

Peter Liljenstolpe

Högskoledirektör

# Riktlinjer för säkerhetsledning

## Inledning

KMH:s ledning ska, enligt 4 § myndighetsförordningen säkerställa att det vid högskolan finns en intern styrning och kontroll som fungerar på ett betryggande sätt, samt ansvarar inför regeringen för att bedriva ett aktivt säkerhetsarbete enligt gällande rätt.

Vidare ska KMH i enlighet med EU:s dataskyddsförordning samt lagen med kompletterande bestämmelser till EU:s dataskyddsförordning värna skyddet för fysiska personer vad gäller behandlingen av personuppgifter samt det fria flödet av sådana uppgifter där så är nödvändigt som ett led i den personuppgiftsansvariges myndighetsutövning eller är tillåtet genom lag eller annan författning.

Med anledning av att de statliga myndigheterna fått en tydligare roll i Sveriges totalförsvaret<sup>1</sup> men också för att KMH till största delen har ett relativt utsatt fysiskt läge, samt därtill en ökad globalisering och att KMH verkar på en internationell arena och för att allt fler av KMH:s informationstillgångar är digitala och därmed utsatta för potentiella cyberangrepp behöver KMH ha en tydlig säkerhetsledning och arbetet med att identifiera hot och säkra skydd intensifieras.<sup>2</sup>

KMH behöver därför tydliggöra KMH:s säkerhetsorganisation och säkerhetsledning så att den på ett adekvat sätt arbetar med fysisk säkerhet, personalsäkerhet, informationssäkerhet/cybersäkerhet.<sup>3</sup>

I detta ingår att sätta sig in i säkerhetsarbetet genom att skapa sig en förståelse kring förekomsten av eventuella skyddsvärden, genom att ställa krav på systematiskt säkerhetsarbete i organisationen och genom att vidta de åtgärder som behövs. Detta regleras i säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955). Här ställs krav vad gäller riskbedömningar, klassificering av uppgifter och skyddsåtgärder för säkerhetskänslig verksamhet. Lagen innehåller bestämmelser med vissa skyldigheter för den som bedriver säkerhetskänslig verksamhet, däribland att göra en säkerhetsskyddsanalys samt att planera och vidta de säkerhetsskyddsåtgärder som behövs, liksom att anmäla och rapportera sådant som är av vikt för säkerhetsskyddet.

---

<sup>1</sup> Lärosätenas roll i totalförsvaret (Pro Memoria från SUHF:s Expertgrupp för fastighets och säkerhetsfrågor), Dnr SU-850-0047-15.

<sup>2</sup> Jfr. Långsiktig plan för god myndighetsförvaltning 2021–2026, dnr. 22/181.

<sup>3</sup> Se not 2.

Utöver säkerhetsskyddsregleringen finns det i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap<sup>4</sup>, i förordningen (2015:1053) om totalförsvaret och höjd beredskap och i förordningen (2006:942) om krisberedskap och höjd beredskap bland annat reglerat att myndigheter ska göra risk- och sårbarhetsanalyser, att man ansvarar för sina egna informationshanteringssystem,<sup>5</sup> för att förebygga, motstå och hantera krissituationer samt att vissa IT-incidenter ska rapporteras.<sup>6</sup>

## Verksamhetsskydd och säkerhetsskydd

KMH är inte någon utpekad s.k. bevakningsansvarig myndighet och omfattas därför inte av sådan särregleringen. Inte heller omfattar KMH:s ordinarie verksamhet, enligt den säkerhetsskyddsanalys som gjorts, någon säkerhetsskyddskänslig verksamhet.

KMH hanterar inte säkerhetsskyddsklassificerade uppgifter. KMH omfattas inte av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Inte heller bedriver KMH verksamhet som är av betydelse för Sveriges säkerhet (dvs. Sveriges yttre säkerhet, Sveriges inre säkerhet, nationellt samhällsviktig verksamhet, Sveriges ekonomi eller skadegenererande verksamhet).

Däremot kan KMH, genom en överförd hotbild från annan organisation eller individ som samverkar med KMH eller genom deltagande i forskningsprojekt, komma att omfattas av säkerhetsskyddslagens bestämmelser.

Däremot omfattas KMH:s verksamhet av behov av ett gott s.k. verksamhetsskydd. Verksamhetsskyddet omfattar fysisk säkerhet, person-/personalsäkerhet samt informationssäkerhet inkl. IT-cybersäkerheten (med informationsklassning, riskanalys, kontinuitetsplanering och incidenthantering) och syftar till att säkerställa KMH:s förmåga och uppdrag att i Sverige långsiktigt utbilda och forska inom ämnesområdet musik. Verksamhetsskyddet avser såväl materiella som immateriella skyddsvärden. Ambitionsnivån med KMH:s verksamhetsskydd ska stå i proportion till dels riskbilden och till dels kostnader för skyddet.

Ett systematiskt arbete med verksamhetsskydd bedrivs lämpligen i huvudsak enligt samma systematik som gäller för säkerhetsskydd, då det senare är väl utvecklat och samordnat inom staten.

KMH:s läge längs ett centralt nattligt gångstråk, intill Stockholms stadion och tunnelbanan ökar högskolans lokaler och studenter/anställda sårbarhet. Lägg därtill att mycket av den information som lagras av KMH är angelägen att sprida i forsknings-/utbildnings- eller samverkanssyfte medan personuppgifter och annan känslig information är skyddsvärd och där lagring av dessa båda kategorier data ibland sker på samma ytor.

Å andra sidan finns ett behov av att inte överdimensionera verksamhetsskyddet, då KMH:s verksamhet kräver stor öppenhet. Vid sidan av den ordinarie utbildningen och forskningen samverkar KMH med ett stort antal aktörer. Undervisning av övnings elever, festivaler, forsknings sammankomster och redovisningar, konserter, workshops, föreläsningar och mässor utgör tillfällen då

---

<sup>4</sup> Vissa myndigheter är särskilt utpekade (hit hör inga lärosäten) och har ett ytterligare ansvar som så kallade bevakningsansvariga myndigheter. Det innebär att de är ålagda att planera och ha beredskap för samhällsstörningar. De ska till exempel genomföra nödvändig omvärldsbevakning, risk- och sårbarhetsanalyser, utbilda och öva berörd personal samt genomföra utvecklingsinsatser för att klara sina uppgifter vid höjd beredskap. De ska även anskaffa de förnödenheter och den utrustning som behövs för att klara uppgifterna vid höjd beredskap som inte kan vänta till en skärpt säkerhetspolitisk situation.

<sup>5</sup> Se vidare MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6)

<sup>6</sup> Se vidare MSB:s föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8).

deltagare från allmänheten, och som för KMH ofta är okända, befinner sig i högskolans lokaler.

## Definition av säkerhetsledning

Med säkerhetsledning avses den formella ledningen av utveckling, tillämpning och utvärdering på säkerhetsområdet för att säkerställa optimal enskild effekt, efterlevnad och samordning av de olika säkerhetsområdena såsom en del av helheten.

Även om myndighetschefen alltid är högsta ansvarig för säkerhetsledning utövas denna i vardagen från där det centrala säkerhetsansvaret ligger och innebär även upprätthållandet av en samlad bild av aktuellt säkerhetsläge inom den egna organisationen.

Ansvarsområden som konceptuellt och genomförandemässigt innefattas av säkerhetsledningen är bland annat:

- Riskhantering
- Hotanalyser med omvärldsbevakning
- Säkerhetsskyddsanalyser
- Utredningar
- Administration och samordning
- Stöd till kontinuitets- och krishantering
- Särskilda anvisningar i samband med större hot

## Organisation av säkerhetsledningen

För att leda säkerhetsarbetet vid KMH finns en virtuell säkerhetsorganisation som styrs av säkerhetsskyddschefen, tillika högskoledirektören.<sup>7</sup> Huvuduppgiften för denna organisation är att kontrollera så att KMH:s verksamhet bedrivs enligt gällande lagar och föreskrifter på området, vilket innebär att KMH ska bedriva ett adekvat säkerhetsarbete i förhållande till sin kärnuppgift: utbildning, forskning och samverkan.

Säkerhetsskyddschefen rapporterar i enlighet med 2 kap 7 § säkerhetsskyddslagen direkt till rektor.

Säkerhetsskyddschefens ansvar kan inte delegeras. Däremot är arbetsuppgifter inom den virtuella säkerhetsorganisationen kopplade till säkerhets- och säkerhetsskyddsansvar enligt följande delegerade till de funktioner som ingår i den virtuella säkerhetsorganisationen:

- till säkerhetsansvarig är delegerade de arbetsuppgifter som rör fysisk säkerhet, person- och personalsäkerhet.
- till informationssäkerhetsansvarig är delegerade de arbetsuppgifter som rör informationssäkerhet med undantag från de mer teknikbundna delarna som rör IT- och cybersäkerhet.

---

<sup>7</sup> Jfr. beslut om säkerhetsskyddschef (dnr 21/95) och virtuell säkerhetsorganisation för KMH (dnr 21/351)

- till IT/cybersäkerhetsansvarig är delegerade de mer teknikbundna delarna av informationssäkerhetsarbetet.
- till fastighetschefen är delegerade de arbetsuppgifter som av säkerhetsskyddschefen identifieras behöver åtgärdas i KMH:s campus Valhallavägen.
- till fastighetsansvarig vid campus Edsberg är delegerade de arbetsuppgifter som av säkerhetsskyddschefen identifieras behöver åtgärdas vid Edsbergs slott.

Den virtuella säkerhetsorganisationen har regelbundna avstämningar då man identifierar risker, hot och brister samt beslutar om åtgärder för att säkerställa KMH:s fysiska säkerhet, person-/personalsäkerhet och informationssäkerhet.

För att öka kontinuiteten gällande säkerhetsfrågor bör dessa vara en stående punkt på lämpliga mötesagendor, t.ex. vid högskoleförvaltningens chefsmöten för att fånga upp för säkerhetsområdet relevanta frågor.

Lokala riskbedömningar och kontinuitetsplanering ska göras inom ramen för akademiernas och förvaltningsavdelningarnas verksamhet, såsom identifiering av risker i samband med evenemang och samarbetsprojekt med vidhängande åtgärdsplaner som upprättas i ett särskilt digitalt formulär.

## Säkerhetsledning, styrdokument

Säkerhetsledningen ska ske utifrån följande centrala styrdokument:

- Riktlinjer för säkerhetsledning (dnr. 22/)
- Säkerhetsskyddsanalys (dnr. 22/)
- Riktlinjer för informationssäkerhet inkl. IT-/cybersäkerhet (dnr. 22/)
- Riktlinjer för fysisk säkerhet och person-/personalsäkerhet (dnr. 22/)
- Krisledningsplan (dnr. 22/xxx)
- Därtill finns bestämmelser om säkerhetsskyddschef (dnr 21/95) och virtuell säkerhetsorganisation för KMH (dnr 21/351).

KMH har även kontinuitetsplaner för hotscenarion, som utgör arbetsmaterial för KMH:s krisgrupp.

## Säkerhetsledning, kompetens

Samtliga chefer inom KMH bör ha gått en grundläggande introduktionskurs i säkerhetsskydd.

Därtill bör alla i den virtuella säkerhetsorganisationen ha en för sin roll adekvat utbildning inom sitt respektive säkerhetsområde.

Utbildningar och övningar bör ordnas kontinuerligt för att förbereda KMH:s anställda och studenter på olika hotscenarion.