



Hantering av bärbar datorutrustning

Denna broschyr är en sammanställning och ett komplement till de regler som styr bruket av Göteborgs universitets (GU:s) IT-resurser.

Reglerna ska tillämpas närhelst anställd eller annan medarbetare vid GU använder bärbar datorutrustning i sin anställning, sitt projektdeltagande eller uppdrag.

Med bärbar datorutrustning avses bärbar dator och även handdatorer och mobiltelefoner med handdatorfunktion.

Med lösa minnesmedia avses övrig elektronisk utrustning som innehåller en minnesfunktion såsom lösa hårddiskar, CD, DVD, USB-minnen, band, disketter och dylikt.

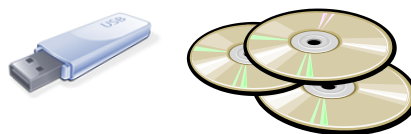


GÖTEBORGS UNIVERSITET



När du har en bärbar dator som tillhandahålls av GU ansvarar du för att:

- ha uppsikt över den bärbara datorn eller förvara den på ett säkert sätt oavsett var du befinner dig,
- datorn endast används i och för GU:s verksamhet,
- använda en av GU godkänd anslutning t ex Direct Access eller VPN vid fjärranslutning till GU:s nätverk,
- uppmärksamma risken med koppla upp den bärbara datorn mot oskyddade trådlösa nätverk,
- följa GU:s regler för informationsklassning. Det innebär att information med skyddsvärde 1 och 2 får finnas på en bärbar dator eller annat löst minnesmedia utan restriktioner. För information med skyddsvärde 3 och 4 finns förbehåll, se regler om informationsklassning som finns på <http://www.sakerhet.gu.se/itsakerhet/>
- det finns adekvata säkerhetskopior av innehållet,
- den bärbara datorn utan onödigt dröjsmål uppdateras med aktuella säkerhetsuppdateringar och antivirus,
- återlämna den bärbara datorn då du lämnar din anställning eller ditt uppdrag.



Viktigt att tänka på då du använder lösa minnesmedia

- GU:s regler för informationsklassning ska följas,
- Om du använder lösa minnesmedia för att göra back-up t ex när du inte har tillgång till GU:s nät, förvara dessa åtskilt från datorn. Detta för att undvika att all information försvinner vid en stöld.
- Lösa minnesmedia som ska förstöras kan kastas i de sekretessboxar som tillhandahålls av GU:s avfallsentreprenör.

Vad måste du göra i övrigt för att skydda din och universitetets information?

Universitetets IT-resurser är avsedda för utbildning, forskning och samverkan med det omgivande samhället, biblioteksverksamhet och administration. För att skydda din och universitetets information ska du tänka på att:

- vid arbete på ordinarie arbetsplats bör det finnas möjlighet att låsa fast en bärbar dator,
- användaridentitet, lösenord och tilldelad behörighet är personlig och får inte lånas ut,
- ett lösenord skall vara konstruerat med minst 8 tecken bestående av blandade versaler, gemener, siffror och specialtecken,
- lösenordet bör bytas varannan månad eller så fort det blir känt för någon utomstående,
- inte använda de lösenord du har på jobbet till privata e-postkonton, sociala nätverkssidor och liknande,
- aktivera skärmlåsning när du lämnar datorn.



Att tänka på då du använder Internet och e-post

- Det är vanligt att virus och annan skadlig kod sprids via Internet och sociala nätverkssidor så tänk på vart du surfar när du använder universitetets IT-resurser.
- E-postbilagor är också ett vanligt sätt att sprida virus och annan skadlig kod. Öppna inte en e-postbilaga om det inte tydligt framgår i meddelandetexten vad bilagan innehåller.
- Svara aldrig på e-post där du uppmanas att lämna ut ditt lösenord.
- Du representerar universitetet med din e-postadress. Använd en privat adress för dina personliga ärenden.

Mer information

Mer information hittar du på Göteborgs universitets webbplats under rubriken ”Regler för användning av GU IT-resurser”,
<http://www.sakerhet.gu.se/itsakerhet/>

Tips på hur du sätter bra lösenord finns på <http://www.it.gu.se/sakerhet/losenord/>