Rules of Conduct for users at the HPC@UCPH cloud facility

I acknowledge that I shall abide to HPC@UCPH security policies, procedures and directives.

I acknowledge that I shall not, without the prior written approval of the HPC@UCPH, disclose, or cause to be disclosed, to any person or organization, other than the HPC@UCPH, any HPC@UCPH material. "HPC@UCPH material" is any material either provided by the HPC@UCPH to me or otherwise stored at the HPC@UCPH computer facility, including, but not limited to, documents, equipment, information and data stored by any means.

I acknowledge that I shall not, without the prior written approval of the HPC@UCPH, connect, or cause to be connected any communications device to any HPC@UCPH provided equipment. In giving written approval the HPC@UCPH may impose such terms and conditions as it thinks fit.
I acknowledge that the Council of Europe's Convention on Cybercrime, Budapest, 23.XI.2001 as well as corresponding laws of Denmark regarding offenses relating to computers may apply to me. I understand that unlawful access, or damage to HPC@UCPH data, or other data stored on HPC@UCPH computers is an offense. I also understand that unlawful access, or damage to HPC@UCPH data, or other data, by means of any access is an offense. Furthermore, I undertake not to engage in unethical or illegal behavior in connection with HPC@UCPH resources, including:

- Intentional harassment of other users.
- Intentional destruction of or damage to equipment, software, or data belonging to HPC@UCPH or other users.
- Intentional disruption or unauthorized monitoring of electronic communications.
- Unauthorized copying of copyrighted materials.
- Violation of computer system security.
- Unauthorized use of computer accounts, access codes or devices, or network ID numbers assigned to others.
- Intentional use of computer telecommunication facilities in ways that unnecessarily impede the computing activities of others.
- Use of computing facilities for private business purposes.
- Academic dishonesty.
- Violation of software licenses.
- Violation of network usage policies and regulations.
- Violation of other users' privacy.
- Violation of privacy laws and regulations, including any kind of processing of data subject to the EU GDPR except on systems officially approved for it.

I understand that a login username and password or key over a secure, encrypted connection are required for me to gain access to HPC@UCPH computers. I undertake to choose only sufficiently complex passwords to avoid anyone guessing them and accept that I may have to change passwords regularly and at least on suspicion of disclosure. I acknowledge that I will not let any other person access my account, nor divulge the login and password to anyone, nor record these details in any insecure locations.

I furthermore undertake never to transmit the username and password over an unencrypted or weakly encrypted link; in particular, I will always use encryption tools such as 'ssh' and 'scp/sftp' (secure shell and secure copy/secure ftp) for every stage of network communication between my

immediate point of network access and the HPC@UCPH facilities. I realize that I must not attempt to access my HPC@UCPH account unless such encrypted protocols are installed and available on the local machine that is my immediate point of network access at any given time. I agree to inform HPC@UCPH immediately should I suspect that my login has been compromised.
In case the workstation, which I use for my secure connection to the HPC@UCPH cloud facility, relies on a network connection from a commercial internet provider, I understand that it is solely my responsibility to make sure that this connection into the cloud facility is secure and that no one else has access to open or access my connection. I also undertake to encrypt any connections to the recognized workstation and keep it updated and secure against known threats.

Similarly all cloud instances I create and run on the cloud facility **must** be kept updated and secure, and it is solely my responsibility to either keep the automatic update facilities functional and running *or* to manually take full responsibility for applying all security updates in due time. Importantly my cloud instances are **only** allowed to run the network services I have explicitly been permitted to run. We at HPC@UCPH reserve the right to regularly scan all running instances for enabled services as well as known vulnerabilities. This includes the right to block access to any such unauthorized or vulnerable instance services to prevent abuse.

I understand that my account can be closed at any time by request of the party (i.e. UCPH-employed collaborator or HPC@UCPH) that initially granted me access. Also, I understand that by request of this party, HPC@UCPH will grant access to any data I have stored on the system.

I understand that if I fail to comply with this undertaking, action may be taken to cancel my accounts.

Finally, I further undertake to report all unusual or suspicious activity immediately to the HPC@UCPH administration.

Printed name:

Signature and date:
