

Föreskrifter för studenters användande av IT-resurser

Dessa föreskrifter gäller för dig som är student. För att få tillgång till Chalmers IT-resurser måste du först läsa igenom föreskrifterna och godkänna dem.

Chalmers IT-resurser är avsedda att användas i och för Chalmers uppdrag att tillhandahålla utbildning, forskning och därtill knuten administration samt för samverkan med det omgivande samhället, den s k tredje uppgiften.

Med Chalmers IT-resurser avses exempelvis (men inte uteslutande) mobila enheter, datorer, datornät, IT-tjänster, informationstillgångar, samt elektroniska resurser som licenser, programvara och databaser.

Användning och hantering av Chalmers IT-resurser och informationstillgångar

Chalmers IT-resurser får inte användas för spridande av information:

- Som är i strid mot gällande lagstiftning, till exempel hets mot folkgrupp, barnpornografibrott, olaga våldsskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott,
- Som är att betrakta som politisk, ideologisk eller religiös propaganda,
- Som är i strid mot personuppgiftslagens bestämmelser om den personliga integriteten,
- Som i annat fall kan uppfattas som kränkande och stötande,
- Som är för kommersiell verksamhet genom marknadsföring av produkter eller tjänster som inte är godkända av Chalmers,
- Som på annat sätt kan störa Chalmers IT-verksamhet.

Behörigheter

- Det är inte tillåtet att använda sig av Chalmers IT-resurser eller nätverk som man har saknar behörighet till.
- Det är inte tillåtet att försöka skaffa sig högre behörigheter i Chalmers IT-resurser än vad man har rätt till.
- Det är inte tillåtet att nyttja Chalmers IT-resurser för att skaffa sig behörigheter man inte har rätt till i andra system.

Användande

- Tilldelade IT-resurser är avsedda för bruk under studier och får inte upplåtas eller lånas ut för privat användning av familjemedlemmar, bekanta eller andra.
- Det är inte tillåtet att använda Chalmers IT-resurser på ett sätt som kan komma att skada Chalmers namn, anseende eller goda rykte, eller att Chalmers exponeras för onödiga risker.

Utrustning & säkerhet

- Alla datorer och annan utrustning (mobiltelefoner, surf eller läsplattor, datorer etcetera) som ansluts till Chalmers nätverk ska oavsett vem som äger dem och var de är placerade uppfylla god säkerhetsnivå (vilket omfattar fungerande antivirus, brandvägg och säkerhetsuppdaterat operativsystem).

Användarkonton och lösenord

- Behörigheter till Chalmers IT-resurser är personliga och får inte upplåtas till någon annan.
- Det är inte tillåtet att uppge eller dela med sig av sitt lösenord till någon annan.
- Det är inte tillåtet att begära att någon ska uppge sitt lösenord.
- Det är inte tillåtet att använda någon annans personliga inloggningsuppgifter oavsett om denne själv har delat med sig av inloggningsinformationen.
- Lösenordet ska vara minst 10 tecken långt och innehålla minst fyra alfabetiska tecken (A-Z eller a-z. Ej ÅÄÖ/åäö), en siffra och ett skiljetecken. Se regelverk från PDB: <https://pdb.chalmers.se/PDB4Web/views/AboutPasswords.jsf>
- Lösenord ska skyndsamt bytas om det finns misstanke att det blivit kända av någon annan än användaren själv.
- Det är tillåtet att använda lösenordshanterare för lagring och hantering av personliga lösenord. Huvudlösenord för lösenordshanterare ska vara komplext, svårgissat och följa tidigare definierat krav på innehåll.

Distansarbete

Vid distansarbete, eller användande av Chalmers IT-resurser utanför campus ska god informationssäkerhet iakttas. Använd alltid Chalmers utrustning och tjänster där det är möjligt.

E-post

Tilldelad Chalmers e-post är avsedd och tillåten för intern och extern kommunikation. Viss användning av Chalmers e-post för privata ändamål är också tillåten under förutsättning att det inte inkräktar på studierna eller att Chalmers utsätts för onödiga risker.

Övervakning och åtgärder vid regelbrott

- För att säkerställa hög säkerhetsnivå kan nätverkstrafik och lagrade data komma att loggas och övervakas samt utredas för eventuella överträdelser av gällande lagar och användarriktlinjer.
- Loggar sparas och arkiveras i enlighet med gällande lagar och föreskrifter om gallring och arkivering
- Datorer och elektroniska resurser anslutna till Chalmers nätverk avses systematiskt och regelbundet efter kända sårbarheter.
- Om du upptäcker eller har anledning att misstänka en säkerhetsbrist eller ett missbruk av Chalmers IT-resurser ska du omgående rapportera detta till Chalmers Servicedesk.
- Tekniskt ansvariga kan med omedelbar verkan tillfälligt stänga av, eller dra in nätverksåtkomst -till misskött eller missbrukat IT-resurs.
- Brott mot dessa riktlinjer kan komma att utredas av IRT/IT-avdelningen och överlämnas till disciplinnämnd för vidare åtgärder. Sådana åtgärder är varning eller avstängning under en viss tid från studierna och annan verksamhet vid högskolan enligt disciplinstadgans bestämmelser.
- Misstänkta lagbrott kan komma att polisanmälas.

Jag förbinder mig härmed att följa gällande föreskrifter för användning av Chalmers IT-resurser. Jag är medveten om att en överträdelse av föreskrifterna kan leda till disciplinära och/eller rättsliga åtgärder, som polisanmälan och skadeståndstalan, kan vidtas mot mig.

(Underskrift, namnförtydligande och datum)

Fastställt 2020-11-06
Dnr C 2020-0459