LUNDS UNIVERSITET

BESLUT

Diarienummer
STYR 2022/587

Datum
2022-03-24

Rektor

# Ledningssystem för informationssäkerhet

# vid Lunds universitet

*Fastställt av rektor 2022-03-24*

*Postadress* 221 00 Lund, *Besöksadress* Arkeologen Sandgatan 1 *Telefon* 076-130 35 66, 046-222 00 00,
*E-post* ingegerd.wirehed@rektor.lu.se

# Innehåll



*Postadress* 221 00 Lund, *Besöksadress* Arkeologen Sandgatan 1 *Telefon* 076-130 35 66, 046-222 00 00,
*E-post* ingegerd.wirehed@rektor.lu.se

# 1. Inledning

Information är en nödvändig resurs och en förutsättning för att Lunds universitet ska kunna bedriva högkvalitativ utbildning och forskning i samverkan med omvärlden och bidra till samhällets utveckling. Ökad digitalisering, användningen av tekniska hjälpmedel, cyberhot, rättsliga krav, föreskrifter och förordningar samt en hög förändringstakt i omvärlden gör att ett systematiskt och riskbaserat informationssäkerhetsarbete är av stor vikt för universitetet. Det systematiska arbetssättet beskrivs här i form av universitetets Ledningssystem för informationssäkerhet (LIS) och syftar till att säkerställa att universitetets kritiska informationstillgångar ges ett adekvat, relevant och kontinuerligt skydd. Se Bilaga 1 Ledningssystem för Informationssäkerhet (LIS).

Universitetets informationssäkerhetsarbete är baserat på svensk standardserie ISO 27000, och ska uppfylla Myndigheten för samhällsskydd och beredskaps (MSB) *föreskrifter om statliga myndigheters informationssäkerhet*, MSBFS 2020:6[1] samt MSBFS2020:7 och MSBFS 2020:8 och därtill följa MSBs s.k. LIS-modell.

**Styrande dokument**
Följande styrande dokument ingår i universitetets Ledningssystem för informationssäkerhet:

- *Policy för informationssäkerhet*

  Uttrycker universitetsstyrelsens viljeinriktning, strategiska mål och ledningssystemets omfattning
- *Ledningssystem för informationssäkerhet vid Lunds universitet*

  Fastställer och beskriver hur universitetet styr sin informationssäkerhet
- *Riktlinjer - Riskbaserat informationssäkerhetsarbete*

  Beskriver riskprocess - informationssäkerhet
- *Anvisningar – Fastställda informationssäkerhetsåtgärder*

  Beskriver säkerhetsåtgärder inom informationssäkerhet

## 1.1 Definitioner

Terminologi och definitioner för området och relaterade områden vid universitetet återfinns i dokumentet ”Terminologi för informationssäkerhet vid Lunds universitet” på Medarbetarwebben.

## 1.2 Omfattning

Ledningssystemet omfattar och gäller för alla verksamheter, medarbetare, studenter samt externa samarbetspartner vid universitetet och därmed all information och data för vilken universitetet är ansvarig huvudman utifrån universitetets organisationsnummer 202100-3211. Informationssäkerhetsarbetet ska bedrivas så

[1] *MSBFS 2020:6*

effektivt som möjligt och som en integrerad del i det dagliga arbetet samt följa universitetets befintliga årscykel, budgetprocess, verksamhetsplanering med flera relevanta processer.

## 2. Ledning och styrning

Universitetsledningen ska styra och följa upp informationssäkerheten så att man kontinuerligt säkerställer dess fortsatta lämplighet, tillräcklighet och verkan. Utvärdering av informationssäkerhetsprestandan sker i form av monitorering, mätning, analys och utvärdering samt revision.

Universitetets modell för verksamhetsstyrning och riskhantering samt krav i MSB:s föreskrifter MSBFS 2020:6, ligger till grund för hur informationssäkerhetsstyrningen sker.

Grundläggande för ett fungerande och effektivt informationssäkerhetsarbete, inklusive IT-säkerhetsområdet, är att kontinuerlig uppföljning och förbättring sker, och att en aktiv dialog förs mellan universitetsledningen, fakultetsledningarna/motsvarande och universitetets CISO (Chief Information Security Officer). MSBs modell beskriver samtliga cykliska steg i ett LIS i Figur 1.


*Figur 1, MSB:s LIS-modell*

### Ansvar och befogenheter

Universitetsstyrelsen har i universitetets arbetsordning fastställt ansvars- och arbetsfördelning inom universitetet och beslutar även om den övergripande *Informationssäkerhetspolicyn.*

Rektor är ytterst ansvarig för den verksamhet som bedrivs vid Lunds universitet och därmed också ytterst ansvarig för att informationssäkerhetsarbetet möter de krav som ställs enligt lagar, förordningar och föreskrifter. Rektor har även fastställt fördelning av beslutsbefogenheter. I detta dokument görs en konkretisering av befintlig delegation och arbetsordning som reglerar ansvars- och uppgiftsfördelning gällande informationssäkerhet samt förutsättningar för delegation.

Rektor beslutar att delegera ansvar och befogenheter enligt fördelningen i:

- Bilaga 3a Ansvar och delegeringar
- Bilaga 3b Ansvar och delegeringar inom informationssäkerhetsområdet

## 2.1 Ledningens genomgång

Rapportering av informationssäkerhetsarbetet sker i form av ledningens genomgång och beskrivs i Bilaga 2 Rutin för Ledningens genomgång av informationssäkerhetsarbetet. Med ledningen avses universitetsledningen.

Rapportering görs av CISO som ett led i att rektor ska kunna bedöma effektiviteten i informationssäkerhetsarbetet samt besluta om mål, handlingsplan och prioriteringar.

Löpande avstämningar och rapportering härutöver sker vid behov.

# 3. Riskprocess - informationssäkerhet

Universitetets process för riskbaserat informationssäkerhetsarbete följer MSB:s metodstöd och innefattar följande moment:

1. *Omvärldsanalys*
2. *Verksamhetsanalys*
3. *Riskanalys*
4. *Gapanalys*
5. *Informationsklassning*
6. *Hantering av identifierade risker/val av säkerhetsåtgärder*
7. *Handlingsplan*

Processen, även kallad riskprocess - informationssäkerhet, beskrivs i Bilaga 4 Riskprocess - informationssäkerhet samt mer utförligt i styrdokument *Riktlinjer – Riskbaserat informationssäkerhetsarbete*.

Den ska genomföras:

- årligen vid fakulteter/motsvarande och vid förvaltningen
- vid behov, t.ex. vid större förändringar och projekt.

Resultaten är ingångsvärden till beslut om handlingsplan och Ledningens genomgång, samt därefter till budgetprocess och verksamhetsplanering.

Processtegen faciliteras av CISO-funktionen (universitetsgemensam informationsäkerhetsfunktion) som även sammanställer, dokumenterar, kommunicerar resultaten samt följer upp i samverkan med respektive verksamhet. I varje steg ska relevanta roller delta. Expertfunktioner vid fakulteter och förvaltning ska bjudas in, vara delaktiga och bidra.

Sista steget är upprättande av handlingsplan för att åtgärda informationssäkerhetsrisker, uppfylla informationssäkerhetsmål och beakta möjligheter för verksamheten.

## 4. Organisation och stöd

Organisation, ansvar och roller för informationssäkerhetsarbetet regleras i detta styrande dokument, i universitetets arbetsordning, genom rektorsbeslut samt i Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet, MSBFS 2020:6.

Ett informationssäkerhetsråd ska etableras på universitetsnivå med uppgift att bereda strategiska frågor, göra riskbedömningar, t.ex. inför rektorsbeslut, samt vara rådgivare till CISO. Ledamöter bör vara representanter från informationsriskägare och utvalda representanter från fakultetsledningar/motsvarande samt FC (förvaltningschefen).

Vid behov kan lokala råd för informationssäkerhet etableras vid fakulteterna, alternativt hanteras informationssäkerhetsområdet i fakultetsledningsgruppen. På fakultetsnivå beslutar fakultetsstyrelsen om lokalt informationssäkerhetsråd bör inrättas. Uppgiften för sådant råd kan isåfall vara att utreda och föreslå generella och riktade åtgärder för att säkerställa att informationssäkerheten uppfyller gällande krav, samt utgöra ett stöd för verksamheten att vända sig till i frågor avseende informations-säkerhet.

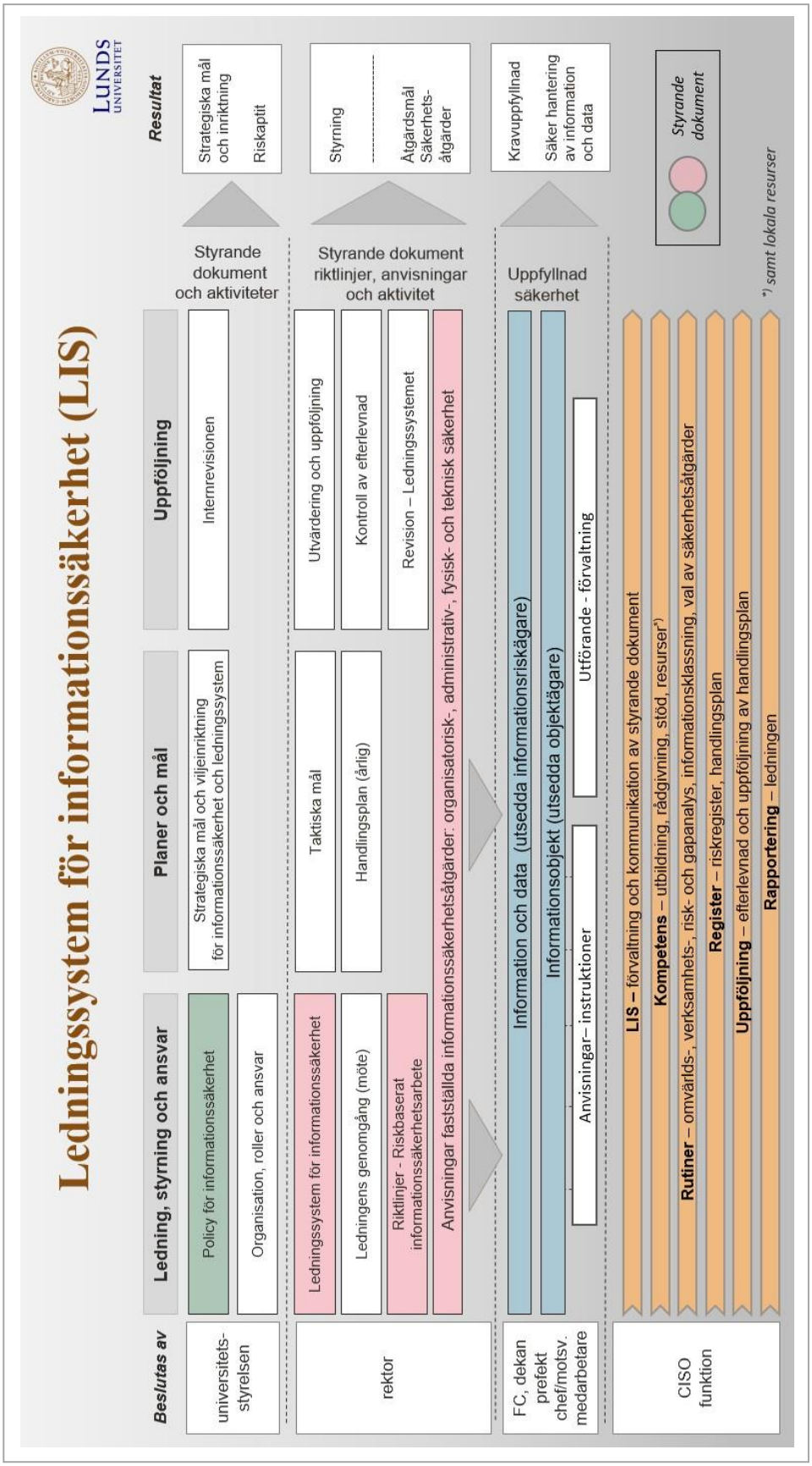
Stöd till verksamheten ges bland annat från den centrala CISO-funktionen. CISO-funktionen tar t.ex. fram och tillgängliggör universitetsövergripande styrdokument, regler, guider, utbildningar och nyheter. Funktionen ger också stöd i genomförande av riskprocess - informationssäkerhet inom ramen för universitetets årscykel och vid behov.

Alla fakulteter/motsvarande och förvaltningen ska utse lokala samordnare för informationssäkerhet. CISO-funktionen ansvarar för forum för lokala samordnare där dialog och erfarenhetsutbyte sker kring operativa frågor. Utbildning kommer att erbjudas lokala samordnare.

I Bilagor 3a och 3b beskrivs samtliga roller, ansvar och delegeringar.

I Bilaga 5 Organisation, rapportering, ansvar och resurser beskrivs organisation, rapportering, ansvar och resurser.

# Bilaga 1 Ledningssystem för Informationssäkerhet (LIS)




*Postadress* 221 00 Lund, *Besöksadress* Arkeologen Sandgatan 1 *Telefon* 076-130 35 66, 046-222 00 00,
*E-post* ingegerd.wirehed@rektor.lu.se

# Bilaga 2 Rutin för Ledningens genomgång av informationssäkerhetsarbetet

## Syfte och omfattning

Syftet med denna rutin är att beskriva hur ledningens genomgång av informationssäkerhetsarbetet ska planeras, genomföras, dokumenteras och följas upp, dels på universitetsövergripande nivå dels kan ske vid fakulteter/motsvarande verksamheter[2].

Syftet med ledningens genomgång är att skapa förutsättningar för universitetet att styra och bedriva ett systematiskt, riskbaserat informationssäkerhetsarbete som är förebyggande med ständiga förbättringar samt att efterleva tillämpliga rättsliga krav samt externa och interna regler. Vid ledningens genomgång ska ledningen informeras och informationssäkerhetsarbetets samt LIS:ets effektivitet utvärderas och en handlingsplan presenteras.

## Universitetsgemensam nivå

Ärenden och rapporteringspunkter ska tas fram av CISO i samråd med universitetets informationssäkerhetsråd.

Ledningens genomgång genomförs i rektors ledningsråd (RL).

CISO ansvarar för att:

- Bereda, sammanställa och tillgängliggöra underlag inför Ledningens genomgång

*Genomförande*
Ledningens genomgång på universitetsgemensam nivå ska hållas i rektors ledningsråd vid två ordinarie mötestillfällen, förslagsvis i april respektive november.
Ledningens genomgång bör innehålla samtliga av de punkter som MSB rekommenderar att högsta ledningen vid statliga myndigheter håller sig informerad om, se *Agenda för Ledningens genomgång* nedan.
Beslut av handlingsplan efter Ledningens genomgång fattas av rektor vid gängse rektorssammanträde (RS).

Vid behov ska specifika frågor som rör informationssäkerhetsarbetet lyftas till rektor även mellan dessa tillfällen.

*Agenda för Ledningens genomgång*

[2] *Med motsvarande verksamheter avses gemensamma förvaltningen, universitetsbiblioteket universitetets särskilda verksamheter (USV), universitetets kultur- och museiverksamhet och MAX IV-laboratoriet*

**April**

**Uppföljning**

Föregående möte och uppföljning av tidigare beslutade åtgärder

**Säkerhetsmedvetenhet**

Status avseende medvetenheten om informationssäkerhet i organisationen. Risker avseende digitalisering och IT-användning.

**Uttalande om tillämplighet**

**Informationstillgångar**

Status på mest kritiska och känsliga informationstillgångar i organisationen.

**Externa krav**

Lagkrav och andra externa krav på informationssäkerhet och status på efterlevnad.

**Risker**

Allvarligaste informationssäkerhetsriskerna. Dels specifika för organisationen, dels för samhället i stort.

**Skydd**

Status på befintligt skydd, allvarliga brister och sårbarheter. Gapanalyser gentemot ISO27000 standards/MSB-krav.

**Incidenter**

Summering och analys av informationssäkerhetsincidenter sedan förra rapporteringen.

**Handlingsplan**

Handlingsplan för kommande verksamhetsår, samt mål presenteras. Handlingsplan och mål beslutas sedan av rektor genom gängse process för rektorsbeslut och rektorssammanträde (RS).

**Övriga frågor**

**November**

**Uppföljning**

Föregående mötesprotokoll, och uppföljning enligt aprilmötet:

- Uttalande om tillämplighet
- Incidenter
- Handlingsplan

**LIS och informationssäkerhetsarbetets effektivitet**

Ev. beslut om förbättringar

**Revisioner och granskningar**

Resultat av genomförda informationssäkerhetsrelaterade revisioner och granskningar av efterlevnad av universitetets styrande dokument för informationssäkerhet.

*Postadress* 221 00 Lund, *Besöksadress* Arkeologen Sandgatan 1 *Telefon* 076-130 35 66, 046-222 00 00,

*E-post* ingegerd.wirehed@rektor.lu.se

**Förbättringsåtgärder**

Åtgärder som vidtagits avseende informationssäkerhet.

*Efter mötet*

Mötessekreteraren för ledningens genomgång skriver protokoll från mötet och ser till att detta justeras av utsedd justeringsperson samt distribuerar protokollet till rektors ledningsråd, samtliga kanslichefer och samtliga sektionschefer/motsvarande. Kanslicheferna ansvarar för att kommunicera det till sina respektive verksamheter.

Samtliga medlemmar i rektors ledningsråd samt CISO ansvarar för att informera sina respektive organisationer om utkomsten av mötet och eventuella uppdrag.

## Fakultetsnivå/motsvarande

Varje fakultet/motsvarande ansvarar för om Ledningens genomgång av informationssäkerhetsarbetet på fakultetsnivå ska ske. En sådan genomförs lämpligen enligt motsvarande struktur som ovan beskriven för universitetsnivå, årligen samt med fördelnära tidpunkten för årlig genomförande av riskprocess - informationssäkerhet med fakultetens ledningsgrupp alternativt lokalt informationssäkerhetsråd om ett sådant etablerats.

# Bilaga 3a Ansvar och delegeringar

Rektor för Lunds universitet:

- har som myndighetschef det övergripande ansvaret för att informationssäkerhets-arbetet uppfyller kraven enligt gällande lagstiftning
- tillser att god informationssäkerhet genomsyrar verksamheten
- håller sig informerad om informationssäkerhetsarbetet, risker mm
- tar beslut om handlingsplaner och hantering av informationssäkerhetsrisker på universitetsnivå
- tillser att universitetets Ledningssystem för informationssäkerhet är ändamåls-enligt och att arbetet bedrivs enligt fastställda styrdokument
- säkerställer att det finns en universitetsövergripande CISO-funktion med nödvändiga resurser och förutsättningar.

Rektor delegerar ansvar och vissa befogenheter inom informationssäkerhetsområdet enligt nedan.

**Alla verksamma**

Alla verksamma vid universitetet, såsom medarbetare, alla studenter samt externa samarbetspartner, har ett ansvar och en skyldighet att skydda verksamhetens information vid hantering av denna samt att inrapportera avvikelser från regelverket eller oönskade händelser som upptäcks. Rapportering ska ske skyndsamt och utan fördröjning enligt instruktioner på universitetets Medarbetarwebb. Inrapporterade avvikelser och oönskade händelser hanteras av berörda säkerhetsfunktioner i enlighet med beslutade processer.

**Verksamhetsansvariga**

Chefer och verksamhetsansvariga ansvarar för arbetet med riskhantering inom sitt ansvarsområde.

Verksamhetsansvariga på alla nivåer ska säkerställa att deras medarbetare/ motsvarande får adekvat utbildning och kontinuerlig information om fastställda säkerhetsåtgärder samt att krav som ställs på den egna verksamheten och individerna uppfylls.

**Dekan**

Dekan/motsvarande ansvarar för informationssäkerheten inom sin fakultet/ motsvarande som en del i det delegerade verksamhetsansvaret. Ansvaret kan delegeras vidare till prefekt eller motsvarande.

Dekan/motsvarande ansvarar för att:

- uppfylla krav på riskhantering och säkerhetsåtgärder som ställs på den egna verksamheten

- regelbundet följa upp och rapportera avvikelser från informationssäkerhetskrav inom sitt ansvarsområde till CISO-funktionen eller enligt gällande processer på universitetets Medarbetarwebb
- tid, resurser och förutsättningar finns för informationssäkerhetsarbetet inom den egna verksamheten
- riskprocess – informationssäkerhet en genomförs enligt universitetets årshjul och vid behov
- utse lokal samordnare för informationssäkerhet vid fakultet/motsvarande. Flera institutioner/motsvarande kan välja att utse gemensam samordnare. I de fall en kontaktperson inte utses svarar dekan/motsvarande själv för kontakter och stöd rörande informationssäkerheten
- efterlevnadsuppföljning och rapporter lämnas till CISO två gånger per år samt vid behov.

**Förvaltningschefen**

Enligt rektors delegation har förvaltningschefen övergripande ansvar för universitetets verksamhet i rättsligt, ekonomiskt och administrativt avseende.

Förvaltningschefen ansvarar för informationssäkerheten inom förvaltningen som en del i det delegerade verksamhetsansvaret. Ansvaret kan delegeras vidare till sektionschef/motsvarande.

Förvaltningschefen ansvarar för att:

- uppfylla krav på riskhantering och säkerhetsåtgärder som ställs på den egna verksamheten
- regelbundet följa upp och rapportera avvikelser från informationssäkerhetskrav inom sitt ansvarsområde till CISO-funktionen eller enligt gällande processer på universitetets Medarbetarwebb
- tid, resurser och förutsättningar finns för informationssäkerhetsarbetet inom den egna verksamheten
- riskprocess - informationssäkerhet genomförs enligt universitetets årshjul och vid behov
- kontinuitetsplanering med avseende på informationssäkerhet sker på verksamhetsövergripande nivå
- CISO-funktionen ges nödvändiga resurser för att kunna utföra beslutat uppdrag och uppgifter samt ge adekvat stöd till verksamheterna.

**Systemägare**

Systemägare/motsvarande:

- har det överordnade ansvaret för administration, drift och den övergripande informationssäkerheten avseende specifikt IT-system

- ansvarar för uppfyllnad av informationsriskägarens krav på informations-säkerhetsåtgärder för IT-systemet/tjänsten, som driftas inom universitetet eller av extern part, så att informationen skyddas på adekvat sätt
- ansvarar för att definiera och följa upp IT-systemets tekniska skyddsåtgärder utifrån aktuell handlingsplan och inom ramen för universitetets systemförvaltningsmodell samt säkerställa att IT-säkerhetsåtgärder är i enlighet med kraven avseende informationssäkerhet.

Arbetsuppgifterna kan delegeras i enlighet med roller och ansvar i universitetets systemförvaltningsmodell. Se universitetets webbsidor.

I det fall systemägare inte utsetts är verksamhetsansvarig, för verksamheten där systemet ingår, ansvarig.

### IT-chefer

IT-chefer/motsvarande ansvarar för att:

- det finns nödvändiga resurser, kompetens, dokumenterade anvisningar och instruktioner för IT-verksamheten så att kravställda, fastställda tekniska IT-säkerhetsåtgärder kan införas och förvaltas baserat på universitetets styrande dokument för informationssäkerhet
- säkerställa efterlevnad avseende de informationssäkerhetskrav som ställs på IT-system och infrastrukturer inom det egna ansvarsområdet.

### Dataskyddsombud / DSO

Dataskyddsombudets uppgift är enligt Dataskyddsförordningen följande med anknytning till informationssäkerhet med avseende på persondata:

- informera, ge råd och utbilda universitetet och dess anställda om deras skyldigheter enligt dataskyddslagstiftningen
- övervaka regelefterlevnaden av dataskyddslagstiftningen och av universitetets strategi för skydd av personuppgifter
- ge råd om den konsekvensbedömning avseende dataskydd som ska göras enligt dataskyddslagstiftningen
- ge stöd vid hantering och rapportering av personuppgiftsincidenter
- fungera som kontaktpunkt för tillsynsmyndigheten och registrerade.

Ombudet bör delta som expert när informationssäkerhetsrisker bedöms.

Roll och uppgifter definieras närmare i särskilt rektorsbeslut.

### Säkerhetsskyddschef

Enligt säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2018:658), rikspolisstyrelsens föreskrifter om säkerhetsskydd och offentlighets- och sekretess-lagen åläggs universitetet att vidta förebyggande åtgärder för att skydda säkerhetskänslig verksamhet vid universitetet mot spionerі, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter.

Vid analyser av informationstillgångar där dessa lagstiftningar kan vara applicerbara och något av följande kan krävas ska universitetets säkerhetsskyddschef kontaktas:

- säkerhetsskyddsanalys
- bakgrundskontroller och säkerhetsprövningssamtal
- säkerhetsklassning.

Roll och uppgifter definieras närmare i särskilt rektorsbeslut.

*Postadress* 221 00 Lund, *Besöksadress* Arkeologen Sandgatan 1 *Telefon* 076-130 35 66, 046-222 00 00,
*E-post* ingegerd.wirehed@rektor.lu.se

# Bilaga 3b Ansvar och delegeringar inom informationssäkerhetsområdet

Rektor delegerar ansvar och befogenheter inom informationssäkerhetsområdet enligt följande

## CISO

CISOs[3] uppdrag och roll är oberoende och rapporteras till rektor. Rollen ansvarar för och har befogenheter att:

- planera och koordinera det universitetsövergripande informationssäkerhets-arbetet i enlighet med beslutade styrdokument, processer, målsättningar och ramar från ledningen, samt ansvarar för universitetsövergripande rutiner och verktyg
- rapportera informationssäkerhetsområdet, dess status samt ta fram och rekommendera handlingsplan till rektor och rektors ledningsråd vid Ledningens genomgång
- rapportera till ledningen samt göra bedömning av lämplig hantering vid större informationssäkerhetsrelaterade incidenter och kriser
- representera universitetet i relationen till andra myndigheter och verksamheter i informationssäkerhetsfrågor som t.ex. incidentrapportering till MSB. Detta gäller ej frågor som ska hanteras av dataskyddsombud eller säkerhetsskyddschef om detta inte kommits överens om tidigare.

Roll och uppgifter definieras närmare i särskilt rektorsbeslut.

### Universitetsgemensam CISO-funktion

Inom universitetsförvaltningen finns en CISO-funktion, för vilken CISO har ledning- och verksamhetsansvar. Funktionens uppgifter är att:

- förvalta LU:s ledningssystem för informationssäkerhet och säkerställa att därtill hörande dokument hålls aktuella, uppdaterade och kommunicerade
- ställa krav mot verksamheten avseende informationssäkerhet
- utbilda och informera medarbetare, studenter samt externa samarbetspartner vid behov
- medverka vid bedömning och hantering av större informationssäkerhetsrelaterade incidenter och kriser
- facilitera och stödja vid genomförande av riskprocess – informationssäkerhet, genom att involvera och samverka med andra stöd- och expertfunktioner vid fakulteter och förvaltning t.ex.; dataskyddsombud, säkerhetsavdelning, IT-säkerhetsexperter, HR, juridiska avdelningen, LU byggnad, dokument- och arkivfunktion.

### Lokal informationssäkerhetssamordnare

Samordnarens arbetsuppgifter avgörs beroende på verksamhetens omfattning och art. Dessa kan omfatta att vara kontaktperson för informationssäkerhet och stöd för den egna ledningen och medarbetare i det dagliga arbetet, delta i det årliga

[3] *MSBFS 2020:6 5§*

riskprocessarbetet som rör den egna verksamheten samt att vara kontaktperson gentemot den universitetsgemensamma CISO-funktionen.

**Informationsriskägare**

Informationsriskägare[4] kopplas till informationstyp, identifieras under riskanalysfasen och ansvarar för att

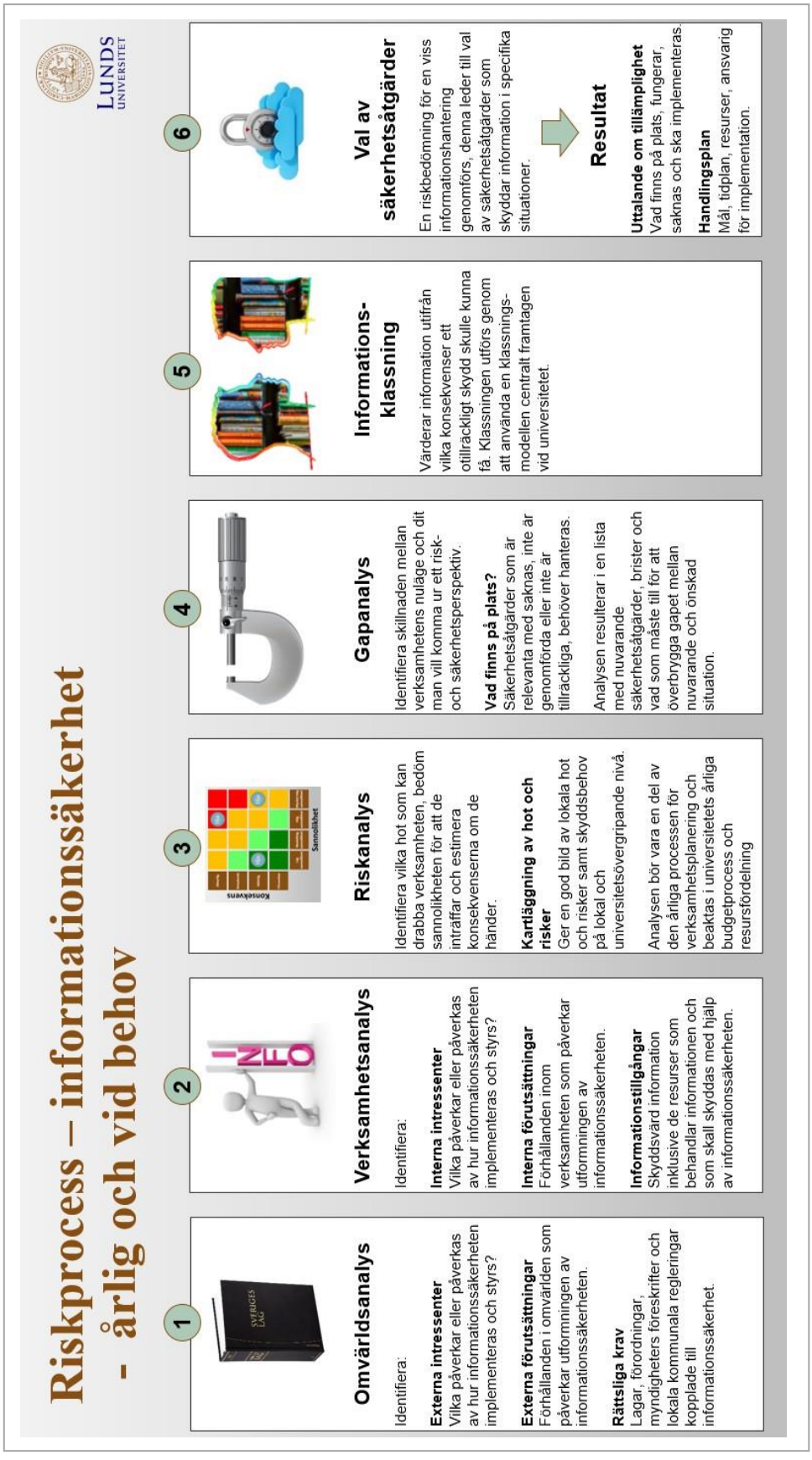
- information hanteras på ett sätt så att den behåller rätt nivå av konfidentialitet samt behåller sin riktighet och tillförlitlighet under hela livscykeln, i till exempel ett IT-system/tjänst, genom att vara formell kravställare
- informationsklassning genomförs enligt beslutad process och är adekvat
- ta beslut om acceptans av eventuella kvarvarande risker (riskacceptans) som överskrider universitetets riskaptit när handlingsplan är beslutad.

Informationsriskägarskap följer ordinarie verksamhetsansvar (linjen) så länge risken endast omfattar den egna verksamheten.

För universitetsgemensamma informationstyper och universitetsövergripande risker beslutas informationsriskägare av rektor.

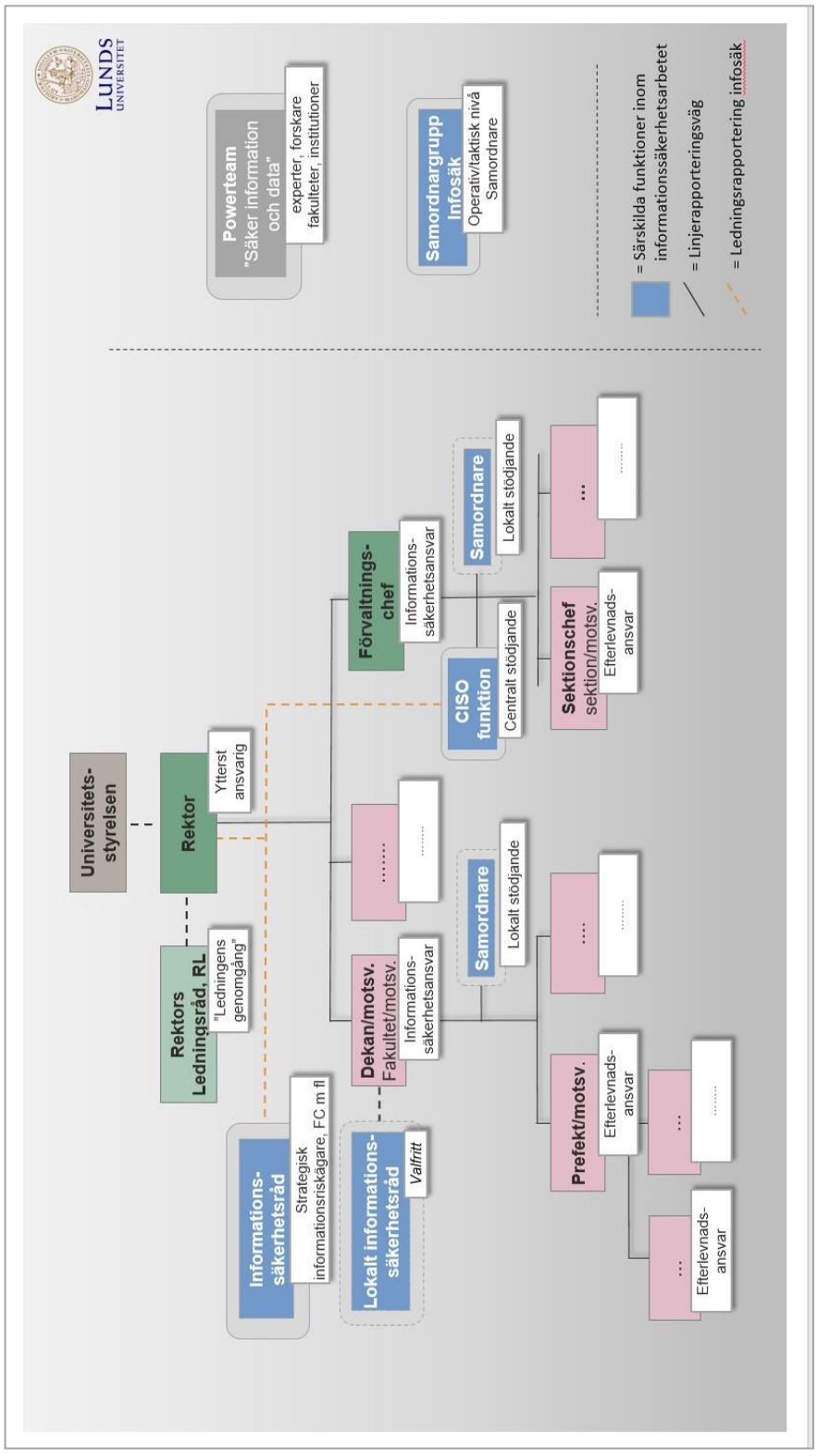
[4] *MSBFS 2020:6 5§*

# Bilaga 4 Riskprocess - informationssäkerhet




*Postadress* 221 00 Lund, *Besöksadress* Arkeologen Sandgatan 1 *Telefon* 076-130 35 66, 046-222 00 00,
*E-post* ingegerd.wirehed@rektor.lu.se

# Bilaga 5 Organisation, rapportering, ansvar och resurser




*Postadress* 221 00 Lund, *Besöksadress* Arkeologen Sandgatan 1 *Telefon* 076-130 35 66, 046-222 00 00,
*E-post* ingegerd.wirehed@rektor.lu.se