Regulations for student use of Chalmers' IT resources

These regulations apply to everyone who is a student. To access Chalmers' IT resources, you must first read and accept these regulations.

Chalmers' IT resources are intended to be used in and for Chalmers' mission to provide education, research and related administration, as well as for collaboration with the surrounding society, referred to as third stream activities.

The term "Chalmers' IT resources" refers to, for example (list is not exhaustive), mobile devices, computers, computer networks, IT services, information assets, and electronic resources such as licences, software and databases.

Use and management of Chalmers' IT resources and information assets

Chalmers' IT resources may not be used for the dissemination of information:

- Which violates applicable law, such as incitement against ethnic groups, child pornography offences, unlawful depiction of violence, libel, harassment, data breach or copyright infringement;
- Which is regarded as political, ideological or religious propaganda;
- Which violates the provisions of the Personal Data Act on personal privacy;
- Which may otherwise be perceived as violating and offensive;
- Which is for commercial activity through the marketing of products or services that are not approved by Chalmers;
- Which in some other way can disrupt Chalmers' IT operations.

Access rights

- Use of Chalmers' IT resources or networks for which you do not have access rights is prohibited.
- Any attempt to obtain higher access rights to Chalmers' IT resources than you are entitled to is prohibited.
- Use of Chalmers' IT resources to acquire access rights you are not entitled to in other systems is prohibited.

Use

- Allocated IT resources are intended for use during studies and may not be made available or lent out for private use to family members, acquaintances or others.
- Use of Chalmers' IT resources in a way that could harm Chalmers' name, standing or good reputation or in a way that exposes Chalmers to unnecessary risks is prohibited.

Equipment & security

- All computers and other equipment (mobile telephones, e-readers or tablets, computers, etc.) that are connected to Chalmers' network must satisfy a good level of security (which includes a functioning antivirus, firewall and security-updated operating system), regardless of who owns them and where they are located.

User accounts and passwords

- Access rights to Chalmers' IT resources are personal and may not be given to another party to use.
- Do not disclose or share your password to anyone else.
- Do not ask anyone else to give you their password.
- Do not use anyone else's personal login details, even if they shared their login information with you.
- The password must be at least 10 characters long and contain at least four alphabetic characters (A-Z or a-z. Not ÅÄÖ/ääö), one number and one punctuation mark. See rules from PDB: https://pdb.chalmers.se/PDB4Web/views/AboutPasswords.jsf
- Passwords must be changed promptly if there is reason to believe that another party may have gained access to it.
- Use of a password manager for the storage and management of personal passwords is permitted. The master password for the password manager must be complex, hard to guess, and follow the previously defined content requirements.

Remote work

When working remotely or using Chalmers' IT resources outside of the campus, good information security must be practiced. Always use Chalmers' equipment and services when possible.

Email

An assigned Chalmers email address is intended and permitted for internal and external communication. Some use of a Chalmers email address for private purposes is also allowed, provided it does not interfere with studies or expose Chalmers to unnecessary risks.

Monitoring and measures in case of violation

- To ensure a high level of security, network traffic and stored data may be logged and monitored and may be investigated for possible violations of applicable laws and user guidelines.
- Logs are saved and archived in accordance with applicable laws and regulations on purging and archiving.
- Computer and electronic resources connected to Chalmers' networks are systematically scanned regularly for known vulnerabilities.
- If you discover or have reason to suspect a security breach or misuse of Chalmers' IT resources, you must report this immediately to the Chalmers Servicedesk.
- Technology officers may temporarily suspend or revoke network access to a mismanaged or misused IT resource with immediate effect.
- Violations of these guidelines may be investigated by the IRT/IT department and referred to the Disciplinary Committee for further action. Such action is warning or suspension from studies or other activities at the University for a set period of time according to the provisions of the Disciplinary Code.
- Suspected violation of law will be reported to the police.

I hereby agree to follow applicable regulations for the use of Chalmers' IT resources. I am aware that violation of the regulations may lead to disciplinary and/or legal action, such as a police report and claim for damages, being taken against me.

Adopted 6 November 2020
Ref. no. C 2020-0459