Checklist for new instrument account

Name…….. Title…….

E-mail…….. Phone…….

Research group…….. ZZ-code…….

Access after working hours required for the following floors at CMM L8 ……

Keys required for the following rooms…… Key number……..

Expiry date (max 5 years)……

Instrument name ……

Instrument responsible (name) ……..

E-mail (instrument responsible)……..

Mandatory read checklist

☐ CMM GDPR policy[1,2] Date……..

☐ Liability agreement CMM IT[1,2] Date……..

I have made sure the new instrument user has received all relevant information and specific instructions regarding his or her work at CMM

Signature (instrument responsible) …….. Date……

I have read and understood all information regarding my work at CMM

Signature (instrument user)…… Date……

[1] Mandatory before applying for CMM IT account, keys and key cards
[2] Documents can be found at CMM website: cmm.ki.se - Resources - Documents

Contingent liability agreement

regarding the use of CMM's and KI's computer, network and system resources.

Owner

All computer resources, computer networks, related equipment and accounts are owned and operated by CMM or KI for use in carrying out all university business. All other use, such as for personal development, is only permitted on the following conditions:

- that it does not disrupt normal usage
- that it does not contravene these regulations
- that it does not conflict with departmental rules, CMM's and KI's regulations, SUNET's rules or prevailing laws

By authorized user in these regulations is meant an employee, student or other person who has been allocated an account or granted authorization to use CMM's and KI's computer, network or system resources.

The following conditions apply to all authorized users:

- Authorization and subsequent access to the related resources are strictly non-transferrable.
- Passwords associated with authorization must be kept secret. See the separate document for further details about password regulations (Data Security on the KI intranet).
- Authorization is limited and will be terminated once the period of employment, the project or equivalent at CMM and KI comes to an end. CMM and KI reserves the right to terminate authorization that has been inactive for more than six months unless agreed otherwise.

The following conditions apply to the use of CMM's and KI's computer, network and system resources:

- Acts of sabotage or disruption to the system or other users, and all hacking or attempted hacking into the system from within or outside CMM and KI, are strictly forbidden.
- All commercial use of CMM's KI's computer resources is strictly forbidden unless otherwise agreed.
- The use of misconfiguration, program errors or other methods to acquire extended system rights or other kind of authorization than that which has been granted by system personnel is strictly forbidden.
- Anyone who detects an error, defect, breach of regulations, irregularity or other such problem shall immediately report it to the system manager.
- No material may be copied or distributed unless it is expressly stated otherwise. Material that is copyright protected may only be copied or distributed with the permission of the copyright owner. KI reserves the right to restrict the use of CMM's and KI's equipment for publishing and distributing material.

Breach of regulations

- System managers are obliged to report all infringements of these regulations and the prevailing laws to the IT department. If there is suspicion of criminal activity, the president is empowered to make arrangements for taking legal action. The subsequent penalties range from exclusion from CMM's and KI's ADP resources to a fine or imprisonment. Certain illegal or illegitimate activity may entail the payment of damages.
- System managers are obliged to sign a declaration of secrecy.
- In order to manage the day-to-day operation of the resources and to ensure compliance with these regulations, system managers are entitled, within their sphere of responsibility, to monitor CMM's and KI's systems and check the contents of traffic, data etc. that is either stored or being transmitted.
- System managers are entitled to prevent access to CMM's and KI's computer, network or system resources should they have grounds to suspect that these regulations are being infringed.

Sensitive or important data?

- Sensitive data or confidential information may not be sent over the network in an unencrypted format.
- Prevailing regulations are available in digital form on KI's webserver.
- CMM's and KI's IT departments have resources and data security personnel that can be consulted for information and advice.
- The KI IT department distributes security information when necessary to the local system managers and at its different departments for further distribution to all department members.

I undertake to keep myself informed about the prevailing regulations governing the use of CMM's and KI's computer systems at any one time and to comply with these regulations in full. By signing the Checklist for new arrivals document, I certify that I have read and understood these regulations. I am also aware that any negligent use of the systems or failure to comply with the instructions of the system managers may mean my being denied access to the computer, network or system resources.