



Gäller från och med 2014-02-01

Anvisning för informations- och IT-säkerhet

Sammanfattning

Syftet med anvisningen är att skapa förutsättningar för en god informations säkerhet vid KTH.

Anvisningen grundar sig på:

- Rektors beslut nr 7, 1996-01-10
- Universitetsstyrelsens beslut 2004-10-28 "Beslut ang ny organisation av KTH", dnr 930-2004-2896, doss 13

Terminologi

Informationssäkerhet har en vid betydelse och vanligen definieras bestå i

- att informationen är tillgänglig inom rimlig tid och i användbar form
- att informationen bevaras riktigt och fullständigt och
- att bara den som är behörig får tillgång till informationen

Med IT-säkerhet avses säkerhet i informationshantering som utnyttjar datorbaserade system. Den tekniska säkerheten i dessa system är en absolut förutsättning för informationssäkerhet.

Bakgrund

Informationssäkerheten ska bygga på en rimlig risknivå och samtidigt tillgodose tillgänglighet, tillförlitlighet och garantera att rätt information är tillgänglig för rätt person.

IT-säkerheten vid KTH ska förhindra att störningar i datanät, datorer och datasystem orsakar allvarliga konsekvenser för KTH, för anställda eller studerande vid KTH.

Allmänt

- Informationssäkerheten ska alltid vara avpassad till rådande hotbild och aktuella risker, till verksamhetens krav och till systemens utformning och användning.
- IT-säkerheten i nät, datorer och datasystem anslutna till SUNET ska uppfylla SUNET:s krav på IT-säkerhet.
- Tillgång till KTH:s datorer, nät och system förutsätter att säkerhetskraven är kända och accepterade
- IT-säkerhetsarbetet ska inordnas i informationssäkerhetsarbetet.
- Informationssäkerhetsarbetet ska samordnas med övrigt säkerhetsarbete vid KTH.

Ansvar

- Ansvaret för informationssäkerheten ligger hos de verksamhetsansvariga
- Ansvaret för informations- och IT-säkerheten inom olika funktioner ska fastställas.
- Vid varje skola/motsvarande ska finnas en ansvarig för informationssäkerheten.

- För datorer, datasystem, datanät eller datautrustning som används vid KTH ska det alltid finnas en IT-säkerhetsansvarig.
- KTH ska ha en gemensam, central funktion för stöd, samordning och kontroll av informationssäkerheten vid KTH.
- Den centrala funktionen ansvarar för att informationssäkerheten vid KTH kontrolleras regelbundet, och för att ledningen hålls informerad om säkerhetsläget.

Säkerhetsnivåer och skyddsåtgärder

- För varje datanät, dator eller datasystem ska kraven på IT-säkerhet vara utredda. För viktiga datasystem ska kraven vara dokumenterade.
- Det ska finnas fastställda riktlinjer för IT-säkerheten och skyddsåtgärderna i sådana nät, datorer och system som används på KTH. För gemensamma system skall dessa riktlinjer beslutas centralt. För övriga system ska de beslutas av systemägaren eller den verksamhetsansvarige i enlighet med denna policy.
- Om så erfordras för att säkerställa att rätt säkerhetsnivå upprätthålls, ska KTH, systemägaren eller den verksamhetsansvarige ta fram detaljerade anvisningar för IT-säkerheten för nät, datorer eller datasystem.
- Hantering och förvaring av information ska ske så att den skyddas mot förlust, skada samt obehörig användning.

Utveckling, upphandling och drift

- Vid utveckling eller upphandling av datorer, datasystem, nät, datautrustning, dator drift eller relaterade tjänster ska IT-säkerhetskraven alltid utredas, och ingå i kravspecifikationen.
- Varje skola/motsvarande eller enhet som använder datorer, datasystem eller datanät måste ha tillgång till kompetent personal i den omfattning som erfordras för att IT-säkerheten ska kunna upprätthållas vid skolan/motsvarande.

Avtal

- För tillgång till KTH:s datorer, nät och system ska ansvarsförbindelse tecknas.
- Då en annan part utför tjänst eller uppdrag åt KTH, ska KTH genom avtal försäkra sig om att parten upprätthåller en informationssäkerhet som motsvarar KTH:s krav.

Kontroll

- IT-säkerheten vid KTH ska kontrolleras regelbundet. För datanät, datorer och datasystem av stor betydelse för KTH:s verksamhet och rykte, eller för KTH:s personal eller studerande, ska kontrollen göras årligen, och resultaten av kontrollen ska redovisas för KTH:s ledning.