REVISIONSRAPPORT	Fastställd datum	Diarienummer
	2020-10-01	V-2020-0104
Föredragen i styrelsen		
2020-10-14		

Granskning av KTH:s lednings-system för informationssäkerhet

Revisionsrapport 1/2020

Sammanfattning

Alla organisationer är beroende av information för att kunna utföra sin verksamhet och måste därför skydda sin information så att den alltid finns där när den behövs, att den är tillförlitlig och att endast de som är behöriga får ta del av den. För att säkerställa en tillräcklig nivå på informationssäkerhet är KTH enligt författning[1] [2]tvungen att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem.

Syftet med vår granskning har varit att kartlägga och bedöma om KTH:s informationssäkerhetsarbete sker med stöd av ett ledningssystem som följer gällande bestämmelser i förordning och föreskrifter.

Vår samlade bedömning är att KTH:s ledningssystem för informationssäkerhet i flera avseenden inte uppfyller kraven i gällande bestämmelser. De brister vi anser vara av störst betydelse är

- att myndighetsledningens och den övriga organisationens ansvar för informationssäkerhetsarbetet inte är tydliggjord,
- att nödvändiga befogenheter inte är tilldelade för de roller som arbetet med informationssäkerhet kräver och särskilt för den som utsetts att leda och samordna arbetet,
- att det inte är säkerställt att informationssäkerhetsarbetet bedrivs samordnat samt att det regelbundet utvärderas och löpande utvecklas,
- att det inte genomförs någon regelbunden utbildning rörande informationssäkerhet och
- att det inte har genomförts en klassning av informationen med utgångspunkt i konfidentialitet, riktighet och tillgänglighet utifrån vilka konsekvenser som kan uppstå av ett bristande skydd.

Utifrån våra iakttagelser och slutsatser så väljer internrevisionen att lämna en överordnad rekommendation avseende ledningssystemet för informationssäkerhet.

- Internrevisionen rekommenderar KTH att se över ledningssystemet för informationssäkerhet och säkerställa att det följer gällande bestämmelser.

[1] Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap
[2] Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2016:1

Innehåll

1 Inledning

1.1 Bakgrund

Alla organisationer är beroende av information för att kunna utföra sin verksamhet och måste därför skydda sin information så att den alltid finns där när den behövs, att den är tillförlitlig och att endast de som är behöriga får ta del av den. För att säkerställa en tillräcklig nivå på informationssäkerhet är KTH enligt författningar[3] [4]tvungen att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem.

Internrevisionen har vid flera tillfällen granskat KTH:s informationssäkerhetsarbete och då lämnat rekommendationer i syfte att stärka arbetet med dessa frågor. Den senaste granskningen gjordes 2014 och sedan dess har det gjorts flera externa utredningar och granskningar inom informations- och cybersäkerhetsområdet som pekar på brister i förhållande till dagens hot och risker. Ett exempel är Riksrevisionen som vid två tillfällen 2016 och 2014 har granskat informationssäkerheten i statsförvaltningen. Även regeringen skriver i den försvarspolitiska inriktningspropositionen 2014/15 att Sveriges samlade förmåga att förebygga, motverka och aktivt hantera konsekvenser av civila och militära hot, händelser, attacker och angrepp i cybermiljön måste utvecklas och förstärkas. Regeringen fastställde 2017 en nationell strategi för samhällets informations- och cybersäkerhet som dels är ett uttryck för regeringens övergripande prioriteringar, dels utgör en plattform för Sveriges fortsatta utvecklingsarbete inom området och omfattar hela samhället d.v.s. statliga myndigheter, kommuner och regioner, företag, organisationer och privatpersoner.

Myndigheten för samhällsskydd och beredskap (MSB) utfärdade de första föreskrifterna som ställde krav på statliga myndigheters informationssäkerhetsarbete redan 2009. Förskrifterna reviderades 2016 och ännu en revidering och komplettering av föreskrifterna har skett som kommer att träda i kraft under hösten 2020. Den senaste revideringen beror dels på de brister som framkommit i många statliga myndigheters informationssäkerhetsarbete, dels på den utveckling som sker inom e-förvaltning och övrig digitalisering i samhället. De största förändringarna i föreskrifterna består i att reglering om fysisk säkerhet och personalsäkerhet har lagts till, dessutom har kraven på uppföljning och utvärdering av informationssäkerheten ytterligare konkretiserats.

Den ökande betydelse som frågor om informations- och cybersäkerhet har fått de senare åren gör det angeläget att KTH bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem som lever upp till gällande krav. Internrevisionen har därför på universitetsstyrelsens uppdrag granskat KTH:s ledningssystem för informationssäkerhet.

1.2 Syfte och avgränsning

Syftet med granskningen har varit att kartlägga och bedöma om KTH:s informationssäkerhetsarbete sker med stöd av ett ledningssystem som följer gällande bestämmelser i förordning och föreskrifter.

Utifrån syftet med granskningen så har en avgränsning gjorts till den administrativa delen av KTH:s informationssäkerhetsarbete. Och följaktligen har det inte gjorts någon granskning av det tekniska säkerhetsarbete KTH bedriver.

[3] Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap
[4] Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2016:1

1.3 Genomförande

Granskningen är genomförd under våren 2020 och har utgått från de föreskrifter och allmänna råd som utfärdats av MSB gällande statliga myndigheters informationssäkerhetsarbete. Vi har också beaktat den vägledning som MSB lämnar i dessa frågor och som grundar sig i internationella standarder för informationssäkerhet.

I granskningen har vi granskat interna dokument, genomfört intervjuer och tagit in fakta från berörda personer. Vi har gjort intervjuer med KTH:s IT- och informationssäkerhetschef, dataskyddsombud, koordinator för forskningsdata, systemägare för e-lärande, systemförvaltare för HR-system och vicerektor för digitalisering. Inom ramen för granskningen har vi gjort iakttagelser och dragit vissa slutsatser och baserat på detta lämnar vi rekommendationer. Universitetsdirektören, chefen för IT-avdelningen och IT- och informationssäkerhetschefen har fått möjlighet att faktagranska och kommentera rapporten.

2 Ledningssystem för informationssäkerhet

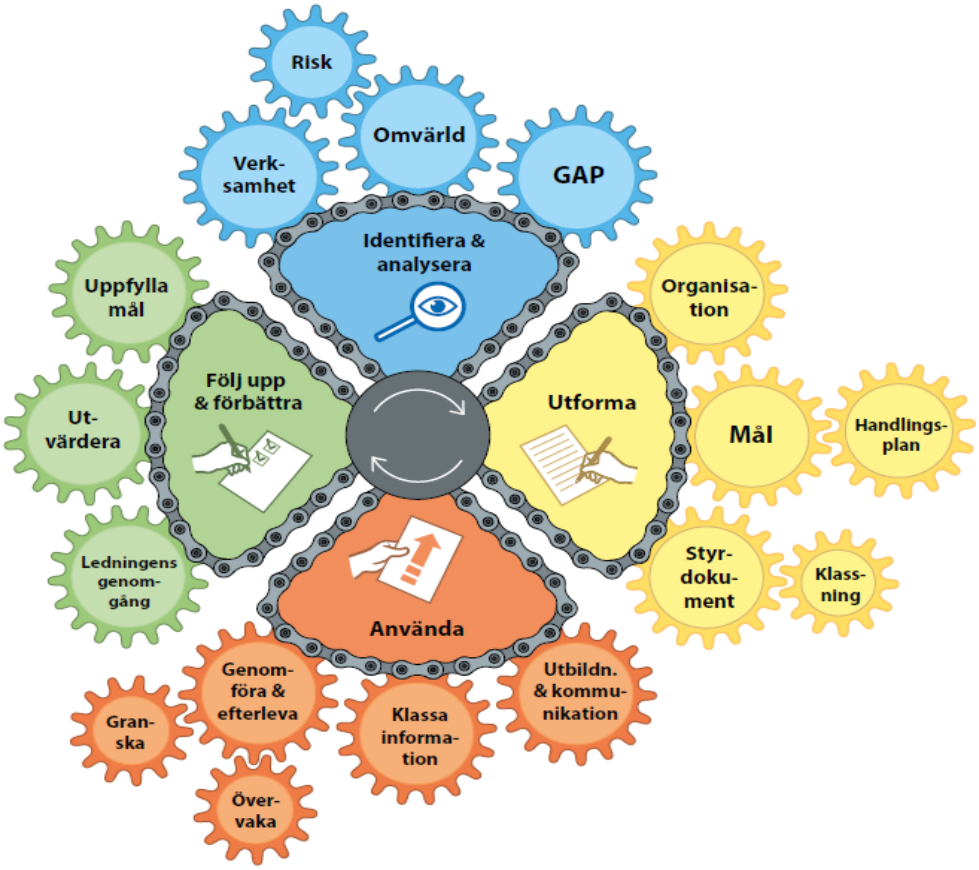
Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk så som policys och riktlinjer, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd. Det handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver. Lagar och författningar fyller en viktig roll i etableringen av informationssäkerhet och handlar i vissa fall om specifikt skydd för viss typ av information och i andra fall om sättet att arbeta med informationssäkerhet generellt.

2.1 Rättsliga krav på informationssäkerhet i statliga myndigheter

Informationssäkerhetsarbete bygger i stor utsträckning på ett systematiskt arbete som involverar ledningen och som grundar sig på risk- och sårbarhetsanalyser samt att rätt åtgärder vidtas. Krav på att statliga myndigheter ska se till att informationshanteringen uppfyller krav på säkerhet finns förordning (2015:1052) om krisberedskap och höjd beredskap. Dessutom föreskriver MSB att myndigheterna dels ska rapportera IT-incidenter och dels ska införa ett ledningssystem för informationssäkerhet. I arbetet med ledningssystemet ska myndigheterna beakta standarderna ISO/IEC 27001 och ISO/IEC 27002.

2.2 Metodstöd för systematiskt informationssäkerhetsarbete

MSB har tagit fram ett metodstöd för att stötta organisationer i att bedriva ett systematiskt informationssäkerhetsarbete. Metodstödet som bygger på standarderna i ISO/IEC 27000-serien beskriver hur de komponenter som utgör ett ledningssystem för informationssystem (LIS) kan utformas. Metodstödet är uppdelat i fyra metodsteg och till varje steg finns tillhörande metoddelar enligt figuren nedan.



Metodstödet och de fyra metodstegen med underliggande metoddelar.

2.3 KTH:s ledningssystem för informationssäkerhet -LIS

En beskrivning av KTH:s LIS finns på intranätet[5] och enligt dokumentet så följer IT- och informationssäkerhetsarbetet PDCA-metoden med steg för planering, genomförande, uppföljning och förbättring. I dokumentet ges det en kort beskrivning av momenten som ingår i respektive steg och i vissa fall finns det också länkar till andra dokument på intranätet. Det första steget planering omfattar momenten informationsklassning och riskanalys. Det andra steget genomförande omfattar momenten policy och regeldokument, organisation, hantering av tillgångar, personal och säkerhet, fysisk och miljörelaterad säkerhet, styrning av kommunikation och drift, styrning av åtkomst, anskaffning, utveckling och underhåll av informationssystem, hantering av informationssäkerhetsincidenter, kontinuitetsplanering i verksamheten och efterlevnad. Det tredje steget uppföljning är fokuserat på momentet uppföljning och rapportering av incidenter. Slutligen är steget förbättring fokuserat på momentet att utifrån resultat av uppföljning vidta förändringar under kontrollerade former.

2.4 Organisering av informationssäkerhetsarbetet vid KTH

Av KTH:s anvisning för informations- och IT-säkerhet framgår att ansvaret för informationssäkerheten följer linjeorganisationen och ligger hos de verksamhetsansvariga. Vid varje skola/motsvarande ska det finnas en ansvarig för informationssäkerheten. KTH ska också ha en gemensam central funktion för stöd, samordning och kontroll av informationssäkerheten vid lärosätet. Den centrala funktionen ansvarar för att informationssäkerheten kontrolleras regelbundet och att ledningen hålls informerad om säkerhetsläget.

[5] https://intra.kth.se/administration/informationssakerhet/ledningssystem-for-informationssakerhet-lis-1.521737

I januari 2017 fattade förvaltningschefen beslut att samla och integrera KTH:s IT- och informationssäkerhetsarbete på den centrala IT-avdelningen[6]. Syftet med beslutet var att förstärka arbetet resursmässigt och IT-chefen fick ansvaret för dess bemanning och organisering. En ny roll som chef för IT- och informationssäkerhet vid KTH inrättades och rollen är en kravställare på lärosätets IT- och informationssäkerhet. Oavsett sin placering på IT-avdelningen rapporterar chefen för IT- och informationssäkerhet funktionellt till rektor och är en del i KTH:s säkerhetsarbete. I november samma år fattade också rektor beslut att förstärka arbetet med planering och uppföljning vid funktionen för IT- och informationssäkerhet[7]. Beslutet innebar att funktionen utökades med två tjänster.

I början av detta år fattade IT-chefen beslut att KTH:s dataskyddsombud ska ingå i funktionen för IT- och informationssäkerhet vid KTH och delta i det löpande arbetet[8]. Syftet med beslutet är att uppnå synergieffekter när det gäller att långsiktigt möta verksamhetens behov och utmaningar inom dataskydd och informationssäkerhet.

3 Iakttagelser

Under granskningen har internrevisionen gjort flera iakttagelser inom det granskade området. Och nedan följer en beskrivning av de iakttagelser som vi anser är de mest väsentliga.

3.1 KTH ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete

KTH ska enligt gällande författningar[9] bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem. Och ledningssystemet ska vara utformat utifrån de risker och behov som identifierats och det ska omfatta all den hantering av information som KTH ansvarar för. Det är ledningen för universitetet som har ansvaret för att styra och skapa förutsättningar för informationssäkerhetsarbetet och uppgiften förutsätter kunskap om organisationens behov av och förutsättningar för säker hantering av information. I förslaget till nya föreskrifter införs krav att utformningen av informationssäkerhetsarbetet ska dokumenteras. Ett stöd för att identifiera och analysera de risker och behov som ska ligga till grund för utformningen av ett ledningssystem finns i MSB:s metodstöd. Där lämnas det förslag på fyra analyser som tillsammans ska tillgodose att informationssäkerhetsarbetet blir utformat med utgångspunkt i verksamhetens risker och behov. De analyser som föreslås är en omvärldsanalys, en verksamhetsanalys, en riskanalys och en gapanalys.

I granskningen kan vi se att av de föreslagna analyserna så har KTH bara genomfört riskanalysen vilket också kan bero på att en genomförd riskanalys är ett krav i förordningen om intern styrning och kontroll[10] som KTH ska följa. Vi kan också se att om KTH skulle valt att genomföra de övriga analyserna så skulle sannolikt flera av de iakttagelser vi gjort blivit upptäckta och fått en lösning. Med en omvärldsanalys skulle KTH fastställt vilka rättsliga krav som finns på informationshanteringen och på utformningen av informationssäkerhetsarbetet. Omvärldsanalysen skulle också kartlagt de externa intressenter som antingen påverkar eller påverkas av hur KTH styr sitt informationssäkerhetsarbete. En sådan kartläggning pågår nu enligt våra intervjuer inom ramen för utvecklingen av ett digitalt forskarstöd men kartläggningen bör omfatta alla verksamhetsområden. Med en verksamhetsanalys skulle KTH kartlagt och fastställt de befattningar eller enheter inom organisationen som antingen påverkar eller påverkas av hur KTH styr sitt informationssäkerhetsarbete. Resultatet av analysen skulle sedan ligga till grund för att fastställa roller och ansvar i informationssäkerhetsarbetet. Slutligen med

[6] Beslut om integration av KTH:s funktion för IT- och Informationssäkerhet i IT-avdelningen, V-2017-0091
[7] Beslut om förstärkt organisation av IT- och informationssäkerhet vid KTH, V-2017-0981
[8] Bemanning för IT-SMC V-2019-1149
[9] Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap samt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1)
[10] Förordning (2007:603) om intern styrning och kontroll

en gapanalys skulle KTH identifierat skillnaden mellan den nivå på informationssäkerhet som behöver uppnås och den faktiska nivån på säkerhet. Resultatet av analysen skulle vara ett stöd i prioriteringen av åtgärder och i utformningen av tydliga informationssäkerhetsmål.

Sammantaget visar våra iakttagelser att det är tveksamt om KTH i tillräcklig omfattning har analyserat de risker och behov som ska ligga till grund för utformningen av sitt informationssäkerhetsarbete.

3.2 KTH ska tydliggöra ansvar och tilldela nödvändiga befogenheter för informationssäkerhetsarbetet via ledningssystemet

KTH ska tydliggöra myndighetsledningens och den övriga organisationens ansvar avseende informationssäkerhetsarbetet. De befogenheter som arbetet med informationssäkerhet kräver ska fördelas och det gäller särskilt för den eller de som utses att leda och samordna arbetet. Stöd i utformningen av organisationen för informationssäkerhetsarbetet finns i MSB:s metodstöd. Och stödet förordar att resultaten från genomförda analyser ska vara ingångsvärden vid utformningen och särskilt viktiga är analyserna av de rättsliga kraven och av befattningar eller enheter inom organisationen.

Roller och ansvar i KTH:s informationssäkerhetsarbete framgår som tidigare nämnts i en anvisning[11] från 2014. Enligt anvisningen så ligger ansvaret för informationssäkerheten hos de verksamhetsansvariga utan att närmare beskriva vilka roller eller funktioner det avser och vad ansvaret innebär. Vidare ska varje skola/motsvarande ha någon som är ansvarig för informationssäkerheten men det framgår inte vilken uppgift och befogenhet rollen har. Anvisningen ger ingen beskrivning av vilket ansvar för informationssäkerheten som exempelvis gäller för rektor, skol- eller avdelningschefer, systemägare och enskilda medarbetare. Den otydlighet som råder i regleringen av ansvar och befogenheter bekräftas också i våra intervjuer då det framkommer en osäkerhet om vad det är gäller. KTH ska enligt anvisningen ha en gemensam, central funktion för stöd, samordning och kontroll av informationssäkerheten. Och den centrala funktionen har ansvar för att regelbundet kontrollera informationssäkerheten och att hålla ledningen informerad om säkerhetsläget. Med förvaltningschefens beslut 2017 samlades och integrerades KTH:s IT- och informationssäkerhetsarbete på IT-avdelningen. En ny roll som chef för IT- och informationssäkerheten inrättades och rollen är kravställare på KTH:s IT- och informationssäkerhet. Vi kan se att utifrån kraven i föreskriften och rekommendationer i metodstödet så är rollen som chef för IT- och informationssäkerheten inte tillräckligt tydlig och klarlagd. Det ska finnas beskrivet vilka beslutade arbetsuppgifter, vilka befogenheter samt vilken rapporteringsplikt som ingår i rollen. Och särskilt viktigt är beskrivningen av befogenheter och rapporteringsplikt så att det inte råder någon tveksamhet kring detta.

Sammantaget visar våra iakttagelser att ledningssystemet inte uppfyller kraven vad gäller att tydliggöra ansvar och tilldela nödvändiga befogenheter för informationssäkerhetsarbetet.

3.3 KTH ska samordna informationssäkerhetsarbetet via ledningssystemet

KTH ska genom sitt ledningssystem säkerställa att informationssäkerhetsarbetet bedrivs samordnat. Förslaget till nya föreskrifter ställer krav att informationssäkerhetsarbetet ska integreras med myndighetens befintliga sätt att leda och styra sin organisation. Stöd för en sådan integration av informationssäkerhetsarbetet finns i MSB:s metodstöd. Stödet beskriver hur utformade informationssäkerhetsmål – både kortsiktiga och långsiktiga kan underlätta att förstå, prioritera och genomföra aktiviteter som leder till ett systematiskt och förbättrat informationssäkerhetsarbete. Ingångsvärden i utformningen av informationssäkerhetsmål är dels resultaten från genomförda analyser, särskilt riskanalysen och gapanalysen, dels andra befintliga mål och visioner som har bäring på informationssäkerhet. Såväl de kortsiktiga och långsiktiga informationssäkerhetsmålen bör

[11] Anvisning för informations- och IT-säkerhet, gäller från och med 2014-02-01

harmonisera med sättet som organisationen vanligtvis arbetar med mål – exempelvis genom strategier och årliga verksamhetsplaner.

I granskningen kan vi se att KTH inte har formulerat några informationssäkerhetsmål för att leda informationssäkerhetsarbetet och försäkra sig om att arbetet är i överensstämmelse med övriga strategier och mål för verksamheten. Det har också framkommit i våra intervjuer att rutiner saknas för att systematisk beakta att informationssäkerhetsarbetet dels påverkar, dels låter sig påverkas av KTH:s övriga strategier och mål för verksamheten.

Sammantaget visar våra iakttagelser att ledningssystemet inte säkerställer att informationssäkerhetsarbetet bedrivs samordnat .

3.4 KTH ska regelbundet utvärdera och löpande utveckla ledningssystemet

KTH ska regelbundet utvärdera och löpande utveckla sitt ledningssystem för informationssäkerhet och det bör ske flera gånger per år. Förslaget till nya föreskrifter förtydligar att kraven på uppföljning och utvärdering avser myndighetens interna regler, arbetssätt och stöd för informationssäkerhetsarbetet. Utvärderingen bör ske minst en gång per år men bör också ske i samband med verksamhetsuppföljning, omorganisationer, förändrade rättsliga krav, förändringar rörande informationssystem samt vid hantering av extern aktör. Vidare bör utvärderingen ske genom interna kontroller, granskningar, interna och externa revisioner eller motsvarande och valet av metod för utvärdering bör tydliggöras av interna regler och arbetssätt. Stöd för att utforma utvärderingen av informationssäkerhetsarbetet finns i MSB:s metodstöd och är särskilt inriktat på arbetets och styrningens lämplighet, tillräcklighet och verkan.

I granskningen kan vi se att KTH:s beskrivning av att följa upp och utvärdera sitt ledningssystem för informationssäkerhet är mycket kortfattad. I avsnittet om informationssäkerhet som ingår i säkerhetspolicyn framgår att informationssäkerhetsarbetet ska regelbundet utvärderas och löpande utvecklas. Anvisningen för informationssäkerhet anger att ansvaret för att kontrollera informationssäkerheten regelbundet och hålla ledningen informerad ligger på chefen för IT-och informationssäkerhet och det ska ske årligen. Men det framgår inte vilken metod som då ska användas eller om det finns händelser som föranleder en mer frekvent uppföljning och rapportering. I samband med vår granskning så fick vi information att en redovisning av informationssäkerhetsläget till rektor var planerad efter sommaren. Vi kan dock notera att de iakttagelser vi har gjort i granskningen borde rimligen framkommit i samband med utvärderingar och då föranlett åtgärder.

Sammantaget visar våra iakttagelser att det förekommer brister i rutinerna för regelbunden utvärdering och löpande utveckling av ledningssystemet för informationssäkerhet.

3.5 KTH ska upprätta styrande dokument för informationssäkerhetsarbetet

KTH ska upprätta en informationssäkerhetspolicy, andra styrande dokument samt den dokumentation som i övrigt krävs för att kunna bedriva ett ändamålsenligt informationssäkerhetsarbete. Stöd för att utforma styrdokumenten som ska reglera informationssäkerhetsarbetet finns i MSB:s metodstöd. Ingångsvärden i utformningen är resultaten av genomförda analyser och särskilt viktiga är verksamhetsanalysen, analysen av rättsliga krav och gapanalysen. Utformningen av styrdokument ska också följa organisationens befintliga regelverk eller praxis för att utforma sina styrdokument.

I granskningen kan vi se att KTH har upprättat ett flertal styrdokument som berör informationssäkerhetsarbetet och de finns publicerade på intranätet. Sammantaget har vi tagit del av informationssäkerhetspolicyn som är en del i KTH:s säkerhetspolicy[12], fem stycken riktlinjer[13], fem

[12] Säkerhetspolicy V-2019-0452
[13] KTH:s närvaro i sociala medier 2012-02-20, Officiell webbpublicering 2005-03-01, Upprättande och drift av KTH:s internettjänster med användargenererat innehåll 2011-03-07, Spridning av information

stycken anvisningar[14] och ett tiotal mer detaljerade instruktioner som avser särskilda områden som e-post, behörigheter, säkerhetskopiering m.m. Vi noterar att någon översyn av riktlinjerna och anvisningarna inte har skett på flera år och i enstaka fall uppgår den tiden till drygt 15 år. Enligt uppgift så ska det pågå en översyn av styrdokumenten men vid granskningstillfället var det oklart hur lång arbetet fortskridit. Vi kan också notera att det inte framgår tydligt i styrdokumenten vem som är dess primära målgrupp, det vill säga till vilken roll eller grupper som dokumenten riktar sig till och förväntas efterleva dess innehåll. Att göra en sådan anpassning av styrdokumenten till olika målgrupper rekommenderar metodstödet i syfte att öka möjligheten till efterlevnad. Och metodstödet föreslår att styrdokumenten inriktas på målgrupper som exempelvis alla medarbetare, informationsägare eller systemägare, IT-verksamhet och informationssäkerhetsorganisationen.

Sammantaget visar våra iakttagelser att flera styrdokument har upprättats avseende informationssäkerhetsarbetet men dokumenten saknar en tydlig målgrupp och har inte regelbundet setts över.

3.6 KTH ska eftersträva en god säkerhetskultur

KTH ska eftersträva en god säkerhetskultur där alla i organisationen har kunskap om och förståelse för behoven av säker informationshantering. Förslaget till nya föreskrifter ställer krav att det ska finnas ett dokumenterat arbetssätt som säkerställer att medarbetarna har kunskap om säker hantering av information. I arbetet ingår att hålla medarbetarna informerade om relevanta interna regler och stöd, regelbundet och utifrån identifierat behov och medarbetarnas arbetsuppgifter utveckla och upprätthålla medarbetarnas kompetens avseende informationssäkerhet genom utbildning, informationsinsatser och övning, samt följa upp och utvärdera att interna regler, arbetssätt och stöd tillämpas på avsett sätt. Vidare bör arbetssättet säkerställa att medarbetare med särskilt utpekade funktioner i informationssäkerhetsarbetet har tillräcklig kunskap och kompetens om säker informationshantering för att kunna utföra sina arbetsuppgifter. Stöd i utformningen av utbildning och kommunikation i informationssäkerhetsrelaterade frågor finns i MSB:s metodstöd. Ingångsvärden i utformningen är resultatet av genomförda analyser, särskilt verksamhetsanalysen. Men viktigt är också organisationens mognad inom informationssäkerhet samt hur styrningen sker i organisationen av kompetensförsörjning och kommunikation.

Information till medarbetare om regler och stöd avseende informationssäkerhet förmedlar KTH som tidigare nämnts via två sidor på intranätet. Men i granskningen kan vi se att KTH inte erbjuder medarbetarna någon utbildning i informationssäkerhet, utöver en webbaserad utbildning i GDPR, för att utveckla och upprätthålla kompetensen i dessa frågor. Vi kan också se att det saknas formaliserade krav på kunskap och kompetens om säker informationshantering för medarbetare med särskilt utpekade funktioner i informationssäkerhetsarbetet.

Sammantaget visar våra iakttagelser att KTH informerar om regler och stöd avseende informationssäkerhet men att man inte erbjuder en regelbunden och behovsanpassad utbildning för sina medarbetare.

3.7 KTH ska klassificera sin information med stöd av en beslutad modell

I syfte att hantera hot och risker som rör informationssäkerheten ska KTH med stöd av en beslutad modell klassificera sin information med utgångspunkt i kategorierna konfidentialitet, riktighet och tillgänglighet. Klassificeringen ska göras i olika nivåer beroende på de konsekvenser som kan uppstå av ett bristande skydd inom respektive kategori. KTH ska utifrån resultatet av informationsklassningen

via webb 2005-03-01, Riktlinje om ansvar, befogenheter och skyldigheter för systemadministratör 2006-06-01

[14] Anvisning för E-post vid KTH 2011-10-11, Anvisning för informations- och IT-säkerhet 2014-02-01, Informationsklassificering för KTH 2015-01-01, Anvisning om dokumenthantering vid KTH 2013-04-03, Ansvarsförbindelse för användning av KTHs datorer, nät och systemresurser

och en genomförd riskanalys identifiera och vidta de åtgärder som krävs för att uppfylla behovet av skydd. Av den beslutade modellen ska det framgå vid vilka tidpunkter och i vilka situationer KTH genomför informationsklassning. Förslaget till nya föreskrifter ställer krav att det ska finnas ett dokumenterat arbetssätt som stöd för att genomföra informationsklassningen. Det framgår också att samma kriterier och nivåer som i riskanalysen bör användas för bedömningen av konsekvens vid informationsklassningen. För att underlätta informationssäkerhetsarbetet bör beslutade säkerhetsåtgärder grupperas i skyddsnivåer som är kopplade till konsekvensnivåerna i informationsklassningsmodellen. Stöd i utformningen av en informationsklassningsmodell finns i MSB:s metodstöd och ingångsvärden i utformningen är resultaten av genomförda analyser tillsammans med modellen för riskanalys.

Med en anvisning[15] från 2015 har KTH fastställt att informationen ska klassificeras i kategorierna åtkomstskydd (sekretess), riktighet och tillgänglighet. Av anvisningen framgår också att en klassificering kan göras separat i kategorin ytterligare krav. Och det kan vara aktuellt när det måste ställas krav som inte ryms i de föregående kategorierna och därför måste skrivas i klartext. I granskningen kan vi se att den obligatoriska informationen saknas om när och i vilka situationer KTH ska genomföra informationsklassningen. Vi kan också se att antalet nivåer eller klasser av skyddsbehov inte är enhetlig för de tre kategorierna. I kategorin riktighet är det tre nivåer eller klasser av skyddsbehov[16] men för kategorierna konfidentialitet och tillgänglighet är det i stället fyra nivåer eller klasser av skyddsbehov[17]. Vi kan också se att det inte är samma kriterier som i riskanalysen[18] som används vid bedömningen av konsekvenser. Enligt anvisningen ska bedömningen av konsekvenser av ett otillräckligt skydd bedömas sammantaget utifrån KTH som myndighet, anställda och studerande samt andra personer associerade med KTH, samarbetspartners och finansiärer, allmänheten och samhället i övrigt. Men vi kan se att den breda ansatsen i bedömningen har utelämnats i de instruktioner som finns för respektive kategori. Bedömningen av konsekvenser ska då vara inriktad på KTH och enskilda. Vidare så har inte KTH enligt uppgift genomfört den föreskrivna klassningen av sin information.

Sammantaget visar våra iakttagelser att det finns brister i KTH:s modell för klassificering av information och att det inte har skett någon informationsklassning.

[15] Anvisning Informationsklassificering för KTH gäller fr.o.m. 2015-01-01
[16] Grundläggande krav på riktighet, höga krav på riktighet och mycket höga krav på riktighet
[17] Grundläggande krav på åtkomstskydd, höga krav på åtkomstskydd, mycket höga krav på åtkomstskydd och särskilt höga krav på åtkomstskydd respektive grundläggande krav på tillgänglighet, höga krav på tillgänglighet, mycket höga krav på tillgänglighet och extremt höga krav på tillgänglighet
[18] Mindre, Måttlig, Betydande och Allvarlig

4 Sammanfattande slutsatser och rekommendationer

Syftet med granskningen har varit att kartlägga och bedöma om KTH:s informationssäkerhetsarbete sker med stöd av ett ledningssystem som följer gällande bestämmelser i förordning och föreskrifter.

Vår samlade bedömning är att KTH:s ledningssystem för informationssäkerhet i flera avseenden inte uppfyller kraven i gällande bestämmelser. De brister vi anser vara av störst betydelse är

- att myndighetsledningens och den övriga organisationens ansvar för informationssäkerhetsarbetet inte är tydliggjord,
- att nödvändiga befogenheter inte är tilldelade för de roller som arbetet med informationssäkerhet kräver och särskilt för den som utsetts att leda och samordna arbetet,
- att det inte är säkerställt att informationssäkerhetsarbetet bedrivs samordnat samt att det regelbundet utvärderas och löpande utvecklas,
- att det inte genomförs någon regelbunden utbildning rörande informationssäkerhet och
- att det inte har genomförts en klassning av informationen med utgångspunkt i konfidentialitet, riktighet och tillgänglighet utifrån vilka konsekvenser som kan uppstå av ett bristande skydd.

4.1 Rekommendation

Utifrån våra iakttagelser och slutsatser så väljer internrevisionen att lämna en överordnad rekommendation avseende ledningssystemet för informationssäkerhet.

- Internrevisionen rekommenderar KTH att se över ledningssystemet för informationssäkerhet och säkerställa att det följer gällande bestämmelser.

Magnus Jonsson	Camilla Ifvarsson	Maria Lindencrona
Internrevisor	Internrevisionschef	Internrevisor