HÖGSKOLAN
I HALMSTAD

Riktlinjer för informationssäkerhet vid Högskolan i Halmstad

Fastställd av högskoledirektören 2018-10-18, dnr L 2018/128

Bakgrund

Enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) är Högskolan skyldig att ha en informationssäkerhetspolicy och andra styrande dokument för att ändamålsenligt arbeta med Högskolan i Halmstads informationssäkerhet. Detta dokument likställs med sådan policy.

Högskolans information är en mycket viktig resurs. Detta dokument syftar till att belysa och vägleda, samt tydliggöra mål och ansvar för informationssäkerheten vid Högskolan. Policyn kompletteras med en årligen uppdaterad handlingsplan som beskriver aktuella åtgärder i informationssäkerhetsarbetet.

Information förekommer i många former – tryckt eller skriven, elektroniskt lagrad, skickad på papper eller elektroniskt, visad på film eller muntlig. All information vid Högskolan ska hanteras så att grundläggande krav på informationssäkerhet uppfylls.

Informationssäkerhetsarbetet syftar till att skydda Högskolans verksamhet, och se till att den kan utföras med god kvalitet. Informationssäkerhet är en grund för god kvalitet och god verksamhetsstyrning.

Informationssäkerhetsarbetet ska samordnas med övrigt säkerhetsarbete vid lärosätet och ska bedrivas förebyggande, riskbaserat, långsiktigt och kostnadseffektivt. Arbetet ska utföras på ett välstrukturerat sätt och med stöd av Högskolans ledning. En viktig grund är engagemang hos alla medarbetare.

Mål

Högskolan i Halmstads informationssäkerhetsarbete ska tillförsäkra att Högskolans information hanteras med upprätthållen

- riktighet – att informationen skyddas mot oönskad förändring,
- tillgänglighet – att informationen ska vara tillgänglig när den behövs för behöriga användare,
- konfidentialitet – att informationen skyddas så att den inte avsiktligt eller oavsiktligt görs tillgänglig för obehöriga.

Inom en femårsperiod bör

- Högskolans informationssäkerhetsarbete genomgå en extern granskning
- Högskolans personal genomgått personalutbildning inom informationssäkerhet vid minst ett tillfälle
- det finnas en intern organisation som arbetar med informationssäkerhetsfrågor

Roller och ansvar

Varje medarbetare och student ansvarar för den information hen hanterar, och för att självständigt följa de regler och riktlinjer som berör vars och ens uppgifter.

Informationssäkerhetsansvarig vid Högskolan i Halmstad är IT-chefen. Uppdraget består av att utveckla och följa upp informationssäkerhetsarbetet vid Högskolan. Dessutom kan informationssäkerhetsansvarig ställa krav på verksamhet som inte fullt ut följer Högskolans

regelverk kring informationssäkerhet. Informationssäkerhetsansvarig ska kontakta Högskolans krisorganisation när denne så finner lämpligt.

All information som hanteras vid Högskolan har en informationsägare. Informationsägare för information som finns i Högskolans IT-system är respektive systemägare. För mer information om systemägares ansvar, se Systemförvaltningsmodell för Högskolan i Halmstad. Informationsägare för övrig information är den person som skapat informationen. Informationsägaren ansvarar för att informationen hanteras korrekt, och i enlighet med lagar, förordningar och interna riktlinjer.

Skyddsåtgärder som avser hela Högskolan beslutas av rektor, eller av den som rektor utser. För IT-system ansvarar styrgrupperna inom respektive förvaltningsobjekt för att utreda och föreslå säkerhetsnivåer och skyddsåtgärder.

Alla personer verksamma som systemförvaltare eller liknande, och som har högre behörighet i system än vanliga användare vid Högskolan, ska ha undertecknat en särskild ansvarsförbindelse där dennes rättigheter och skyldigheter framgår.

Varje användare av IT-tjänster inom Högskolan i Halmstad ska ha och använda en personlig behörighet, anpassad efter sina arbetsuppgifter.

Då annan part utför tjänst eller uppdrag åt Högskolan där IT-tjänster eller IT-system utgör en viktig del, ska Högskolan genom avtal försäkra sig om att parten upprätthåller en informationssäkerhet som motsvarar Högskolans krav.

Hantering av information

All information är skyddsvärd men i olika omfattning. En avvägning mellan önskad skyddsnivå och effektivt utnyttjande av Högskolans resurser ska göras. En effektiv och säker hantering av information kräver att skyddsvärd information identifieras och relevanta risker bedöms.

Detta görs genom att all information som hanteras inom Högskolans centrala och administrativa IT-system genomgår en informationsklassning. Där definieras informationen och vilken skyddsnivå informationen ska omfattas av. Systemägare ansvarar för att detta sker. Informationsklassning kan därutöver göras för specifika verksamhetsgrenar/forskningsprojekt när verksamheten så kräver. Informationsklassning ska revideras vartannat år. Utifrån definierad skyddsnivå ställs olika krav på hur informationen får hanteras.

Riskbedömning med avseende på informationssäkerhet genomförs för den information där konsekvenserna av bristande riktighet, tillgänglighet eller konfidentialitet i informationsklassningen bedöms vara allvarlig eller betydande. Riskbedömning ska dessutom genomföras inför byte av IT-system, eller byte av driftform av IT-system. Ansvarig för att detta sker är systemägaren eller verksamhetsansvarig.

Efter riskbedömningen beslutas om vilka skyddsåtgärder som ska genomföras. Systemägare/verksamhetsansvarig ansvarar för att dessa åtgärder verkställs.

Vid upphandling och utveckling av IT-system och IT-tjänster ska krav på informationssäkerhet ingå i kravspecifikationen och avtalet.

Innan hantering (inkl. lagring) sker, ska det säkerställas att tänkt skydd för informationen kan och får användas för hanteringen, ur ett lag- avtals- och lämplighetsperspektiv. Beakta i synnerhet personuppgifter och forskningsdata, molnlagring samt hantering utanför EU/EES.

Högskolan ska ha testade rutiner för rapportering av informationssäkerhets- och personuppgiftsincidenter. Rapportering ska ske till Högskolans ledning och, i förekommande fall, till andra myndigheter som så kräver.

Varje anställd bör regelbundet (gärna vartannat år) genomgå utbildning kring informationssäkerhet för att säkerställa att den har tillräcklig kompetens på området för att kunna utföra sina arbetsuppgifter.

Högskolan ska ha rutiner för kontinuitetshantering för fall då Högskolans informationshantering drabbas av större störningar och avbrott. Minst vartannat år ska övningar genomföras för att testa och utveckla dessa rutiner.

Informationssäkerhetsarbetet vid Högskolan ska granskas regelbundet. Resultatet av granskningen ska redovisas till styrelse och rektor en gång/år. Eventuellt beslut om åtgärder baserade på granskningens resultat fattas av högskoledirektören. Ansvarig för granskning och rapportering är informationssäkerhetsansvarig.