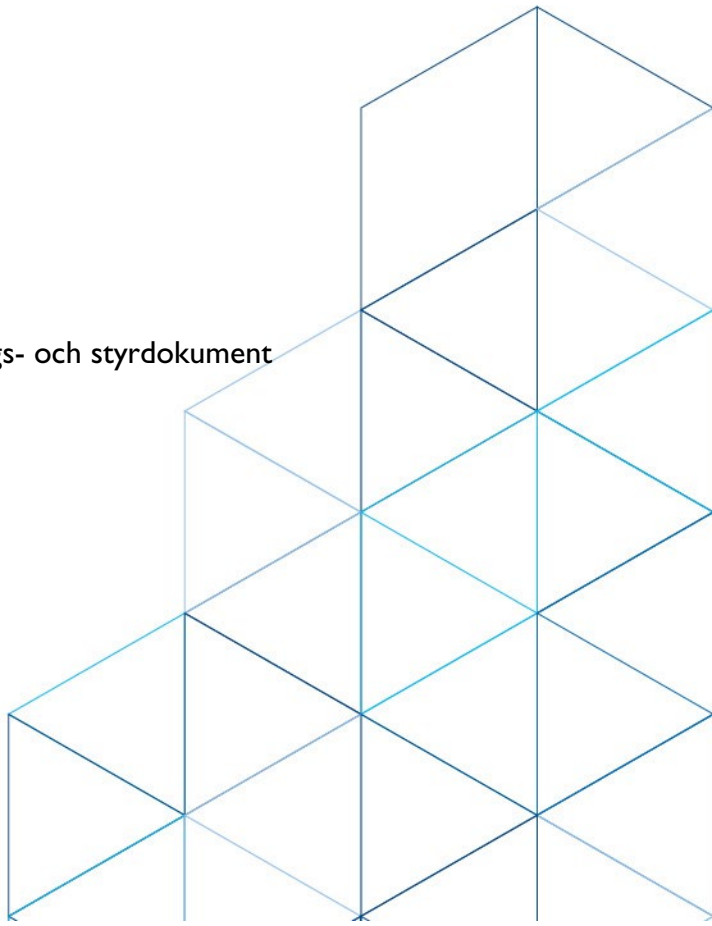
HÖGSKOLAN I HALMSTAD

Ledningssystem för IT, informations- och cybersäkerhet samt integritet

Dnr:	L 2026/22
Dokumenttyp:	Återkommande planerings- och styrdokument
Beslutsfattare:	Högskoledirektör
Beslutsdatum:	2026-10-12
Ansvarig avdelning:	IT-avdelningen
Dokumentansvarig:	Anna Frederiksen



hh.se

Syfte

Detta styrdokument anger hur Högskolan i Halmstad organiserar och följer upp sitt arbete kring IT-system, informations- och cybersäkerhet samt integritet. Detta arbete syftar till att ge Högskolans skyddsvärda tillgångar ett väl avvägt skydd.

Dokumentet riktar sig såväl till Högskolans chefer och andra personer med särskilda uppgifter inom området som till Högskolans medarbetare, då var och en ansvarar för att följa regler och rutiner kring den information man skapar och hanterar.

Bakgrund

God informations- och cybersäkerhet samt integritet blir allt viktigare i dagens samhälle. Att veta vilken information som hanteras inom Högskolan och att tillse att den är fri från otillbörlig påverkan är en förutsättning för god kvalitet och god verksamhetsstyrning.

Utformningen av detta ledningssystem bygger till stor del på de föreskrifter kring informationssäkerhet som Nationellt cybersäkerhetscenter ansvarar för.

Innehållet i detta dokument kompletterar och konkretiserar Högskolans Policy för säkerhet och de krav som ställs på Högskolans informations- och cybersäkerhet samt integritet i lagar, förordningar och direktiv från svenska myndigheter och från EU.

I detta dokument används hädanefter samlingsbegreppet ”informationssäkerhet” för informations- och cybersäkerhet samt integritet.

Utgångspunkter för Högskolans arbete med informationssäkerhet

Högskolans informationssäkerhetsarbete ska

- baseras på de risker och konsekvenser som identifierats för hela verksamheten,
- omfatta den information som Högskolan ansvarar för,
- dokumenteras på ett enkelt och strukturerat sätt i Högskolans metodstöd för informationssäkerhet, och
- grundas i inbyggt dataskydd och dataskydd som standard.

När säkerhetsåtgärder väljs ska resultatet från informationsklassning utgöra en viktig del av utgångspunkterna. Grundläggande säkerhetsåtgärder framgår av dokumentet Anvisningar för informationssäkerhet.

När personuppgiftsincident eller incident/avvikelse som påverkar Högskolans informationssäkerhet inträffat ska grundorsaker till händelsen utredas även av dataskyddsombud respektive IT-avdelningen och åtgärder vidtas för att motverka att liknande incidenter och avvikelser inträffar på nytt.

Verksamhetens behov av kontinuitet vid behandling av information under incidenter och kriser ska identifieras så att avvägda krav kan ställas på Högskolans leverantörer.

Organisation och ansvar

Högskolans ledning är ytterst ansvarig för informationssäkerheten vid Högskolan och ställer kraven på Högskolans ledningssystem för informationssäkerhet. Ledningen ska säkerställa att Högskolan efterlever lagar och regler inom området och främja en säkerhetsmedveten kultur inom Högskolan.

Högskolans chefer ansvarar för att deras respektive verksamhet följer de krav som ställs på Högskolans säkerhet. Kraven kan ställas av såväl externa parter som parter inom Högskolan. Ofta är chefer systemägare för de IT-system som används inom respektive ansvarsområde.

Ansvarsroller inom området

Högskolans dataskyddsombud ställer krav på, följer upp och granskar oberoende Högskolans arbete utifrån dataskyddsförordningen. Förutom behovsstyrt stöd ska dataskyddsombudet tillhandahålla instruktioner, checklistor och annat stödmaterial som beskriver de krav som ställs på Högskolan genom dataskyddsförordningen.

Dataskyddsgruppen, bestående av dataskyddsombud och högskolejurister, informerar och ger stöd till medarbetare och studenter i frågor som rör dataskyddsförordningen samt granskar avtal inom området. Dataskyddsgruppen rapporterar till högskoledirektör.

Högskolans IT- och informationssäkerhetssamordnare ansvarar för att samordna och administrera Högskolans systematiska informationssäkerhetsarbete. I detta ingår även att tillse att övriga rollinnehavare har tillgång till det stöd som de behöver för att upprätthålla kraven i detta dokument samt ställa krav på, följa upp och granska informationssäkerhetsarbetet vid Högskolan.

Systemägare har i normalfallet budgetansvar för ett IT-system och fattar, i samråd med IT-chef, nödvändiga beslut kring IT-systemet. Ofta är systemägaren också informationsägare för aktuellt IT-system.

Systemförvaltare har ofta högre behörighet i ett IT-system än övriga användare. Systemförvaltaren håller kontakten med systemleverantören och IT-avdelningen kring systemet.

Informationsägare har kontroll över och kunskap om vilken information som återfinns inom IT-system.

IT-avdelningen är den enhet som främst lämnar stöd till övrig verksamhet kring informations- och IT-säkerhet.

Ansvarsuppgifter

Systemägare ansvarar för att:

- säkerställa (tillsammans med IT-avdelningen och leverantör) att systemet
  - fungerar med samverkande IT-system och i Högskolans centrala IT-miljö
  - över tid uppfyller Högskolans krav baserat på verksamhetens behov och IT-avdelningens driftsäkerhetskrav
- ställa krav på
  - grundläggande utbildning för användare av systemet
  - drift, säkerhet, tillgänglighet och tillförlitlighet
- se till att

    - användarstöd finns tillgängligt för användare av systemet
    - systemet kan användas på avsett vis genom anpassning av arbetssätt och funktionalitet
    - lagar, förordningar, avtal, interna regelverk och överenskommelser följs
- besluta om
    - nyutveckling, vidareutveckling och avveckling av systemet och dess innehåll. Besluten ska baseras på dels verksamhetens krav, dels krav som rör säkerhet och andra krav från omvärlden och fattas i samråd med IT-avdelningen
    - vem som ska vara systemförvaltare
- teckna nödvändiga avtal för systemet

Systemförvaltare ska:

- ha adekvat kompetens inom informationssäkerhet och dataskydd
- uppdatera Högskolans metodstöd för informationssäkerhet med nödvändig information kring systemet och dess informationsinnehåll
- tillse att information om systemet, dess funktioner och nytta i verksamheten, finns tillgänglig för användarna
- tillse att önskemål och krav (såsom rätten till information eller rättelse) baserade i dataskyddsförordningen uppfylls
- delta i informationsklassning, riskbedömning och konsekvensbedömning enligt dataskyddsförordningen kring systemet
- rapportera eventuella informationssäkerhetsincidenter och personuppgiftsincidenter kring systemet

Informationsägare ansvarar för att:

- information hanteras korrekt och enligt Högskolans styrdokument
- informationsklassning, riskbedömning och konsekvensbedömning enligt dataskyddsförordningen utförs
- besluta om vilka åtgärder baserade på riskbedömning eller konsekvensbedömning som ska genomföras inom ramen för Högskolans verksamhetsplanering och vilka risker som ska accepteras
- besluta om vilken information som flyttas i integrationer mellan IT-system, tillsammans med dataskyddsombud och IT-avdelningen
- erforderligt skydd för informationen finns och att säkerheten uppfyller ställda och rättsliga krav.

IT-avdelningen ska tillhandahålla instruktioner, checklistor och annat stödmaterial som beskriver:

- de kompetenskrav som ställs på övriga rollinnehavare
- nyanskaffning av IT-resurser
- informationsklassning
- riskbedömning ur informationssäkerhetsperspektiv
- rapportering av IT-incidenter.

Krav vid informationshantering

Material som skapats inom ramen för Högskolans verksamhet ska skyddas från obehörig åtkomst och ändring. Det ska vara möjligt för Högskolan att ge andra behöriga medarbetare på Högskolan tillgång till materialet om medarbetaren blir hastigt onåbar eller slutar sin tjänst.

Resultatet av informationsklassning och riskbedömning ställer krav på hur information ska hanteras. IT-chef eller informationssäkerhetssamordnare får besluta om undantag gällande hanteringskraven.

I de fall riskbedömningens resultat kräver att information krypteras ska framtidssäkrad kryptering användas.

Informationsklassning

Information som hanteras inom Högskolans verksamhet har olika känslighetsnivåer, vilka ställer olika krav. För att veta vilken nivå som gäller för respektive informationstyp måste en informationsklassning göras. Informationsklassning ska utföras inför nya och förändrade behandlingar samt när krav från omgivningen eller relevanta arbetssätt förändras.

Riskbedömning

Riskbedömning ska utföras inför nya behandlingar och IT-system och vid förändringar av befintliga behandlingar (exempelvis byte av driftform). Vid riskbedömning ur informationssäkerhetsperspektiv ska alltid hänsyn tas till informationens typ och informationsklassningsnivå. Används IT-system eller -tjänst för hantering av informationen ska till exempel även driftform, åtkomstmetod och systemets tekniska uppbyggnad bedömas.

Incidentrapportering

En IT-incident är en eller flera relaterade och identifierade händelser som kan skada Högskolans tillgångar eller få negativa konsekvenser för verksamheten.

En personuppgiftsincident är en incident som leder till oavsiktlig eller olaglig förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter. Anmälan ska göras vid de fall då konsekvenserna av incidenten kan innebära risk för de registrerades fri- och rättigheter.

Högskolan är skyldig att snabbt vidarerapportera allvarliga IT- och personuppgiftsincidenter till andra myndigheter. För att möjliggöra detta ska var och en som upptäcker sådana rapportera in dessa.

Granskning och uppföljning

Informationssäkerhetsarbete är en kontinuerlig process som ska utvärderas regelbundet. För att få en struktur i utvärderingsarbetet finns en årlig planering där mycket av arbetet utförs i metodstödet för informationssäkerhet. Granskning och uppföljning av informationssäkerhet samordnas med den samlade riskbedömningen, verksamhetsuppföljning och med övrigt säkerhetsarbete.

En årlig rapport till Högskolans ledning ska tas fram. Av rapporten ska minst framgå:

- säkerhetsåtgärder som Högskolan eller dess leverantörer genomfört under året för att höja respektive behålla nuvarande nivå på informationssäkerheten
- större händelser i omvärlden som kan påverka Högskolans informationssäkerhet
- antal inträffade incidenter under senaste året samt hur man arbetat för att minska risken för upprepning
- resultat från riskbedömningar och självvärderingar, såsom mognadsdialogen och cybersäkerhetskollen, och eventuella externa granskningar
- planerade införanden av större säkerhetsåtgärder kommande år.