Intendentur och service
Chef Fredrik Nilsson

STYRDOKUMENT
Diarienummer: GIH 2018/245
Datum: 2018-04-24
Beslutat av: Rektor
Beslutsdatum: 2018-06-13
Ersätter Dnr: Ö 2013/219
Giltighetstid: Tillsvidare

Informations-säkerhetspolicy

INFORMATIONSSÄKERHETSPOLICY FÖR GYMNASTIK- OCH IDROTTSHÖGSKOLAN

Informationssäkerhetspolicy

Policyn gäller för studenter, anställda och uppdragstagare vid Gymnastik- och idrottshögskolan i Stockholm

Information förekommer idag i många olika former, tryckt, skriven, analog och digital, oavsett form bör den alltid ha ett godtagbart skydd.

Informationssäkerhet uppnås genom att lämpliga skyddsåtgärder införs, inkluderande riktlinjer, processer, organisation samt program- och maskinvarufunktioner.

Dessa åtgärder behöver utformas, införas, övervakas, granskas och förbättras för att säkerställa att verksamhetens specifika säkerhets- och verksamhetsmål uppnås. Detta bör göras samordnat med andra verksamhetsprocesser.

För att säkra informationen vid lärosätet krävs en helhetssyn på informationssäkerheten mot bakgrund av att befintliga informationssäkerhetslösningar är av avgörande betydelse för möjligheten att nyttja informationstekniken.

Denna policy syftar till att belysa, vägleda samt tydliggöra mål och ansvar för informationssäkerheten vid lärosätet. Utgångspunkten är att lärosätets information är en mycket viktig resurs och om informationen inte hanteras på rätt sätt kan lärosätets verksamhet, goda namn och rykte äventyras.

Säker information utgör också en förutsättning för att lärosätet skall kunna fullgöra uppdraget med att tillhandahålla utbildning, bedriva forskning samt att samverka med det omgivande samhället.

Informationssäkerhetsarbetet skall ske med utgångspunkt från ett förebyggande, långsiktigt och kostnadseffektivt förhållningssätt där genomförandet skall ske välstrukturerat och har ett tydligt stöd från lärosätets ledning.

Förankring av och medvetenhet hos varje medarbetare utgör själva grunden i säkerhetsarbetet. Lärosätet skall sörja för att medarbetarna får tillgång till lämplig utbildning och kontinuerlig kompetenshöjning inom området.

Med informationssäkerhet avses såväl administrativ säkerhet som teknisk säkerhet. Administrativ säkerhet avser säkerhet vid behandling och/eller lagring av information. Med teknisk säkerhet avses säkerhet genom tekniska lösningar. Teknisk säkerhet kan uppdelas i fysisk säkerhet och IT-säkerhet. Fysisk säkerhet avser fysiskt skydd för t.ex. datamedia. Begreppet IT-säkerhet avser säkerhet för information i informationsbehandlande tekniska system. IT-säkerhet kan därtill uppdelas i datasäkerhet och kommunikationssäkerhet. Datasäkerhet avser skydd av data och IT-system mot t.ex. obehörig åtkomst. Kommunikationssäkerhet avser säkerhet i samband med överföring av data.

Ansvar och organisation

Det övergripande ansvaret för lärosätet har dess styrelse och rektor, vilket inbegriper ansvaret för lärosätets informationssäkerhet.

Rektor utser ansvarig för samordningen av informationssäkerheten. Ansvaret följer därefter den vid lärosätet gällande delegationsordningen.

Varje medarbetare och student ansvarar för den egna tillämpningen av gällande policy, riktlinjer och regler inom det egna ansvarsområdet.

Målsättning

Målet för informationssäkerheten är att inom lärosätet skydda dess information mot olika hot och att skapa ett effektivt skydd genom att tillförsäkra,

- **riktighet** – informationen skall vara oberörbar i den meningen att den skyddas mot oavsiktlig och avsiktlig förvanskning,
- **tillgänglighet** – informationen skall vara tillgänglig för behörig användare efter dennes behov på förväntat sätt och i önskad omfattning,
- **sekretess** – informationen skall skyddas så att den inte avsiktligt eller oavsiktligt görs tillgänglig eller avslöjas för obehöriga eller kan nyttjas på annat otillåtet sätt,
- **spårbarhet** – utförda bearbetningar och andra operationer skall vara möjliga att härleda genom befintliga rutiner till enskild individ (användare) och tidpunkt.

Med hot menas – möjlig, oönskad händelse som ger negativa konsekvenser för verksamheten.

All information är skyddsvärd, men till olika skyddsnivåer. För att nå önskad skyddsnivå krävs en jämvikt mellan önskad skyddsnivå och ett effektivt utnyttjande av befintliga resurser.

För att nå målet för en effektiv hantering av informationen utifrån ett säkerhetsperspektiv, krävs identifiering av skyddsvärda tillgångar och bedömning av relevanta hot. Vidare krävs organisation och kontroll av verksamheten.

Genomförande

För att nå de uppsatta målen ska resurser avdelas för att systematiskt genomföra:

- riskbedömningar och konsekvensanalyser
- framtagande och revidering av riktlinjer, föreskrifter och handlingsplaner.
- informationssäkerhetshöjande åtgärder
- utbildning och information

Årligen ska en plan för säkerhetsarbetet upprättas. Planen ska innehålla en beskrivning av säkerhetsläget, samt de planerade åtgärder som ska vidtas för att uppnå önskad säkerhetsnivå.

Incidentrapporteringsskyldighet

IT-incidenter

GIH har rapporteringsskyldighet vid IT-incidenter till MSB, Myndigheten för samhällsskydd och beredskap, och dess enhet CERT (www.cert.se).

Rapportering av incident skall då ske inom 24 timmar från det att incident inträffat.

Personuppgiftsincidenter

GIH har rapporteringsskyldighet vid personuppgiftsincidenter till Datainspektionen, tillsynsmyndigheten enligt Dataskyddsförordningen.

Rapportering av incident skall då ske inom 72 timmar från det att incident inträffat.