Kortfattat om påföljder vid överträdelse av IT-regler

Reglerna för universitetets IT-tjänster är bindande och förpliktar alla användare. Även dig.

Med överträdelser av IT-regler avses användning av IT-tjänster på ett sätt som strider mot regler eller lagar. Alla överträdelser som upptäcks ska anmälas till dataförvaltningschefen.

Vid misstanke om överträdelse kan universitetet medan förundersökningen pågår begränsa användarens rätt till IT-tjänster. Med hänsyn till gärningens grovhet och avsiktlighet kan överträdelsen ha interna påföljder och leda till polisanmälan.

Påföljder vid överträdelse av IT-regler

Med databrott avses användning av universitetets datasystem i strid mot givna regler eller bestämmelser eller att datasystemet används i strid mot finsk lag.

Denna instruktion beskriver åtgärder som vidtas vid upptäckt eller grundad misstanke om databrott. Åtgärderna indelas i begränsning av användarbehörigheten under tiden som brottet utreds samt i eventuella preciserade påföljder av brottet.

Universitetet kan begränsa behörigheten att använda IT-tjänster under en förundersökning

Beslut om begränsningar fattas när databrott har observerats eller misstänks. Användarbehörigheten begränsas alltid om man på goda grunder kan misstänka att användaren gjort sig skyldig till missbruk och att behörigheten kan störa utredningen alternativt minimera skadorna. Vid behov hörs användaren.

Beslut om begränsning av användarbehörighet fattas av systemägaren, dataförvaltningschefen eller annan person utnämnd för uppgiften. Administratören verkställer åtgärden.

I brådskande fall kan administratören själv fatta beslut om att begränsa användarbehörigheten för högst tre dagar, vilket genast ska rapporteras till den person som ansvarar för begränsningar.

Vid behov kan användarens arbetsstation kopplas från datanätet.

Begränsningen upphör efter avslutad utredning ifall återställande av behörighet inte är till uppenbar skada.

Påföljder

I lindriga fall får användaren en anmärkning för otillbörlig handling.

Databrott kan leda till att användaren blir ersättningsskyldig för missbruk av resurser (till exempel servrar eller datanät), direkta skador samt utredningskostnader.

Påföljder för studerande

Påföljder för studerande kan vara förlorad eller begränsad användarbehörighet för viss tid, administrativa åtgärder som universitetet vidtar (skriftlig varning, avstängning under viss tid) och polisanmälan (vid handlingar som enligt lag är straffbara).

Dataförvaltningschefen eller systemägaren beslutar om åtgärder gällande användarbehörighet. Begränsningen omfattar inte den tid utredningen tar. Universitetets rektor beslutar om utfärdande av skriftlig varning och universitetets styrelse om avstängning för viss tid. Användarbehörigheten dras in under avstängningen.

Påföljder för personal

Påföljder för personalen kan vara universitetets arbetsrättsliga åtgärder (skriftlig varning, uppsägning, upphävning av anställningsförhållande) och polisanmälan (vid handlingar som enligt lag är straffbara).

Användarbehörigheten till enskilda system kan stoppas temporärt eller permanent när brist på förtroende till följd av missbruk uppstår. Dataförvaltningschefen eller systemägaren beslutar om åtgärder gällande användarbehörighet.

Påföljder för övriga användare

Påföljder för användare som inte hör till universitetets personal eller forskargrupp kan vara indragen eller begränsad användarbehörighet och polisanmälan (vid handlingar som enligt lag är straffbara).

Användarbehörigheten till enskilda system kan stoppas temporärt eller permanent när brist på förtroende till följd av missbruk uppstår. Dataförvaltningschefen eller systemägaren beslutar om åtgärder gällande användarbehörighet.

Exempel på överträdelser

- Olaglig hantering av material som lyder under strafflagen eller upphovsrättslagen
  - material som lyder under strafflagen är till exempel barnpornografi, djurpornografi, grovt våld, rasdiskriminering och hets mot folkgrupp
  - hantering avser bland annat distribution och innehav av material.
- Material som lyder under upphovsrättslagen är till exempel musik, videor, serier, filmer, spel och program.
- Tillgängliggöra användarnamnet genom att till exempel
  - avslöja lösenordet för annan person
  - lämna datorn utan uppsikt så att någon annan kan använda lösenordet.
- Äventyrande av konfidentialitet är till exempel
  - att lämna ut sekretessbelagd eller lagskyddad information till person som inte har rätt till den (till exempel att lämna ut användaridentiteten till servrar)
  - underlåta att skydda sekretessbelagd information (passiv handling)
  - avsiktliga sekretessbrott (aktiv handling)
  - brott mot personuppgiftslagen.
- Underlåtenhet att skydda den personliga integriteten är till exempel
  - att lämna lösenordet utan uppsikt
- Användning av IT-tjänster för kommunikation eller propaganda som kränker god sed