HÖGSKOLAN
I SKÖVDE

Högskoledirektör

Beslut

2015-03-01

Dnr HS 2015/182

Revidering av riktlinjer för Informationssäkerhet vid Högskolan i Skövde

Härmed fastställs reviderad version av informationssäkerhetspolicyn vid Högskolan i Skövde. I samband med detta byter styrdokumentet namn till "*Riktlinjer* för Informationssäkerhet vid Högskolan i Skövde".

Beslut har fattats efter föredragning av Campuschef Magnus Littmarck,

Johan Almer

Kopia till

Högskoleledningen
Fakultetsnämnden
Prefekter
Förvaltningens chefer
Studentkåren
Arbetstagarorganisationerna (OFR-S och SACO-S)

HÖGSKOLAN
I SKÖVDE

Dokumenttyp	Datum	Utgåva	Sida
Riktlinjer	2015-03-01	0.2	1 (5)

Revideringsdatum	Diarienummer
	HS 2015/182

Riktlinjer för informationssäkerhet vid Högskolan i Skövde

Innehåll

Utgåvehistorik för dokumentet

Utgåva	Datum	Kommentar
0.1	2015-01-15	Första remissutgåva
0.2	2015-03-01	Fastställd utgåva

Riktlinjer för Informationssäkerhet vid Högskolan i Skövde

Dessa riktlinjer ersätter tidigare informationssäkerhetspolicy för Högskolan i Skövde (HS 2014/19).

Övriga styrande dokument är Myndigheten för Samhällsskydd och Beredskap (MSB) föreskrifter att statliga myndigheter ska tillämpa ett ledningssystem för informationssäkerhet, se MSBFS 2009:10. I denna föreskrift sägs bl a att myndigheten skall bedriva sitt säkerhetsarbete enl. följande etablerade svenska standarder

- Ledningssystem för informationssäkerhet – Krav (SS-ISO/IEC 27001: 2006)
- Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005)[1]

Ledningens viljeinriktning – varför är det viktigt med informationssäkerhet?

Högskolan i Skövde behöver skydda sin information på ett sätt som passar organisationens verksamhet. Det är nödvändigt för att vi ska uppnå verksamhetsmålen och för att studenter, uppdragsgivare, samarbetspartners, allmänhet och anställda ska känna förtroende för oss. Därför arbetar vi aktivt med informationssäkerhet så att all vår information alltid har rätt **konfidentialitet**, är **riktig** och **tillgänglig** samt i särskilda fall **spårbar**.

Vad behöver vi göra - hur ska viljeinriktningen uppnås?

Vi har valt ett gemensamt och strukturerat sätt att arbeta med informationssäkerhet som bygger på den svenska och internationella standarden LIS (ledningssystem för informationssäkerhet). Med stöd av LIS får vi rätt nivå på informationssäkerheten samtidigt som våra anställda får ett stöd i sitt dagliga arbete. Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av vår verksamhet och alla de informationstillgångar som vi äger eller hanterar. Personalen ska få fortlöpande utbildning för att förstå hur informationssäkerhetsarbetet fungerar.

Ansvar

Övergripande ansvar

Högskolestyrelsen och rektor är formellt ytterst ansvariga för Högskolans informationssäkerhet. Högskolans högskoledirektör har, efter beslut om delegation från rektor, det övergripande ansvaret för skolans informationssäkerhet, (Dnr: HS2010/57-114) och därmed också för upprättandet och underhållet av denna policy.

För centrala och gemensamma system ska särskild systemägare utses av högskoledirektören. Systemägaren ansvarar för informationssäkerheten i respektive system eller resurs.

[1] *Standarderna har sedan MSB:s föreskrift publicerades uppdaterats till senare utgåva, vilket ännu inte slagit igenom i föreskriften.*

Institutionernas och förvaltningens ansvar

Ansvaret för informationssäkerhet följer verksamhetsansvaret: Prefekt, avdelningschef eller motsvarande har ansvaret för informationssäkerheten vid respektive institution och avdelning.

Högskolans IT-avdelning och Campusavdelning utgör kompetenscentra i informationssäkerhetsfrågor och ska utarbeta riktlinjer samt ge råd och stöd till institutioner och avdelningar i deras säkerhetsarbete.

Användarnas ansvar

Alla anställda och studenter har ett ansvar för att säkerheten fungerar. Den som upptäcker brister i informationssäkerheten måste uppmärksamma sin chef och enligt fastställda rapporteringsrutiner. Alla medarbetare måste också rapportera händelser som kan göra att våra informationstillgångar utsätts för risker.

Alla användare ska underteckna särskild ansvarsförbindelse som tydliggör deras ansvar.

Begrepp

Begreppsförklaringar (bygger på definitioner hämtade från "Terminologi för informationssäkerhet, SIS HB550 utgåva 3, SIS förlag) samt *i kursiv stil Högskolan i Skövdes komplettering*:

- **Informationstillgångar** är allt som innehåller information och allt som bär på information.
- **Informationssäkerhet** är säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet, tillgänglighet *och spårbarhet.*
- **Konfidentiell information** får inte nås av eller avslöjas för någon obehörig. Oftast gäller det innehållet i en informationstillgång men ibland är även tillgångens existens hemlig.
- **Riktig information** innebär att informationen inte obehörigen får förändras, inte av misstag och inte på grund av en funktionsstörning.
- **Tillgänglig information** innebär att informationen går att utnyttja av behörig användare när det behövs och så mycket som det behövs.
- ***Spårbar information*** *innebär att det går att utröna vem som har haft tillgång till och/eller förändrat information och vid vilken tidpunkt detta skedde.*
- Ett **ledningssystem för informationssäkerhet (LIS)** är ett verktyg som hjälper oss att upprätta, införa, driva, övervaka, granska, underhålla och förbättra den önskade nivån på informationssäkerhet i vår organisation.

Ansvar för riktlinjerna och giltighet

Högskoledirektören är ansvarig för riktlinjerna, vilka årligen ska ses över och revideras.
Detta dokument gäller till 2015-12-31.