RESOURCE USER AGREEMENT
for the Mosler system for sensitive data

To have access to the Mosler system the user must belong to an approved project, be a registered user in SNIC:s SUPR system (supr.snic.se) and have signed this agreement.
In signing this agreement, You are agreeing to be bound by the terms and conditions of access set out in this agreement.

For the sake of clarity, the terms of access set out in this agreement apply both to the researcher that will be granted access to the Mosler resources and the organisation, at which the User is employed, affiliated or enrolled (the "**Institution**"). The researcher and the Institution are referred to within the agreement as "You", and "Your" shall be construed accordingly.

Terms and Conditions:

In signing this Agreement:

- You confirm that You understand that neither NBIS, UPPMAX nor Uppsala University will be responsible for any personal data that You will subsume into the Resources, and that any such responsibility will remain with You.
- You confirm that You understand that the personal data subsumed into the Resources must be associated with an approval(s) from an ethical committee, and that You will adhere to the terms in such approvals.
- You confirm that You understand that you have full responsibility for ensuring that non-authorized persons to not get access to the Resource through your connection to it, and that you must use appropriate security procedures to prevent this, such as e.g. using password protection and activating locking screen savers on computers from which you access the Resource.
- You agree to acknowledge the use of the Mosler system in publications according to this example: "*Support by NBIS (National Bioinformatics Infrastructure Sweden) for the use of the Mosler system for sensitive data is gratefully acknowledged.*"

Name of user: ______________________________

UPPMAX username: ______________________________

Name of Researchers Institution: ______________________________

Signature User:	**Signature on behalf of Researcher Institution:**
______________________________	______________________________
Date of signature:	Date of signature:

Password token

The second password token has been generated and given to the user after controlling the user's identity.

User identification control:

□ User is known □ ID (type & no.): ______________________________

Signature, Token Administrator:
____
Date of signature: