utilisation de son mot de passe. Il ne doit se connecter au logiciel qu'avec les accès qui lui ont été communiqués et ne doit pas transmettre à un tiers son accès et mot de passe.

En cas de perte de mot de passe, le nouveau mot de passe ne sera communiqué qu'à la personne à laquelle l'accès a été attribué.

Utilisation du mot de passe dans secuTrial®

(English section) Connecting to the secuTrial® system: Your user-ID, your password, and your responsibilities

Please, keep in mind that your secuTrial® account is **strictly personnel** and your access parameters must remain confidential.

In the production mode, you are **responsible** and accountable for any active or passive action performed in secuTrial® with your login parameters, as it is made under your name (Audit Trail system).

Upon your first login to the system, you agree to these terms.

The access to the data entry module is created by the Data Manager upon request of the Sponsor and/or the Principal Investigator. Only institutional addresses are used to communicate. Accesses are strictly personal and must not be transmitted to a third party. To ensure security access is denied after four wrong attempts. In case of problem you should contact the CRC Data Manager at:

datamanager.crc@hcuge.ch (CC: Kahled.Mostaguir@hcuge.ch)

Upon your first login, the system will ask you to immediately replace the password that you received with a new password that is personal.

1.

2.

3.

4.

You should choose a password with at least 8 characters including at least 1 number, excluding passwords easily identifiable; such as your user ID, the study name, your role or the name of the software. The system will require a new password change every 3 months.

A secuTrial® user is responsible for his access and of the use of his password. He/she must connect to the software using only his personal account and should not transmit to a third party his access information or his password.

In case of a password loss, the new password will be communicated to the person to whom access has been assigned.