Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

STYRANDE DOKUMENT

SLU ID: SLU.ua.2025.1.1-315

Version: 1.0.2

Sakområde: IT, service, säkerhet och miljö

Dokumenttyp: Regel
Beslutsfattare: Universitetsdirektör
Avdelning/kansli: IT-avdelningen
Beslutsdatum: 2025-01-28

Träder i kraft: 2025-02-03
Giltighetstid: Tills vidare
Senast granskad: 2025-01-28
Bör uppdateras före: 2026-02-28

Dokument som upphävs: –

Bilaga till: Universitetsdirektörens beslut av den 28 januari 2025, SLU.ua.2025.1.1-315

Regler för tillåten användning av IT-resurser

Målgrupp och syfte

Alla användare (anställda, studenter, entreprenörer, konsulter, partner och övriga nyttjare) av universitetets IT-resurser omfattas av dessa regler som fastställer tillåten användning.

Syftet med reglerna är att säkerställa säker och ändamålsenlig användning av SLU:s IT-miljö samt att skydda universitetets information, tillgångar och immateriella rättigheter. Samtidigt ska reglerna möjliggöra ett effektivt och säkert arbete för alla användare. Gränsdragningen kan i många fall vara svår, och användarens eget omdöme är därför viktigt.

Sammanfattning

Dokumentet förtydligar att följande är otillåten användning:

- olaglig verksamhet
- skadlig kod och attacker
- otillåten åtkomst och hackning
- överbelastning och nätverksmissbruk
- trakasserier och skadlig kommunikation
- otillåten delning och lagring av information
- otillåten användning av programvaror.

För att säkerställa efterlevnad och göra det möjligt att följa upp och hantera incidenter sker viss automatiserad övervakning. All användning ska ske i enlighet

med gällande lagstiftning och universitets övriga regelverk. Vid regelbrott kan disciplinära åtgärder vidtas.

Omfattning

Dessa regler förtydligar och fastställer regler för tillåten användning av universitetets IT-resurser. IT-resurser inkluderar bland annat fysisk hårdvara (datorer, servrar, nätverk, mobiler etc.), tjänster och applikationer. Reglerna gäller SLU:s IT-resurser oavsett var användaren är placerad.

Alla användare av SLU:s IT-resurser förbinder sig att följa dessa regler. Reglerna är en del av SLU:s ledningssystem för informationssäkerhet.

Tillåten användning

Användare får endast använda SLU:s tjänster och system för legitima och tillåtna ändamål som stämmer överens med universitetets verksamhetsmål och som sker i enlighet med tillämplig lagstiftning. Tillåten användning omfattar bland annat följande:

- utföra arbetsuppgifter eller uppgifter relaterade till SLU:s verksamhet
- använda SLU:s e-postadresser för kommunikation i tjänsten; det är tillåtet att använda en SLU-adress för privat bruk i ringa omfattning
- använda SLU:s nätverk och resurser inom ramen för SLU:s verksamhet. Användning i andra syften ska hållas inom rimlig omfattning.

Otillåten användning

Olaglig verksamhet

Användning av SLU:s tjänster, system eller nätverk för att bedriva eller underlätta olaglig verksamhet är förbjudet. Dit hör

- bedrägeri, identitetsstöld eller försök att komma över information utan tillstånd
- distribution eller tillgängliggörande av olagligt material, inklusive piratkopior av programvara, filmer, musik eller andra upphovsrättsskyddade verk.

Skadlig kod och attacker

Det är förbjudet att använda SLU:s utrustning, system och tjänster för att initiera eller distribuera skadlig kod, virus, trojaner, ransomware eller annan programvara som är avsedd att skada, störa eller få obehörig tillgång till nätverk eller system. Det är även förbjudet att missbruka SLU:s IT-resurser i syfte att begå dataintrång hos SLU eller annan part.

Otillåten åtkomst och hackning

All form av försök att få obehörig åtkomst till system, nätverk eller data är strikt förbjuden. Detta inkluderar

- försök att kringgå säkerhetsåtgärder eller begränsningar som tillämpas för att skydda nätverket
- försök att bryta sig in i system eller servrar, både inom och utanför universitetets nätverk
- "phishing" eller andra bedrägerier för att få obehörig tillgång till känslig information.

Överbelastning och nätverksmissbruk

Användning av universitetets resurser för att överbelasta, störa eller negativt påverka nätverkskapacitet, prestanda eller stabilitet är förbjuden. Detta inkluderar att

- delta i eller skapa överbelastningsattacker (DDoS)
- oavsiktligt eller avsiktligt skapa överdriven nätverkstrafik som påverkar tjänsternas kvalitet.

Trakasserier och skadlig kommunikation

Det är förbjudet att använda SLU:s tjänster för att sprida förolämpande, hotfulla, trakasserande eller kränkande budskap, exempelvis:

- skräppost, massutskick utan tillstånd eller oönskad reklam (spam)
- förföljelse, mobbning eller hot mot andra användare eller tredje part via SLU:s tjänster.

Otillåten delning och lagring av information

Det är förbjudet att

- dela sekretessbelagd, upphovsrättsskyddad eller annan konfidentiell information med någon obehörig
- dela personuppgifter, framförallt känsliga personuppgifter, som SLU ansvarar för med interna eller externa mottagare som saknar behörighet för och behov av att ta del av personuppgifterna.

Otillåten användning av programvaror

IT-resurser som ansluter till universitetets nätverk (datorer, mobiltelefoner, surfplattor och liknande) bör helst vara uppdaterade med senaste versionen av operativsystem och programvaror. Kravet är att åtminstone ha en supporterad och därmed fortfarande aktivt säkerhetsuppdaterad version. Om detta inte är möjligt ska undantag anmälas via support.slu.se och adekvata säkerhetsåtgärder vidtas.

SLU förbehåller sig rätten att avinstallera programvaror eller rensa enheter som inte följer reglerna.

Det är förbjudet att

- ändra konfigurationen, ta bort, inaktivera eller på annat sätt manipulera säkerhetsskydd eller annan programvara
- ladda ner och nyttja programvaror som inte är korrekt licensierade.

Säkerhetsansvar

Alla användare har ett ansvar att skydda universitetets system och data genom att

- inte dela inloggningsuppgifter med obehöriga individer
- rapportera identifierade avvikelser eller incidenter på support.slu.se eller till support@slu.se
- skydda sina enheter från virus och skadlig programvara
- säkerställa att kommunikation och dataöverföring sker på ett säkert och krypterat sätt när det är möjligt.

Sekretess och konfidentialitet

Att röja uppgifter som enligt offentlighets- och sekretesslagen är sekretessbelagda är ett brott mot tystnadsplikten. Tystnadsplikt innebär en plikt att hemlighålla uppgifter och inte röja eller utnyttja dem vare sig muntligen eller på annat sätt. Brott mot den lagstadgade tystnadsplikten är straffsanktionerat genom brottsbalken.

Övervakning och rapportering

SLU förbehåller sig rätten att övervaka användningen av universitetets IT-resurser för att säkerställa efterlevnad av regelverket. Exempelvis att

- övervaka nätverkstrafik, loggar, och annan relevant information
- övervaka e-post, filer och annan kommunikation relaterad till universitetets verksamhet.

Övervakningen sker enligt gällande lagstiftning och automatiskt utan personell inblandning mer än vid avvikelser och incidenter.

Disciplinära åtgärder

Överträdelser av dessa regler kan leda till disciplinära åtgärder, däribland tillfällig avstängning av användarkonto, nedstängning av datorutrustning, telefon eller därmed likställd IT-resurs.

Vid allvarliga överträdelser som innebär brottsliga förseelser, till exempel brott mot tystnadsplikten, hanteras överträdelsen av universitetets personalansvarsnämnd för anställda respektive disciplinnämnden för studenter.

Ändringar av regelverket

Detta dokument kommer att uppdateras vid behov. Användare ska informeras om väsentliga ändringar och den aktuella versionen av reglerna hållas tillgänglig på medarbetarwebben och/eller andra kommunikationskanaler.

Kontaktinformation

Frågor om dokumentet och IT-säkerhet kan ställas till csirt@slu.se. Frågor om informationssäkerhet ställs till sakerhet@slu.se och frågor om dataskydd och dataskyddsförordningen (GDPR) till dataskydd@slu.se.

Vid support, avvikelser och incidenter sker kontakt via support@slu.se eller support.slu.se.