



## Säkerhetspolicy för KTH

KTH:s vision är att vara ett ledande tekniskt universitet. KTH:s säkerhetspolicy bidrar till detta genom att garantera säkerhetsmässiga förutsättningar för kontinuitet i verksamheten.

Säkerhetspolicyen uppdateras och fastställs årligen av KTH:s universitetsstyrelse som genom denna ger sitt stöd för säkerhetsarbetet formulerat i denna policy. KTH:s säkerhetspolicy ska vara vägledande och kommuniceras till anställda och studenter.

Säkerhetsarbetet på KTH syftar till att trygga de anställdas, studenternas och besökarnas liv och hälsa. Det syftar vidare till att förhindra och begränsa skador på KTH:s varumärke, egendom och miljö genom konsekventa åtgärder vid avbrott och att upprätthålla kontinuitet i vitala verksamhetsprocesser.

Säkerhetsarbetet ska utgå ifrån gällande lagar, förordningar, författningar och där det förutsätts förhålla sig till KTH:s beslutade policyer; etisk policy, kvalitetspolicy, policy för hållbar utveckling, personalpolicy, säkerhetspolicy och placeringspolicy för KTH:s donationskapital och på riktlinjer, anvisningar och rutiner som följer på dessa policyer.

Säkerhetspolicyen stöds av riktlinjer och anvisningar för styrning av informations och IT-säkerhet, riskhantering, krishantering, fysisk säkerhet och det systematiska brandskyddsarbetet. Styrdokumentet i sin respektive form vänder sig till anställda och studenter, vilka ansvarar för att i tillämpliga delar sträva efter att förverkliga dessa och verka säkerhetsmässigt förebyggande.

KTH:s säkerhetschef ansvarar för KTH:s övergripande säkerhetsarbete, samverkan med andra myndigheter, utbildning och information om förebyggande säkerhet för anställda och studenter, samordna säkerhetsfrågor inom förvaltningen och med KTH:s skolor.

### Informations och IT-säkerhet

KTH bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet, LIS. Standarder som ska beaktas ingår i informationssäkerhetsstandard ISO/IEC 27000. LIS möjliggör styrning och mätning av säkerhetsnivån i verksamheten och att den följs upp. Informationssäkerhet består av de tre delarna; administrativ säkerhet, fysisk säkerhet och IT-säkerhet.

Det är KTH:s IT-säkerhetschef som ansvarar för att samordna, utbilda i och informera om informations och IT-säkerhetsfrågor på KTH, samt utveckla rutiner för att förhindra att störningar, spridning av skadlig kod och dataintrång i datanät, datorer och datasystem orsakar allvarliga konsekvenser.

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

KTH ska ha interna rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten svarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. KTH ska även ha processer för att lära av sådana inträffade incidenter och utförda åtgärder. KTH har tagit fram och utvecklar processer och rutiner som myndigheten behöver för att

kunna uppfylla kraven på it-incidentrapportering.

## Riskhantering

KTH ska vidta lämpliga åtgärder för att begränsa risker och förebygga skador eller förluster. Med riskhantering i säkerhetspolicyen menas identifiering och värdering av större säkerhetsrisker som hot, våld, terror, brand etc. KTH ska värdera riskerna och beräkna vilka kostnader som riskerna kan medföra. Resultatet ska sammanställas i en riskanalys.

KTH:s säkerhetschef ska stödja skolorna i riskhanteringsarbetet genom att verka rådgivande och föreslå lämpliga åtgärder som leder till att förhindra att risker uppstår, förebygga skador och begränsa dess konsekvenser.

## Krishantering

Varje myndighet, vars ansvarsområde berörs av en krissituation, ska vidta de åtgärder som behövs för att hantera konsekvenserna av denna. KTH ska samverka internt och externt med en känslighet för förändringar i samhället och vår omvärld för att kunna möta och hantera oförutsedda händelser. KTH:s krishanteringsförmåga ska vara hög och processen tydligt formulerad på central nivå och inom skolorna. KTH ska genom utbildning och övning utveckla och bibehålla färdigheter för att möta och hantera krissituationer som uppstår internt kopplat till arbetsmiljön och externt genom yttre påverkan. En kris på KTH kan orsakas av brand, hot, våld eller en allvarlig olycka. En kris externt som påverkar KTH kan orsakas av naturolyckor, allvarliga epidemier, terrorhot och kollapsande IT-system. KTH:s säkerhetschef är krisledningsgruppens sammankallande och bedömer tillsammans med krisledningsgruppens ordförande, tillika förvaltningschef, om krisledningsgruppen skall sammankallas.

KTH:s krishantering vilar på tre principer:

- Ansvarsprincipen; innebär att ansvarsförhållandet med rektor som myndighetschef ska vara det samma vid en kris som under normala förhållanden.
- Likhetsprincipen; KTH:s organisatoriska utformning och lokalisering i normalläge är densamma vid kris. Det innebär att universitetsförvaltningen ska verka rådgivande, sakkunnig, samt samverka mot KTH:s skolor och att händelser hanteras lokalt vid skolorna, till dess krisledningsgruppen beslutar annat.
- Närhetsprincipen; innebär att händelser ska hanteras av berörd skola och dess ansvariga funktioner så länge situationen tillåter det.

## Fysisk säkerhet

Fysisk säkerhet på KTH ska verka för att försvåra tillträde för obehöriga till KTH:s lokaler i syfte att förebygga risk för otrygghet för personal, studenter och KTH:s besökare. I förhållande till skyddskrav förhindra risk för skada och förlust genom brand, vatten, klimat – och miljöpåverkan, skadegörelse, tillgrepp och obehörig åtkomst. Den fysiska säkerheten bygger på effektiva och strategiska säkerhetslösningar som verkar i balans med KTH:s öppenhet och tillgänglighet.

## Systematiskt brandskyddsarbete

KTH ska på ett strukturerat sätt planera, utbilda, öva, dokumentera och kontrollera samt åtgärda och följa upp brandskyddsarbetet i organisationen och samverka med externa organisationer, ägare, nyttjare och verksamheter när verksamhet bedrivs inom KTH eller i direkt anslutning där till.

KTH ska i egenskap av ägare eller nyttjanderättshavare till byggnad eller lokal där KTH bedriver verksamhet, i skäligen omfattning hålla utrustning för släckning av brand och livräddning, samt aktivt verka för att anställda och studenter ska ha kunskap om brand och brandförlopp, för att förhindra, förebygga och begränsa skador, tillbud och olyckor till följd av brand.