

Kontrakt för nyttjande av SLU:s datorresurser

Kontraktet upprättas mellan undertecknad och SLU genom IT-enheten för att reglera användningen av SLU:s datorresurser.

Rättigheter

1. Kontraktet ger undertecknad rätt **att inom ramen för sin verksamhet** vid SLU utnyttja SLU:s datorer, nätverk, modempool och andra nätrelaterade resurser.
2. Undertecknad får en **personlig** användaridentitet som ger tillgång till datorer, servrar, e-post mm.

Skyldigheter

Föreskrifter för användning av SLU:s datornät skall följas.

Det innebär, men är inte begränsat till följande:

1. Undertecknad skall alltid använda sin egen användaridentitet i kombination med ett väl konstruerat lösenord och de inställningar för anslutningen som anvisats av IT-enheten/IT-samordnare. Undertecknad får aldrig låna ut sin användaridentitet/lösenord till någon annan (bilaga "Hur ser ett bra lösenord ut?")
2. Undertecknad får använda annan användares filutrymme endast efter medgivande av denne (Se punkt 5.3).
3. Undertecknad får inte låna ut eller överlåta SLU:s dator- eller nätverksresurser till utomstående (inkl maka/make och barn). Inte heller får olika tjänster spridas via nätet (t.ex.: filarkiv, filmarkiv,

musikarkiv, programarkiv, handel , informationspublicering) som inte ingår i SLU:s verksamhet .

4. Upphovsrätten till programvara och data skall respekteras.
5. Undertecknad är skyldig att rapportera inträffade eller misstänkta säkerhetsincidenter till IT-enheten.

Påföljder

1. Vid misstanke om missbruk kan undertecknads användaridentitet stängas av och filerna låsas medan utredning pågår.
2. Vid överträdelse stängs undertecknad av från användning av SLU:s datorer och andra nätverksresurser.
3. Olämplig eller otillbörlig användning av datorer i datornätverk kan för anställda medföras disciplinära åtgärder i enlighet med lagen om offentlig anställning.
4. Upprepat fall av missbruk anmäls till SLU:s ansvarsnämnd.

Missbruk av datorer kan även vara brott mot svensk eller utländsk lag vilket kan resultera i rättsliga följder.

Undertecknad har tagit del av och accepterat ovanstående.

Student Anställd

Datum Ort.....

Om anställd:
Inst/motsv..... Personnummer.....

Underskrift.....

Förtydligande.....

Detta avtal har upprättats i 2 exemplar varav IT-enheten (i förekommande fall institutionens IT-samordnare) arkiverar 1.

Hur ser ett bra lösenord ut

Ett säkert (=svårknäckt) lösenord bör uppfylla följande kriterier:

1. *Det bör vara 7-8 tecken långt (alla ord på upp till sex tecken bedöms kunna genereras och testas maskinellt, på rimlig tid och många system testar inte mer än 8 tecken).*
2. *Använd inte lösenord som har direkt anknytning till dig själv, din familj eller din arbetsplats och som andra kan känna till, exempelvis personnummer, telefonnummer, bilnummer, dina initialer, användarid eller annan tillgänglig information.*
3. *Använd inte bara bokstäver tag med någon siffra eller något specialtecken. Helst bör både stora och små bokstäver finnas med. (Vissa nätprogramvaror kan emellertid ge problem.)*
4. *Ordet skall inte kunna återfinnas i någon ordlista eller något lexikon det bör heller inte vara en enkel sammanskrivning av två ord.*
5. *Personnamn (enkla eller sammanskrivna) skall undvikas, av samma skäl.*
6. *Använd inte enkla tangentbordsmönster av typen QWERTYU eller 1qaz2wsx.*
7. *Om det tänkta lösenordet innehåller delar av ord så byt ut, tag bort eller lägg till något eller några tecken. Att använda ett normalt, helt ord eller namn med ett tecken utbytt, borttaget eller inskjutet ger dock inte tillräcklig säkerhet inte heller duger det att vända på ett normalt ord eller namn.*
8. *Använda inte de svenska tecknen å ä ö i lösenordet.*

Självfallet bör man också undvika att låta datorn spara användaridentifikation och lösenord för automatisk inloggning.

Med utgångspunkt från att ett lösenord ska vara rimligt svårt att härleda eller testa sig fram till samtidigt som det ska vara relativt enkelt att komma ihåg rekommenderas följande metoder:

- A. *Bilda lösenordet av de första bokstäverna ur varje ord i en fras hämtad från en dikt, boktitel, litterärt citat, sångtext, psalmsvers, teaterreplik, ramsa, slogan eller en helt vanlig mening. (Resultatet får naturligtvis inte bli ett normalt ord som finns i ordlistor som nämndes tidigare. Undvik också mycket kända citat och bevingade ord.) Tag med någon versal och någon siffra eller specialtecken. Till exempel kan man ur frasen Det är säkert som amen i kyrkan bilda lösenordet dassAik. OBS, vi valde a inte ä, å ä ö är ju inte lämpliga i lösenord.*
- B. *En annan variant är att välja ut en teckensträng om 7-8 tecken (utan mellanrum) ur en sådan fras, med början på ett godtyckligt ställe. Dessutom bör även här någon versal och siffra eller specialtecken vara med. Exempelvis kan lösenord som rtsOM+am och kertsomA bildas ur den nyss nämnda frasen.*

Man skall lägga ner stor omsorg på att konstruera ett säkert lösenord. Att behålla ett bra lösenord under lång tid är självklart väsentligt bättre än att ofta byta mellan dåliga lösenord. (Misstänker man att någon obehörig kan ha fått kännedom om lösenordet så måste det naturligtvis bytas omgående.)

Det är självklart inte lämpligt att skriva ned lösenordet och dessutom förvara lappen nära sin datorarbetsplats som t.ex på en lapp under skrivbordunderlägget eller upptejpat på väggen.

Ett nytt lösenord skall noga planeras, inte konstrueras på stunden. Har man en bra regel för hur det bildas en nyckel så blir det lätt att komma ihåg och behöver då inte heller antecknas.