Ansvar och roller i ledningssystem för Informationssäkerhet (LIS) vid Högskolan i Borås

1 Inledning

Ansvaret för informationssäkerhet uppdelas i ledningsansvar och verksamhetsansvar. Det är högskolans ledning som med hjälp av Ledningssystem för informationssäkerhet (LIS) styr så att myndighetens informationshantering sker med adekvat säkerhet utifrån verksamhetens behov och externa krav. Verksamheten ska tillämpa de av ledningen beslutade åtgärderna för att uppnå lämplig organisatorisk och teknisk säkerhetsnivå vid all informationshantering.

Grundprincipen är att ansvaret för informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret. Detta gäller ända från ledning ner till enskilda medarbetare. Denna princip innebär att den person som är ansvarig för ett visst verksamhetsområde också är ansvarig för informationssäkerheten inom det specifika området. En verksamhet kan bedrivas i en organisatorisk del (t.ex. avdelning, institution eller enhet), ett löpande arbetsflöde (t.ex. process) eller ett tidsbegränsat arbete (t.ex. projekt).

2 Ledningsansvar

2.1 Rektor

Rektor har som myndighetschef huvudansvaret för att säkerställa att verksamheten bedrivs författningsenligt och effektivt. Rektor har det yttersta ansvaret för det strategiska informationssäkerhetsarbetet vid högskolan samt att säkerställa att det på högskoleövergripande nivå finns resurser för att genomföra det som förskrifter och internt beslutade regler föreskriver. Rektor ansvarar för att högskolans styrelse en gång per år får en statusrapport av säkerhetsarbetet.

2.2 Förvaltningschef

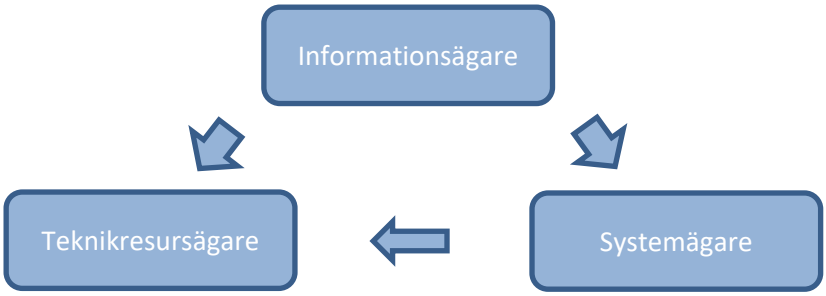
Förvaltningschefen ansvarar för det övergripande systematiska informationssäkerhetsarbetet vid högskolan, i detta ingår att fatta beslut om policy och riktlinjer. Förvaltningschefen ska ha en uppdaterad lägesbild över identifierade risker som kan få allvarliga konsekvenser för högskolans verksamhet och beslutar i samråd med rektor om hur dessa risker ska hanteras. Förvaltningschef ansvarar för att högskolans ledning två gånger per år får en statusrapport av säkerhetsarbetet.

2.3 Akademichef/enhetschef/stabschef

På akademi-/enhets-/stabsnivå är det respektive chef som har det övergripande ledningsansvaret för akademins/enhetens/stabens informationssäkerhetsarbete. Detta ledningsansvar innefattar att ha en uppdaterad lägesbild över identifierade risker som kan få en allvarlig konsekvens för respektive verksamhet.

3 Verksamhetsansvar

Centrala roller i kravställning respektive utförande av informationssäkerhet är informationsägare, systemägare och teknikresursägare. Aktiviteter som följer av ledningssystemet ska ingå i den ordinarie verksamhetsplaneringen och uppföljningen. Verksamhetsansvar för informationssäkerhet inom högskolan är uppbyggt kring samverkan mellan informationsägare, systemägare och teknikresursägare.



Figur 1, Informationsägare ställer krav på systemägare och teknikresursägare medan systemägare i sin tur kan ställa ytterligare krav på teknikresursägare.

3.1 Informationsägare

Alla informationstillgångar ska identifieras och inordnas under en informationsägare. Informationsägaren ansvarar för att säkerställa att informationstillgången klassificeras i syfte att precisera skyddsbehov utifrån verksamhetens beroende av informationen. Genom att tillämpa högskolans metodstöd för informationsklassning och skyddsnivåer bestäms också vilka tillgångar som är verksamhetskritiska för att kunna prioritera införandet av lämpliga skyddsåtgärder.

Eftersom skadeverkningarna av bristande säkerhet i system och tjänster uppstår inom informationsägarens verksamhet är det informationsägaren som ska säkerställa att risker bedöms och adekvata säkerhetskrav ställs med stöd av genomförd informationsklassning.

Rollen som informationsägare innebär ett ansvar och ett förvaltarskap för den information som skapas och hanteras inom de processer/aktiviteter som ingår i den egna verksamheten. I detta ansvar ingår att säkerställa att lämpligt skydd för informationstillgångarna upprättas och vidmakthålls i enlighet med exempelvis dataskyddslagstiftning, arkivlagstiftning och föreskrifter från MSB. Rollen innehas främst av prefekt, föreståndare för forskningscentrum eller avdelningschef. Informationsägarskapet innebär ett chefsansvar på samma sätt som budget-, kvalitets- och miljöansvar.

3.2 Systemägare

Varje system och tjänst som används för högskolans verksamhet ska ha en utsedd systemägare. Rollen som systemägare innebär att vara mottagare av de krav på säkerhet som följer av informationsklassningen som genomförts av berörda informationsägare och säkerställa rätt säkerhetsåtgärder. Systemägaren ansvarar för leveransen av ett system eller en tjänst och har att säkerställa att personella och ekonomiska resurser finns för förvaltningen. Om externa system- eller tjänsteleverantörer används ska systemägaren på högskolan säkerställa att säkerhetskraven ställs, uppfylls och följs upp.

3.3 Teknikresursägare

Rollen som teknikresursägare är ett samlingsbegrepp och innebär att vara ägare av teknikresurser som används för högskolans informationshantering. Detta omfattar allt ifrån interna till externa IT-resurser och även lokaler. I ansvaret ligger att tillse att resursen har rätt säkerhetsnivå utifrån systemägarens krav.

3.3.1 IT-infrastrukturägare

IT-infrastrukturägare ska finnas för alla resurser, som t.ex. nät, servrar och annan hårdvara. IT-infrastrukturägaren kan finnas inom högskolans organisation men kan även vara en extern leverantör. Det är IT-infrastrukturägaren som ansvarar för att IT-säkerhetskraven som ställs av systemägaren eller informationsägaren uppfylls. IT-infrastrukturägare motsvarar resursägare IT enligt högskolans systemförvaltningsmodell. Vid anlitande av externa leverantörer ska adekvata säkerhetskrav alltid fastställas i avtalet med leverantören.

3.3.2 Lokalansvarig

Lokalansvarigs ansvar avgränsas till de byggnadstekniska förutsättningarna, medan utrustning m.m. som nyttjas i lokalen är exempelvis IT-infrastrukturägares eller informationsägares ansvarsområde. För utformning av fysiskt skydd för olika typer av lokaler, gemensamma såväl som verksamhetsspecifika, ska anvisningar för fysiskt skydd tillämpas. För att samordna användningen av resurserna ska det finnas en centralt ansvarig för högskolans lokaler. Vid högskolan innehas denna roll av avdelningschefen för Campus och hållbarhet.

3.4 Övriga roller inom verksamhetsansvaret

Utöver det ansvar som tillfaller nyckelrollerna informationsägare, systemägare och teknikresursägare förutsätter ett systematiskt och effektivt informationssäkerhetsarbete att alla medarbetare verkar för en god säkerhetskultur vid utförandet av sina arbetsuppgifter.

3.4.1 Chefer

Respektive chef ansvarar för att samtliga medarbetare inom sitt ansvarsområde får lämplig utbildning. Medarbetare med ansvar för vitala resurser som exempelvis brandväggar, nätverk, datorhallar och arkiv ska ges särskild utbildning i säkerhetsfrågor. Cheferna ansvarar även för att extern personal, som t.ex. konsulter och gästföreläsare, tar del av och följer högskolans säkerhetsregler.

3.4.2 Medarbetare och konsulter

Alla medarbetare ska följa högskolan säkerhetsregler och ta del av informations- och utbildningsinsatser inom informationssäkerhetsområdet. Medarbetare ska också vara medvetna om högskolans inriktning för god informationssäkerhet, de säkerhetsrisker som kan finnas i det dagliga arbetet och verka för en god säkerhetskultur.

4 Övriga nyckelroller och funktioner

Vid Högskolan i Borås finns ett antal övriga nyckelroller och funktioner som stödjer verksamhetens informationssäkerhetsarbete.

4.1 Informationssäkerhetsansvarig

Informationssäkerhetsansvarig svarar under förvaltningschefen för det systematiska och operativa arbetet med informationssäkerhet inom högskolan.

Ansvaret för informationssäkerhetsansvarig omfattar bland annat följande punkter:

- Att analysera omvärlden och den egna organisationen avseende informationssäkerhet.
- Att utveckla informationssäkerhetsområdet genom att utforma och förvalta dokument, planer och modeller inom informationssäkerhet
- Att stödja den egna organisationen att efterleva, genomföra och använda utformade dokument, planer och modeller – till exempel genom olika metoder, vägledningar, utbildningar och kravställning.

- Rapportera till ledningen i informationssäkerhetsfrågor i enlighet med MSB:s föreskrifter.
    - Rapportera två gånger per år till högskolans ledning.
    - Rapport av allvarliga brister till förvaltningschef så snart som möjligt.

4.2 IT-chefen

IT-chefen är den som ansvarar för högskolans IT-säkerhet och ska vidta lämpliga IT-säkerhetsåtgärder. IT-säkerhet är därmed en del i IT-chefens generella chefsansvar och ska ingå i den ordinarie verksamhetsplaneringen.

Ansvaret för IT-chefen omfattar bland annat följande punkter:

- Att analysera omvärlden och den egna organisationen avseende IT-säkerhet.
- Säkerställa att föreskrifter om IT-säkerhet uppfylls.
- Ta fram och besluta om skyddsnivåer som berör IT-säkerhet.
- Säkerställa att en aktuell tillgängliggjord dokumentation upprättas av hur högskolans IT-system och IT-tjänster uppfyller myndighetens skyddsnivåer som berör IT-säkerhet som används tillsammans med högskolans informationsklassning.
- Ta fram högskoleövergripande styrdokument avseende IT-säkerhet.
- Ta fram och besluta om interna rutiner avseende IT-säkerhet för högskolan.
- Stödja systemägaren vid anskaffning/utveckling av system och tjänster med att säkerställa att IT-säkerhetskraven ställs, uppfylls och följs upp.
- Årligen sammanställa IT-incidenter och rapportera dessa till informationssäkerhetsansvarig.

4.3 Kommunikationschef

Kommunikationschefen har specifikt ansvar för att skapa systematik och helhetssyn inom högskolan avseende praktisk hantering av tillämpning av dataskyddsförordningen (GDPR) inom högskolan.

Ansvaret för kommunikationschef omfattar bland annat följande punkter:

- Att analysera omvärlden och den egna organisationen avseende tillämpningar av dataskyddsförordningen.
- Att stödja den egna organisationen att efterleva, genomföra och använda utformade dokument, planer och modeller – till exempel genom olika metoder, vägledningar, utbildningar och kravställning.

4.4 Ekonomichef

Ekonomichefen har specifikt ansvar för att skapa systematik och helhetssyn inom högskolan avseende arkivering.

Ansvaret för ekonomichef omfattar bland annat följande punkter:

- Att analysera omvärlden och den egna organisationen avseende tillämpningar av arkivlagen.
- Att stödja den egna organisationen att efterleva, genomföra och använda utformade dokument, planer och modeller – till exempel genom olika metoder, vägledningar, utbildningar och kravställning.

4.5 Säkerhetsansvarig

Säkerhetsansvarig har ett övergripande ansvar för fysisk säkerhet vid högskolan. Säkerhetsansvarig svarar under förvaltningschefen för det systematiska och operativa arbetet med fysisk säkerhet inom högskolan. Säkerhetsansvaret är en del i Campus- och hållbarhetschefens generella chefsansvar och ingår i den ordinarie verksamhetsplaneringen.

Under Säkerhetsansvarig finns rollen Säkerhetssamordnare som ansvarar för att utveckla och förvalta säkerhetsarbetet. Säkerhetsansvarig ska tillse att Säkerhetssamordnare har tillräckliga resurser för att genomföra arbetet.

4.6 Säkerhetssamordnare

Säkerhetssamordnaren har ett delegerat ansvar från Säkerhetsansvarig för fysisk säkerhet vid högskolan i Borås.

Ansvaret för Säkerhetssamordnaren omfattar bland annat följande punkter:

- Ta fram högskoleövergripande styrdokument för hur säkerhetsarbetet ska bedrivas.
- Ta fram instruktioner och lathundar för hur säkerhetsarbetet ska bedrivas.
- Ta fram skyddsnivåer för fysisk säkerhet.
- Rapportera till ledningen i säkerhetsfrågor.
    - Rapportera två gånger per år till högskolans ledning.
    - Rapportera allvarliga brister till förvaltningschef så snart som möjligt.
- Utgöra ett stöd till organisationen i säkerhetsfrågor.
- Årligen sammanställa incidenter inom säkerhetsområdet.
- Initiera och genomföra revisioner och kontroller av säkerheten.
- Ta fram informations- och utbildningsmaterial rörande säkerhet samt genomföra utbildningar för olika grupper.

4.7 Dataskyddsombud

Dataskyddsombudets ansvar beskrivs i ”Beslut om förordnande som dataskyddsombud”, dnr 271-18.

4.8 Expertfunktioner

Informationssäkerhetsamordnare, arkivarie, dataskyddsombud, GDPR-handläggare, IT-säkerhetssamordnare, säkerhetssamordnare, HR-specialist m.fl. ska delta aktivt i det operativa arbetet, t.ex. delge sin expertkunskap vid genomförande av informationsklassning och riskanalys.

4.9 Informationshanteringsrådet

Vid högskolan finns ett informationshanteringsråd som stödjer verksamheten i frågor om informationshantering, vilket inkluderar informationssäkerhet, integritetsskydd samt arkivering och gallring.

Informationshanteringsrådet har bland annat följande uppgifter inom informationssäkerhet:

- Samverka inom området informationshantering.
- Omvärldsbevaka inom området informationshantering.
- Stödja vid kravställning inför upphandling/inköp av nya system.

Informationshanteringsrådet leds och sammankallas av informationssäkerhetssamordnaren.

4.10 Säkerhetsgruppen

På högskolan finns en övergripande säkerhetsgrupp som samordnar inom området säkerhet samt arbetar operativt med högskolans säkerhetsfrågor.

Säkerhetsgruppen har bland annat följande uppgifter:

- Informera och levandegöra säkerhetsfrågorna i verksamheten
- Säkerställa att berörda målgrupper kan hålla sig uppdaterade och ges möjlighet till regelbunden utbildning.

Säkerhetsgruppen leds och sammankallas av säkerhetssamordnaren.

4.11 CSIRT

På högskolan finns en CSIRT-grupp (Computer Security Incident Response Team) som samordnar incidenter inom IT-säkerhetsområdet. Enligt vedertagen praxis ska en sådan grupp finnas inom vissa organisationer med direktanslutning till Internet.

CSIRT har bland annat följande uppgifter:

- övervaka, logga, utreda, bedöma allvarlighetsgraden och hantera IT-relaterade incidenter
- vid behov rapportera IT-säkerhetsincidenter till MSB
- vid brottsmisstankar samverka med rättsvårdande myndigheter