HÖGSKOLAN
I SKÖVDE
Rektor

BESLUT

2021-03-09 Dnr HS 2021/202

Informationssäkerhetspolicy

Beslut

Härmed fastställs *Informationssäkerhetspolicy* för Högskolan i Skövde att gälla från den 9 mars 2021. Policyn ersätter därmed det tidigare dokumentet *"Riktlinjer för informationssäkerhet vid Högskolan i Skövde"* från 2015-03-01 (dnr HS 2015/182). Informationssäkerhetspolicyn upphäver även *Säkerhetspolicy för Högskolan i Skövde* från 2016-03-29 (dnr HS 2016/301).

Motivering

Högskolan, i egenskap av myndighet, ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete i enlighet med Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:6. Informationssäkerhetspolicyn är en del av informationssäkerhetsarbetet på Högskolan.

Beslutet är fattat vid rektors beslutsmöte 9 mars 2021 efter föredragning av säkerhetsansvarig/informationssäkerhetssamordnare Emelie Dolfe. För att se vilka som närvarat vid föredragning och slutgiltig handläggning, utan att delta i avgörandet, hänvisas till aktuellt protokoll från rektors beslutsmöte.

Lars Niklasson

Emelie Dolfe

Sändlista

Rektorsfunktionen
Rektors kansli
Prefekter
Avdelningschefer vid institution
Verksamhetsstödets chefer
Fakultetsnämnden
Studentkåren
SACO-S
OFR-S

HÖGSKOLAN
I SKÖVDE

Informationssäkerhetspolicy

Informationssäkerhetspolicyn är fastställd av rektor 9 mars 2021 och träder i kraft samma datum.

Dnr HS 2021/202

1 Inledning

Denna policy gäller för informationssäkerhet på Högskolan i Skövde (Högskolan). Styrelsen är ytterst ansvarig för informationssäkerheten vid Högskolan. Utförandet av uppgifter, beslutsfattande och verkställighet kan delegeras, däremot inte ansvaret.

För Högskolan är god informationssäkerhet ett förhållningssätt som ska genomsyra hela Högskolans verksamhet. Det omgivande samhället såväl som studenter och medarbetare ska känna tillit till att information finns tillgänglig när den behövs, att den är korrekt och att den inte kommer i orätta händer

Ökad digitalisering medför en ökad exponering av Högskolans informationstillgångar. Därmed är det angeläget att utvecklingen av skyddet för Högskolans informationstillgångar följer digitaliseringsutvecklingen. Det finns i grunden inget motsatsförhållande till ökad digitalisering och informationssäkerhet. Dock måste informationssäkerhetsarbetet utvecklas parallellt med ökad digitalisering.

På Högskolan är arbetet med att upprätthålla en god informationssäkerhet inom vår verksamhet nödvändigt, då det arbetet ligger som grund för att våra verksamheter ska uppnå sina verksamhetsmål och för att studenter, uppdragsgivare, samarbetspartners, anställda samt allmänheten ska känna förtroende för oss.

Policyn är ett övergripande dokument som redovisar ledningens inriktning med informationssäkerhet samt hur ansvaret i dessa frågor är fördelat på Högskolan. Informationssäkerhetspolicyn ska ses över regelbundet. Informationssäkerhetssamordnaren ansvarar för översynen.

2 Om informationssäkerhet

Högskolan hanterar en mängd information med varierande värde för individ, verksamhet och det omgivande samhället. Information utgör en grund i Högskolans verksamhet, vilket innebär att vi måste ha en adekvat skyddsnivå för vår information.

Information och de resurser som används för att hantera information benämns informationstillgångar. Informationssäkerhet är ett arbete för att skydda informationstillgångar och definieras som bevarande av informationens *konfidentialitet, riktighet* och *tillgänglighet* (SIS teknisk rapport, SIS-TR 50:2015).

Informationssäkerhet utgår från följande principer:

- **Konfidentialitet:** Skydd mot obehörig insyn. Att information inte tillgängliggörs eller avslöjas för obehörig, exempelvis innehåll i tentamina, forskningsdata eller övrig administrativ information.
- **Riktighet:** Skydd mot oönskad förändring. Att information är korrekt, aktuell, fullständig och inte på något sätt manipulerad eller förstörd, exempelvis att forskningsdata, betygsunderlag och viktig administrativ information inte förvanskas och/eller förstörs.
- **Tillgänglighet:** Åtkomst för behörig person vid rätt tillfälle. Att verksamheten har tillgång till information och IT-tjänster när det behövs.

Informationssäkerhet omfattar områdena administrativ säkerhet och teknisk säkerhet. Informationssäkerhet är ett förhållningssätt som inte bara begränsas till system, utan även gäller för olika former av informationsbärare, som exempelvis papper, tal mellan individer, bild och annan lagringsmedia.

För Högskolan är det viktigt och nödvändigt att våra olika verksamheter verkar i en miljö med ett noga avvägt skydd för den information som Högskolans institutioner och avdelningar förfogar över.

Informationssäkerhet uppnås inte enbart genom att införa olika tekniska säkerhetsåtgärder utan det krävs ett grundläggande systematiskt arbete med en tydlig styrning av planering, införande, kontroll och uppföljning. Som helhet ska informationssäkerhetsarbetet anpassas till en nivå som är lämplig för verksamhetens behov, vilket i Högskolans fall innebär samverkan och aktivt deltagande, från högsta ledning till avdelningsnivå samt varje enskild individ.

3 Strategiska mål

Allt arbete inom informationssäkerhet på Högskolan utgår från denna informationssäkerhetspolicy. Policyn gäller all verksamhet och alla medarbetare som använder Högskolans information. Informationssäkerheten implementeras delvis genom Högskolans *Ledningssystem i informationssäkerhet (LIS)*. Underliggande styrdokument syftar till att ge vägledning till chefer och övriga medarbetare i genomförandet.

Målet är att Högskolans information ska hanteras och lagras korrekt och säkert, utifrån behov, lagstiftning, förväntningar och omvärld.

Högskolans informationssäkerhetsarbete bygger på nationella bestämmelser (exempelvis Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet; MSBFS 2020:6, offentlighets- och sekretesslagen (2009:400) och dataskyddsförordningen) samt internationella standarder som SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 om ledningssystem för informationssäkerhet, vilka utgår ifrån:

- Att information hanteras och lagras enligt gällande bestämmelser och efter identifierat behov.
- Att information klassificeras utifrån konfidentialitet, riktighet och tillgänglighet.
- Att information som behandlas också tydligt dokumenteras.
- Att nödvändig information lagras enligt lagringsminimeringsprincipen och uppgiftsminimeringsprincipen.
- Att säkerhetsåtgärder vidtas utifrån konsekvensbedömning.
- Att tydlig ansvarsfördelning finns och efterlevs.
- Att informationssystem och verksamhetssystem, där det är möjligt, är integrerat, effektivt och processbaserat.

För Högskolan är det viktigt att information hanteras korrekt och säkert. Förhållningssättet är en del av Högskolans professionalism. Det uppnås genom att samtliga anställda eftersträvar att ha kunskap att kunna särskilja om information är skyddsvärd eller inte. Som stöd till samtliga verksamheter i detta arbete har Högskolan inrättat en säkerhetsorganisation (dnr HS 2020/829).

4 Ansvar och roller

Ansvaret för informationssäkerhetsarbetet följer lärosätets linjeorganisation, arbets- och delegationsordningar, vilket innebär att styrelsen har det yttersta ansvaret för informationssäkerheten på Högskolan i Skövde. Nedanstående roller har ett specifikt uppdrag och ansvar inom informationssäkerhet.

Rektor är som myndighetschef ansvarig för verkställandet av informationssäkerhetsarbetet på Högskolan.

Högskoledirektören är, på delegation från rektor, övergripande ansvarig för verkställandet av informationssäkerhetsarbetet på Högskolan.

IT-chefen (chef för avdelningen för service, IT och säkerhet, SITS) ansvarar för Högskolans strategiska utveckling inom IT och för att denna är i linje med Högskolans utvecklingsplan. IT-chefen är även ansvarig för genomförandet av Högskolans systematiska informationssäkerhetsarbete.

Informationssäkerhetssamordnaren ansvarar för samordningen av informationssäkerhetsarbetet på Högskolan och rapporterar till Högskolans styrelse och till rektorsfunktionen vad gäller informationssäkerhetsarbetet.

Dataskyddsombudet ansvarar för att övervaka efterlevnaden av dataskyddsförordningen och av Högskolans strategi för skydd av personuppgifter.

Chefer vid Högskolan ansvarar för informationssäkerhetsarbetet inom sin respektive verksamhet. I ansvaret ingår att, med stöd av informationssäkerhetsansvarig och Högskolans säkerhetsorganisation, regelbundet bedöma risker, konsekvenser och åtgärder för den egna verksamheten.

Medarbetare ansvarar för att följa Högskolans regler och riktlinjer gällande informationssäkerhet. I ansvaret ingår att själv bedriva informationssäkerhetsarbete i enlighet med ledningssystemet för informationssäkerhet, samt relevanta riktlinjer. Varje medarbetar ansvarar för att rapportera incidenter rörande informationssäkerhet.

Fastighetsansvarig ansvarar för att Högskolans lokaler uppfyller de säkerhetskrav som chefer har formulerat genom sitt informationssäkerhetsarbete för respektive verksamhet.

Externa parter. Den som tecknar ett avtal med en extern part ansvarar, i de fall det är relevant, för att avtalet även hänvisar till Högskolans relevanta styrdokument om informationssäkerhet, samt att den externa parten ges möjlighet att efterleva Högskolans regler.

Studenter ansvarar för att ta del av och följa Högskolans regler och riktlinjer gällande informationssäkerhet.

5 Avvikelser och undantag

Avvikelser och undantag från denna informationssäkerhetspolicy kan endast beslutas av rektor. En sådan begäran av undantag ska vara skriftlig. Ett beslut om undantag ska dokumenteras.

6 Ikraftträdande

Denna informationssäkerhetspolicy är fastställd 9 mars 2021. Policyn ersätter därmed det tidigare dokumentet "Riktlinjer för informationssäkerhet vid Högskolan i Skövde" från 2015-03-01 (dnr HS 2015/182), samt även dokumentet "Säkerhetspolicy för Högskolan i Skövde" från 2016-03-29 (dnr HS 2016/301).