



Stockholms
universitet

Universitetsstyrelsen

Protokoll fört vid sammanträde

2025-12-05 (nr 6 2025)

kl 09.00-12.00

- Närvarande: Justitierådet Helena Jäderblom (ordförande), rektor Hans Adolfsson, stadsdirektör Fredrik Jurdell, senior ekonom Robert Bergqvist, civilingenjör Anna Rathsmann, verkställande direktör Erik Brandsma, styresman Sanne Houby-Nielsen, universitetsrektor Tiit Land, rektor Sunniva Whittaker, professor Martin Jakobsson, professor Stefan Helgesson, professor Pernilla Leviner (tjänstgörande ersättare), kårordförande Victor Nygren, vice kårordförande Kai Nuñez Wiklund och doktorand Karl Sigfrid
- Huvudföredragande: Universitetsdirektör Åsa Borin
- Föredragande: Vicerektor Stefan Helgesson (p. 4), internrevisionschef Tobias Björn (pp. 5, 6 och 8), universitetsdirektör Åsa Borin (pp. 7-8), säkerhetschef Peter Klysing (p. 9), sektionschef Hanna Ridefelt (pp. 10-11), Elisabet Jamal Bergström och Mikael Lundgren (SEB) (p. 12), stiftelseansvarig Bertil George (p. 12), utredare Ulrika Bjare (p. 13) och utredare Gabor Schubert (p. 13)
- Övriga närvarande: Professor Joakim Edsjö (ersättare), universitetsdirektör Åsa Borin, internrevisionschef Tobias Björn, avdelningschef Lena Ousbäck, planeringschef Karin Fürstenbach, chefsjurist Markos Stavroulakis, controller Clara Ersson (p. 8), säkerhetschef Peter Klysing (p. 9), sektionschef Hanna Ridefelt (pp. 10-11), Elisabet Jamal Bergström och Mikael Lundgren (SEB) (p. 12), stiftelseansvarig Bertil George (p. 12), utredare Ulrika Bjare (p. 13), utredare Gabor Schubert (p. 13), Camilla Gamrell (ST), Rebecca Adami (SACO) samt utredare Anna Riddarström
- Protokollförelse: Utredare Anna Riddarström

1. Utseende av justeringsperson Kai Nuñez Wiklund utses till justeringsperson.
2. Fastställande av dagordning Dagordningen fastställs.
3. Information från rektor Rektor informerar om den kommande utredningen om associationsformer för universitet och högskolor samt om lärdomar från Finland kring detta. Vidare informerar rektor om att Knut och Alice Wallenbergs stiftelse har fattat beslut om två nya Wallenberg Academy Fellows till Stockholms universitet.

- | | | |
|-----|---|--|
| 4. | Presentation av det humanvetenskapliga området – Humanistiska fakulteten och lärarutbildningen | Presentation |
| 5. | Beslut om Internrevisionsplan 2026 (dnr SU FV-0003-25) | Universitetsstyrelsen beslutar att fastställa Internrevisionsplan 2026 enligt bilaga 1. |
| 6. | Beslut om revidering av riktlinjer för internrevisionen (dnr SU FV-0003-25) | Universitetsstyrelsen beslutar att fastställa Riktlinjer för internrevisionen enligt bilaga 2.
Detta beslut ersätter Riktlinjer för internrevisionen beslutade av universitetsstyrelsen 2024-09-20. |
| 7. | Åtterrapporing med anledning av Internrevisionens granskning av IT-säkerhet (dnr SU FV-0975-25) | Information |
| 8. | Beslut om åtgärder med anledning av rapport från Internrevisionen avseende granskning av informations- och säkerhetskultur (dnr SU FV-0003-25 och FV-3761-25) | Universitetsstyrelsen beslutar att uppdra åt rektor att vidta erforderliga åtgärder enligt yttrandet (bilaga 3) samt att lägga Internrevisionens rapport till handlingarna (bilaga 4). |
| 9. | Information om säkerhetspolicy (dnr SU FV-4281-25) | Information |
| 10. | Diskussion om förslag till revideringar av Ägaranvisningar för Stockholms universitet Holding AB (dnr SU FV-4201-25) | Diskussion |
| 11. | Diskussion om process för nominering av ledamöter till styrelsen för Stockholms universitet Holding AB (dnr SU FV-4200-25) | Diskussion |
| 12. | Diskussion om revidering av Placeringspolicy för stiftelser anknutna till Stockholms universitet (dnr SU FV-2029-25) | Diskussion |
| 13. | Redovisning av forskningsindikatorer (dnr SU FV-3998-25) | Information |
| 14. | Diskussion om synpunkter från Hörandeförsamlingen angående rektors- och prorektorsrekrytering (dnr SU FV-4283-25) | Styrelsen beslutar att bordlägga ärendet. |
| 15. | Övriga frågor | Inga övriga frågor anmäldes. |



Stockholms
universitet

Internrevisionsplan
2025-12-05

SU FV-0003-25

Internrevisionen

Internrevisionsplan 2026

Internrevisionen

Innehållsförteckning

1.	Inledning	3
2.	Internrevisionsstrategi	3
3.	Genomförande av riskanalys	3
4.	Översikt granskningsområden 2026	4
5.	Beskrivning av granskningsområden 2026	5
5.1	Förebyggande arbete mot oegentligheter samt hantering av bisysslor	5
5.2	Granskning av lokaloptimeringsprojektet	6
5.3	Ansvarsfull internationalisering	6
5.4	Regelefterlevnad – tjänsteresor	7
5.5	Institutions- och avdelningsgranskningar	7
5.6	SUHF	7
5.7	Uppföljning tidigare granskningar och årsrapport	8
6.	Övrigt.....	8
7.	Resursplanering	9

1. Inledning

Internrevisionen ska utifrån en analys av verksamhetens risker stödja Stockholms universitetsstyrelse genom att självständigt, utifrån internrevisionsförordningen (2006:1228), granska om ledningens interna styrning och kontroll är utformad så att myndigheten med en rimlig säkerhet fullgör sina uppgifter, uppnår verksamhetens mål och uppfyller kraven i myndighetsförordningens § 3. Det vill säga att verksamheten bedrivs effektivt och med god hushållning med statens medel, följer gällande lagar och förordningar, samt rapporteras på ett tillförlitligt och rättvisande sätt.

Internrevisionens förslag till granskningsområden presenteras i denna internrevisionsplan. Revisionsplanen innehåller även en preliminär tidplan och resursplanering för de granskningar som planeras till 2026. Stockholms universitetsstyrelse beslutar, i enlighet med Internrevisionsförordningen, om internrevisionsplanen.

2. Internrevisionsstrategi

Enligt internationell standard för internrevision ska internrevisionschefen utarbeta och genomföra en strategi för internrevisionsfunktionen som stödjer organisationens strategiska mål och framgångsfaktorer. Internrevisionsstrategin ska bland annat innehålla en vision och strategiska mål. Utifrån dessa nya krav har internrevisionen under 2025 utarbetat en internrevisionsstrategi som fastställts av internrevisionschefen under oktober 2025.

Vision:

- Internrevisionen bidrar till universitetets strategiska områden genom värdeskapande granskningar.

Internrevisionens strategiska mål:

- Vårt uppdrag är känt och förankrat i universitetets verksamheter.
- Vårt arbete leder till förbättringar av universitetets interna styrning och kontroll.
- Vi arbetar med utvärdering och utveckling av revisionen.

3. Genomförande av riskanalys

Internrevisionen genomför årligen en riskanalys i syfte att identifiera väsentliga riskområden som kan vara aktuella för granskning. Riskanalysen utgår från såväl universitetets egen riskanalys som från Internrevisionens egen riskidentifiering. I analysen bedöms även risken för korruption, otillbörlig påverkan, bedrägeri och andra oegentligheter. Internrevisionens riskanalys har skett i tre huvudsakliga steg.

Det första steget består av *inventering av risker*. I detta steg har IR gjort omvärldsbevakning och research med fokus på såväl sektorsspecifika risker som allmänna utvecklingstendenser och händelser som kan tänkas spela roll för universitetets uppdrag och måluppfyllelse. I denna del har Internrevisionen utgått från bland annat regleringsbrev till universitet och lärosäten, centrala dokument från Stockholms universitet såsom strategier, årsredovisning, verksamhetsplan och universitetets riskanalys 2025-2026, ny lagstiftning, jämförelser med andra lärosäten, erfarenheter från Internrevisionens tidigare granskningar, samt omvärldsförändringar och aktuella frågor.

Utöver inhämtande av ovan nämnda underlag har Internrevisionen även genomfört ett flertal intervjuer med utvalda ledande personer inom organisationen i syfte att inhämta information att beakta i processen för vår riskanalys. Inventeringen har utmynnat i en sammanställd bruttolista av identifierade risker.

I det andra steget har Internrevisionen *värderat de identifierade riskerna*. I detta steg har riskerna kategoriserats. Vidare har IR gått igenom huruvida området eller angränsande riskområde har granskats tidigare. Utifrån en bedömning av väsentlighet och risk har Internrevisionen sedan gjort en bedömning om granskning bör ske 2026, efterföljande år eller om granskning bör avvaktas.

I det tredje steget har bestått av *framtagande av granskningsförslag*. Framtagande av granskningsförslag har utifrån vad som bedöms granskningsbart utmynnat i beskrivningar av respektive föreslaget granskningsområde (beskrivningarna återfinns i avsnitt 4 i internrevisionsplanen).

Internrevisionens förslag till revisionsplan bereds i revisionsutskottet och presenteras för styrelsen för diskussion vid sammanträdet 24 oktober 2025. Styrelsen fattar därefter beslut om revisionsplanen vid sammanträdet 7 december 2025.

4. Översikt granskningsområden 2026

Nedan presenteras en översikt av de granskningsområden Internrevisionen föreslår ska ingå i revisionsplanen för 2026.

Ref	Granskningar/riskområden
5.1	Förebyggande arbete mot oegentligheter samt hantering av bisysslor
5.2	Lokaloptimeringsprojektet
5.3	Ansvarsfull internationalisering
5.4	Regelefterlevnad – tjänsteresor
5.5	Institutions- och avdelningsgranskningar
5.6	SUHF
5.7	Uppföljning tidigare granskningar

Internrevisionen ska bedöma risk för att verksamheten utsätts för korruption, otillbörlig påverkan, bedrägeri och andra oegentligheter. Dessa aspekter bedöms vara beaktade genom de valda granskningsområdena under 2026.

Utifrån genomförd riskanalys har ett flertal tänkbara framtida granskningar identifierats. Här kan exempelvis nämnas hantering av data på institutionsnivå; administrativa processer och effektivitet; NIS2; kontroll rörande inköp, leverantörer och fakturor; implementering av klimatfärdplan; samt efterlevnad av förvaltningslag och offentlighetsprincip.

Internrevisionen föreslår inte någon granskning inom informations- och IT-säkerhet under 2026, trots högsta risknivå i SU:s riskanalys. Internrevisionen delar uppfattningen i SU:s riskanalys att risker rörande informations- och IT-säkerhet är av största vikt att beakta och förebygga för universitetet, men området har granskats utifrån ett flertal aspekter de senaste åren och vi bedömer därför att ytterligare granskning är inte lämplig redan 2026. IT-avdelningen och dess förhållandevis nya ledning arbetar med frågan och har redan ett flertal tidigare rekommendationer från IR att förhålla sig till. IR avser istället återkomma i frågan i kommande revisionsplaner, särskild med tanke på införandet av NIS2-direktivet som ställer tydligare krav på bland annat riskanalyser och olika säkerhetsåtgärder. NIS2-direktivet kommer att genomföras i Sverige genom en cybersäkerhetslag som preliminärt träder i kraft 15 januari 2026.

5. Beskrivning av granskningsområden 2026

I detta avsnitt presenteras 2026 års granskningsområden. En fördjupad analys kommer att genomföras i samband med att varje enskild granskning inleds, i syfte att säkerställa att revisionen fokuseras på de mest väsentliga riskerna inom respektive granskningsområde.

5.1 Förebyggande arbete mot oegentligheter samt hantering av bisysslor

Regeringen har tydliggjort myndighetsledningens ansvar för att säkerställa att det finns en intern styrning och kontroll som fungerar på ett betryggande sätt. I detta ansvar ingår även att arbeta förebyggande mot korruption, otillbörlig påverkan, bedrägeri och andra oegentligheter. Förändringen trädde i kraft den 1 juli 2025.

År 2016 granskade Internrevisionen universitetets interna kontroll av lärarnas bisysslor, samt om hanteringen av dessa var förenlig med gällande regelverk. Stickprov visade att endast omkring hälften av lärarna registrerade uppgifter om bisysslor. Internrevisionen har även granskat universitetets skydd mot ekonomiska oegentligheter. Denna granskning rapporterades i februari 2019 och visade att det fanns behov av förbättringar i universitetets systematiska arbete med att förebygga och hantera upptäckta oegentligheter. Internrevisionen genomför även årligen institutions- och avdelningsgranskningar. Ett av granskningsområdena är hur institutionerna hanterar lärarnas bisysslor, samt om lärarna registrerar uppgifter om dessa i universitetets personalsystem Primula. Granskningarna visar återkommande brister i lärarnas registrering av bisysslor.

Mot bakgrund av vikten av ett systematiskt och målmedvetet arbete för att förebygga oegentligheter, samt för att uppfylla externa krav, avser Internrevisionen att granska universitetets förebyggande arbete inom detta område. En god intern styrning och kontroll är avgörande för universitetets anseende, särskilt i frågor som rör oegentligheter.

5.2 Granskning av lokaloptimeringsprojektet

Lokaloptimeringsprojektet är ett universitetsövergripande projekt som startade 2023 efter beslut av rektor. Syftet är att skapa ett mer sammanhållet och levande campus på Frescati med lokaler som används effektivt och är bättre anpassade till verksamhetens behov – både nu och i framtiden. Genom att använda lokalerna mer ändamålsenligt ska universitetets totala förhyrda ytor minska. Sedan hösten 2024 befinner sig projektet i genomförandefasen.

Projektet sträcker sig över flera år och innebär förändringar och anpassningar som i olika grad påverkar samtliga verksamheter, fastigheter och förhyrningar vid universitetet. Ett komplext, omfattande och långsiktigt projekt medför risker ur ett intern styrning- och kontrollperspektiv. Det kan finnas risk för brister i projektets styrning, riskhantering och uppföljning, vilket kan leda till att projektets mål inte nås.

Mot denna bakgrund avser Internrevisionen att granska om det finns en tillräcklig struktur för styrning, riskhantering och uppföljning som säkerställer att projektet genomförs på ett ändamålsenligt sätt i linje med uppsatta mål.

5.3 Ansvarsfull internationalisering

Geopolitiska förändringar i omvärlden ställer nya krav på svenska lärosätens förhållningssätt till internationella kontakter och samarbeten. Stockholms universitet beskriver att eftersom internationalisering är avgörande för att stärka svensk konkurrenskraft innebär detta förhållningssätt att internationella samarbeten ska bedrivas så öppet som möjligt och så säkert som nödvändigt. En ökad medvetenhet om möjliga risker behövs för att kunna fatta välgrundade beslut.

Öppenhet och samarbete är avgörande för ett lärosätes verksamhet, och det är en utmaning att samtidigt förhålla sig till ansvarsfull internationalisering. Å ena sidan behöver risker beaktas och gränsdragningar göras, å andra sidan kan risker övervärderas i relation till möjligheterna och vinsterna med internationella samarbeten, vilket inverkar negativt på den akademiska friheten och forskningssamarbeten.

Som stöd i dessa frågor finns bland annat ett internt vägledningsdokument (Forskning och studier utomlands – vägledning avseende etik och riskhantering) framtaget vid Stockholms universitet. Dokumentet innehåller bland annat vägledning, tydliggörande av krav och checklista inför utlandsvistelse.

Ett förslag föreligger om att inrätta en nationell stödfunktion för frågor om ansvarsfull internationalisering vid utbildnings-, forsknings- och innovationssamarbeten. Den



övergripande målsättningen med stödfunktionen är att den ska ge stöd och bidra till att öka kunskapen, medvetenheten och förmågan hos lärosäten, myndigheter och andra aktörer att själva agera ansvarsfullt i frågor som rör internationalisering.

Då avvägningarna mellan risker och möjligheter med internationella samarbeten kan vara svåra och löpande måste hanteras, bland annat i väntan på inrättandet av en nationell stödfunktion, avser Internrevisionen att under 2026 granska hanteringen av ansvarsfull internationalisering vid olika samarbeten.

5.4 Regelefterlevnad – tjänsteresor

Universitetets medarbetare genomför regelbundet tjänsteresor inom ramen för sin anställning. Tjänsteresor ska utföras på uppdrag av Stockholms universitetet och efter beslut av prefekt eller motsvarande. För att säkerställa kostnadseffektivitet och följsamhet till upphandlade avtal har universitetet tecknat avtal med en resebyrå som ska användas vid bokning av transport och logi. Universitetets policy för möten och resor betonar att behovet av tjänsteresor alltid ska utvärderas noggrant och att resor ska planeras och genomföras så miljöanpassat och kostnadseffektivt som möjligt.

Om medarbetare bokar resor utan att använda upphandlad resebyrå trots att universitetets regelverk endast medger undantag i begränsad omfattning kan det leda till bristande regelefterlevnad avseende avtal och styrande dokument. Det finns även andra risker kopplade till tjänsteresor såsom att universitetet belastas med kostnader som inte är kopplade till verksamheten, att dokumentation och underlag för att bedöma kostnader är otillräckliga samt att kontroll och uppföljning, som sker på institutionsnivå, inte är ändamålsenlig och fångar brister.

Internrevisionen avser därför att granska om universitetet har en tillräcklig intern styrning och kontroll avseende tjänsteresor.

5.5 Institutions- och avdelningsgranskningar

Internrevisionen ska utifrån en analys av verksamhetens risker självständigt granska om ledningens interna styrning och kontroll är utformad så att myndigheten med rimlig säkerhet fullgör sina uppgifter, uppnår verksamhetens mål och uppfyller kraven i myndighetsförordningens 3 §. Universitets styrmodell, med ett långtgående delegerat beslutsmandat ut till institutionerna, ställer höga krav på ändamålsenliga och effektiva styrstrukturer för att önskad intern styrning och kontroll ska genomsyra alla nivåer i organisationen. Med utgångspunkt i detta kommer Internrevisionen att översiktligt granska den interna styrningen och kontrollen på ett antal institutioner/avdelningar även under 2026.

5.6 SUHF

Sveriges universitets- och högskoleförbund (SUHF) bildades år 1995 och utgör ett nationellt samverkans- och intresseorgan för universitet och högskolor som bedriver högre utbildning.



Vid förbundets inrättande utsågs Stockholms universitet till värdorganisation. Detta innebär att SUHF är organisatoriskt integrerat i universitetets struktur. Förbundets ekonomiska och personaladministrativa hantering sker i enlighet med de rutiner och regelverk som tillämpas för övriga institutioner och enheter inom universitetet. Mot bakgrund av att SUHF är en del av Stockholms universitet avser internrevisionen även 2026 att granska förbundets ekonomiska redovisning, med särskilt fokus på intern styrning och kontroll.

5.7 Uppföljning tidigare granskningar och årsrapport

Internrevisionen kommer under hösten 2026 att följa upp åtgärdsarbete med anledning av tidigare internrevisionsrapporter.

I enlighet med den rutin som etablerades 2021 kommer Internrevisionen endast att följa upp de rapporter som har följts upp av rektors kansli i enlighet med den tidplan som anges i rektors yttrande. Kansliets uppföljning ingår därmed som en del av det material Internrevisionen tar del av i samband med den årliga uppföljningen. Resultatet från uppföljningen presenteras i årsrapporten, tillsammans med en sammanfattning av årets granskningar och Internrevisionens uttalande om intern styrning och kontroll i de processer som har granskats.

6. Övrigt

Internrevisionen har inga kända rådgivningsuppdrag inför 2026. Internrevisionsplanen innehåller dock en post oplanerad tid i syfte att skapa viss flexibilitet och utrymme för behovsbaserad rådgivning under året. Internrevisionen har löpande kontakter med universitetsförvaltning, fakulteter och institutioner. I dessa kontakter ingår att till viss del vara rådgivare och bollplank i främst frågor kring intern kontroll.

Internrevisionens riskanalys har identifierat ett antal riskområden där bedömningen har gjorts att det är lämpligt att avvakta med granskning till längre fram pga. exempelvis pågående utvecklingsarbete eller granskning av annat revisionsorgan. Internrevisionen arbetar löpande med omvärldsbevakning och följer relevanta områden. Under 2026 planerar Internrevisionen bland annat att bevaka utvecklingsarbetet inom AI, säkerhet, informations- och IT-säkerhet.

Internrevisionen behöver även fortsatt avsätta resurser för att anpassa arbetet i lämpliga delar efter de nya globala standarder för internrevision som tagits fram av The Institute of Internal Auditors (IIA) och trädde i kraft 9 januari 2025. En gap-analys och åtgärder identifierades under 2025, bland annat framtagande av en internrevisionsstrategi samt revidering av riktlinjer för internrevisionen. Fortsatt arbete kommer krävas i takt med att praxis och förhållningssätt till nya internrevisionsstandards utvecklas inom statliga sektorn.

Internrevisorerna vid lärosätena inom Mälardalen (SU, UU, SLU, MdU, KI, KTH, ÖrU) träffas en gång per år för erfarenhetsutbyte och fortbildning. Under 2026 kommer SU stå värd och arrangera nätverksträffen.

7. Resursplanering

Internrevisionen består av tre heltidstjänster: internrevisionschef och två internrevisorer. Resursläget inför verksamhetsåret 2026 är att samtliga tjänster är tillsatta vid tidpunkten för framtagandet av denna revisionsplan.

Nedan redovisas preliminär tidplan och resursplanering (dagar) för Internrevisionens arbete under 2026.

Resursplanering	Preliminär tidplan	Internrevisionen	Extern konsult
Granskningar och rådgivning			
Förebyggande arbete mot oegentligheter samt hantering av bisysslor	VT	X	
Ansvarsfull internationalisering	VT	X	
Lokaloptimeringsprojektet – styrning och uppföljning	HT	X	(X)
Regelefterlevnad – tjänsteresor	HT	X	
Institutions- och avdelningsgranskning	HT	X	
SUHF	VT	X	
Uppföljning och årsrapport	HT	X	
Oplanerad tid/uppdrag	VT/HT	X	
Antal dagar – granskning/rådgivning		500	
Planeringsarbete/Intern tid			
Riskanalys och revisionsplan 2027	HT	X	
Värdskap Mälardalsnätverket 2026	VT	X	
Vidareutveckling av metod och arbetssätt	Löpande	X	
Tertialrapportering och övrig administration	Löpande	X	
Internt kvalitetsarbete	Löpande	X	
Kompetensutveckling/Nätverk	Löpande	X	
Antal dagar – administration		160	
TOTALT		660	

Riktlinjer för Internrevisionen

Typ av dokument	Riktlinjer
Beslutad av	Universitetsstyrelsen
Beslutsdatum	2025-12-05
Dnr	SU FV-0003-25
Giltighetstid	2025-12-05, t.o.m./tillsvidare
Ersätter dokument	Riktlinjer för Internrevisionen, Stockholms universitet Dnr SU FV-0495-24, 2024-09-20
Ansvarig förvaltningsavdelning	Internrevisionen
Ansvarig handläggare	Tobias Björn

Beskrivning: Internrevisionen är en organisatoriskt fristående funktion placerad direkt under universitetsstyrelsen. Internrevisionen granskar och lämnar förslag till förbättring av processen för intern styrning och kontroll vid universitetet. Riktlinjer för Internrevisionen vid Stockholms universitet beslutas av universitetsstyrelsen i enlighet med 10 § internrevisionsförordningen (2006:1228). Riktlinjerna beskriver Internrevisionens syfte, uppdrag, befogenheter och arbetssätt.

1 Inledning

Internrevisionen är en organisatoriskt fristående funktion placerad direkt under universitetsstyrelsen. Internrevisionen granskar och lämnar förslag till förbättring av processen för intern styrning och kontroll vid universitetet. Riktlinjer för Internrevisionen vid Stockholms universitet beslutas av universitetsstyrelsen i enlighet med 10 § internrevisionsförordningen (2006:1228). Riktlinjerna beskriver Internrevisionens syfte, uppdrag, befogenheter och arbetsätt.

2 Internrevisionens uppdrag

Internrevisionen ska granska och lämna förslag till förbättringar av myndighetens process för intern styrning och kontroll. Internrevisionen ska utifrån en analys av verksamhetens risker självständigt granska om ledningens interna styrning och kontroll är utformad så att myndigheten med rimlig säkerhet fullgör sina uppgifter, uppnår verksamhetens mål och uppfyller kraven i 3 § myndighetsförordningen (2007:515). Internrevisionen skall omfatta den verksamhet som universitetet bedriver eller ansvarar för.

Internrevisionens arbete ska bedrivas i enlighet med bestämmelserna i Internrevisionsförordningen samt Ekonomistyrningsverkets (ESV) föreskrifter och allmänna råd/anvisningar till förordningen (SFS 2006:1228). ESV hänvisar även till det internationella regelverket för internrevision som kan ge vägledning: The Institute of Internal Auditors (IIA:s) international professional practices framework (IPPF). ESV anser att IIA:s definition och etiska riktlinjer kan tillämpas inom det svenska statliga området. Internrevisionen vid Stockholms universitet ska därför där så är tillämpligt inhämta vägledning från internationella riktlinjer för internrevisorer (IPPF) från IIA och uppfylla syfte och intention som anges i standards. Vidare ska Internrevisionen beakta de principer och standarder som anges i området för etik och yrkesmässighet, vilka är: påvisa integritet, upprätthålla objektivitet, kompetens, utöva lämplig yrkesomsorg, samt upprätthålla konfidentialitet.

3 Ansvar, befogenheter och oberoende

Internrevisionen svarar, tillsammans med verksamheten i övrigt, för att universitetsstyrelsen får underlag för att utöva sitt ansvar enligt 3 § myndighetsförordningen (2007:515), högskolelagen (1992:1434) samt kap 2 § 2 i högskoleförordningen (1993:100).

Internrevisionen är en organisatoriskt fristående funktion direkt under universitetsstyrelsen. Internrevisionen granskar och bedömer självständigt universitetets ledningsprocesser, riskhantering och den interna styrningen och kontrollen. Funktionen har en egen budget.

För att säkra efterlevnad till kraven på att bedriva en oberoende, objektiv gransknings- och rådgivningsverksamhet ska Internrevisionen inte delta operativt i den verksamhet som den är

satt att granska. Internrevisionen får inte avlasta någon funktion inom Stockholms universitet och får inte heller delta i beslut gällande universitetets verksamhet.

Internrevisionen har rätt att ta del av information och dokument i den omfattning som Internrevisionen bedömer nödvändig för att kunna fullgöra sina uppdrag. Om Internrevisionen varit förhindrad att ta del av information som är väsentlig för ett uppdrags genomförande ska Internrevisionen upplysa om det i sin rapportering och ange hur det kan ha begränsat granskningen.

4 Organisation

4.1 Universitetsstyrelsen

Styrelsen är uppdragsgivare och har det ansvar för Internrevisionen som anges i Internrevisionsförordningen (2006:1228) med tillhörande föreskrifter och allmänna råd. Här framgår det att styrelsen ska besluta om:

- Riktlinjer för internrevisionen
- Revisionsplan för internrevisionen
- Åtgärder med anledning av internrevisionens iakttagelser och rekommendationer

4.2 Revisionsutskott

Revisionsutskottet är ett beredande organ inom universitetsstyrelsen i frågor som rör den interna revisionen och dess granskning av processen för intern styrning och kontroll vid universitetet. Utskottet avrapporterar löpande sitt arbete till universitetsstyrelsen. Chefen för Internrevisionen medverkar i revisionsutskottets möten.

Internrevisionens årliga riskanalys, förslag till revisionsplan, granskningsrapporter och internrevisionens årsrapport ska diskuteras i revisionsutskottet. Internrevisionen har även möjlighet att initiera andra ärenden inom sitt ansvarsområde till revisionsutskottet.

4.3 Internrevisionschef

Chefen för Internrevisionen anställs vid Stockholms universitet efter beslut av universitetsstyrelsens ordförande. Styrelsens ordförande beslutar om lön för chefen för Internrevision, efter samråd med rektor avseende lönestrukturen inom universitetet.

Internrevisionschefen svarar för:

- Att Internrevisionens mål uppnås.

- Att årligen utarbeta ett förslag till riskbaserad revisionsplan, där föreslagna granskningar planeras med avseende på tidpunkt, omfattning, metod och interna alternativa externa resurser.
- Att säkerställa att Internrevisionen bedrivs i enlighet med interna och externa regelverk.
- Att inom ramen för budget och regelverk besluta om interna och externa specialistkompetenser för arbetet.
- Att säkra att extern kvalitetsgranskning genomförs vart femte år i enlighet med standards.

4.4 Resurser

Internrevisionen ska tillförsäkras resurser, tid och kompetens, för att kunna utföra sina arbetsuppgifter. Budget för Internrevisionen bereds av internrevisionschefen.

Internrevisionschefen ska snarast meddela universitetsstyrelsen om det saknas resurser eller kompetens för att fullgöra det revisionsarbete som planerats.

Granskning för Internrevisionens räkning kan utföras av externa konsulter vid resursbrist eller om granskningen kräver kompetens som ligger utanför Internrevisionens aktuella kunskapsområde. Internrevisionsplanen bör innehålla uppgift om vilka planerade insatser som kommer att genomföras med anställd personal respektive externa konsulter.

5 Arbetsätt

Internrevisionens bidrag till att utveckla universitetets interna styrning och kontroll kan ske genom granskningssuppdrag alternativt rådgivningssuppdrag. Arbetsätt för dessa två olika inriktningar beskrivs översiktligt nedan.

5.1 Internrevisionsgranskningar

5.1.1 Riskanalys och revisionsplan

Internrevisionen ska årligen upprätta och dokumentera en riskanalys i syfte att identifiera väsentliga riskområden som kan vara aktuella för granskning. Riskanalysen ska utgå från såväl organisationens egen riskanalys som från internrevisionens egen riskidentifiering. I analysen ingår att bedöma risken för korruption, otillbörlig påverkan, bedrägeri och andra oegentligheter.

Baserat på risk- och prioriteringsarbetet tar internrevisionschefen fram ett förslag till revisionsplan för nästkommande år. I revisionsplanen anges även om det finns aktuella områden som Internrevisionen avser att följa närmare under revisionsåret samt exempel på tänkbara framtida granskningar utifrån genomförd riskanalys.

Internrevisionens förslag till revisionsplan bereds i revisionsutskottet och presenteras för styrelsen för diskussion vid novembermötet. Styrelsen fattar därefter beslut om revisionsplanen vid decembermötet.

Väsentliga avsteg från fastställd revisionsplan under löpande kalenderår ska beslutas av universitetsstyrelsen. Med väsentligt avsteg avses att ett eller flera granskningsuppdrag i en beslutad revisionsplan utgår eller tillkommer. Revisionsutskottet kan godkänna mindre avvikelser från revisionsplanen, exempelvis förändringar i uppskattad tid för en revision eller förändrad tidplan för enskilda granskningar. Revisionsutskottet ska löpande hållas underrättat om revisionsplanens genomförande.

5.1.2 Genomföra granskning

Varje enskild granskning inleds med en fördjupad riskanalys för att säkerställa relevanta fokusområden/revisionsfrågor i granskningen. En övergripande granskningsplan och ett mer detaljerat granskningsprogram upprättas för varje enskilt granskningsuppdrag.

Bedömning av den enskilde revisorns objektivitet och Internrevisionens oberoende ska genomföras före varje granskningsuppdrag.

Internrevisionens granskningar ska dokumenteras på sådant sätt att underlag för bedömningar kan spåras. Intern kvalitetssäkring av genomförda granskningar beskrivs i avsnitt 9.

Avslutade granskningar sammanställs i en skriftlig rapport med iakttagelser, bedömningar och rekommendationer. Om Internrevisionen varit förhindrad att ta del av information som är väsentlig för ett uppdrags genomförande ska Internrevisionen upplysa styrelsen om det i sin rapportering och ange hur det kan ha begränsat granskningen.

Den som ansvarar för berörd verksamhet ska ges möjlighet att faktakontrollera rapporten och lämna synpunkter på det sakliga innehållet. Internrevisionen fastställer därefter rapporten och lämnar den till rektor för yttrande om vilka åtgärder som avses bli vidtagna med anledning av rapportens bedömningar och rekommendationer. Slutligen presenteras rapporten, tillsammans med rektors yttrande, för styrelsen som i sin tur fattar beslut om åtgärder. Internrevisionens granskningar rapporteras löpande till styrelsen i samband med avslutade rapporter.

Om internrevisionschefen anser att universitetsledningen godtar en oacceptabel risknivå ska internrevisionschefen ta upp saken med ledningen och, om bedömningen därefter kvarstår, med revisionsutskottet/styrelsen.

Iakttagelser av förhållanden som fordrar omedelbar åtgärd ska rapporteras till styrelsen och rektor så snart som möjligt, även under pågående granskning.

5.1.3 Uppföljning och årsrapport

Internrevisionen ska lämna en årsrapport till styrelsen över det gångna årets arbete. I rapporten ska resultatet från uppföljningar av tidigare granskningar samt utfört kvalitetssäkringsarbete ingå. I årsrapporten ska eventuella avvikelser från beslutad revisionsplan kommenteras. Det gäller även eventuella åtgärder som beslutats av universitetsstyrelsen men som verksamheten inte har genomfört.

Årsrapporten innehåller Internrevisionens bedömning av myndighetens interna styrning och kontroll inom ramen för genomförda granskningar. Internrevisionens årsrapport ska presenteras så att det kan vara en del av underlaget för styrelsens uttalande om intern styrning och kontroll i årsredovisningen.

5.2 Rådgivningsuppdrag

Styrelsen och rektor kan även tilldela Internrevisionen enskilda rådgivningsuppdrag om det uppstår behov av särskilda utredningar eller annan form av rådgivning avseende universitetets interna styrning och kontroll.

Internrevisionschefen avgör om ett rådgivningsuppdrag kan antas i mån av resurser, kompetens och med utgångspunkt om uppdraget bedöms kunna förbättra organisationens interna styrning och kontroll. Internrevisionschefen avgör även om uppdraget kan antas utan att påverka Internrevisionens oberoende ställning. Större kända utredningar/rådgivningsuppdrag ska inkluderas i Internrevisionens revisionsplan.

Syfte, omfattning och form för avrapportering av antagna rådgivningsuppdrag/särskilda utredningar utformas i samråd med beställaren, utifrån identifierat behov. Om ett rådgivningsuppdrag identifierar väsentliga brister i myndighetens interna styrning och kontroll ska detta rapporteras till styrelsen under pågående uppdrag.

Internrevisionen kan i rådgivande syfte delta i referensgrupper till projekt och andra möten, under förutsättning att Internrevisionens oberoende ställning inte påverkas

6 Kommunikation

Styrelsen och revisionsutskottet

Internrevisionschefen har närvaro- och yttranderätt vid styrelsens sammanträden.

Regelbundna möten ska ske mellan internrevisionschef och revisionsutskott. Dessa möten ska ge möjlighet till att bland annat bereda Internrevisionens ärenden samt till avstämning av aktuella frågor.

Universitetsledningen

Internrevisionschefen ska ha regelbundna avstämningsmöten med rektor och universitetsdirektör.

Internrevisionen ska underrättas vid förändring i till exempel organisation eller riskstrategi som kan påverka verksamhetens riskprofil.

7 Samverkan

Riksrevisionen

Internrevisionen och Riksrevisionen kommunicerar revisionsplan, granskningsrapporter samt årsrapport till varandra i syfte att dela information och säkerställa att planerade granskningar ej överlappar varandra.

Intern samverkan

Internrevisionen bör ha en kontinuerlig dialog med universitetsförvaltningens avdelningar samt de två vetenskapsområdena för gemensamt erfarenhetsutbyte och information om pågående verksamhet. Internrevisionen bör informera berörda delar av verksamheten om årets revisionsplan. Internrevisionsrapporter som berör väsentliga delar av verksamheten bör publiceras på medarbetarwebben för information.

Internrevisionen ska ha informationsutbyte med andra funktioner inom universitetet som har en granskande roll, exempelvis verksamhetsrevisorerna och dataskyddsombud, i syfte att undvika dubbelarbete mellan de olika funktionernas granskningar och för att undvika onödig belastning av verksamheten.

8 Kompetensutveckling

Internrevisorerna ska besitta de kunskaper, färdigheter och annan kompetens som behövs för att kunna fullgöra sitt uppdrag. Internrevisionen ska fortlöpande utveckla sin yrkeskompetens utifrån upprättade kompetensutvecklingsplaner.

Internrevisorerna som är certifierade (CIA respektive CISA) ska ges utrymme för tillräcklig kompetensutveckling för att kunna upprätthålla certifieringen.

Internrevisionschefen ska erbjudas utvecklingssamtal med styrelseordförande.

9 Kvalitetssäkring och uppföljning

Intern kvalitetssäkring

Internrevisionschefen ska löpande följa upp att utförda gransknings- och rådgivningsuppdrag utförs i enlighet med denna riktlinje, interna styrdokument och mallar, aktuell internrevisionsplan samt budget. Internrevisionschefen ska årligen följa upp om riktlinjerna efterlevs samt bedöma behov av uppdatering.

Internrevisionschefen ansvarar för att årligen undersöka hur funktionen uppfattas och använda resultatet i kvalitetsförbättrande syfte i enlighet med program för kvalitetsförbättring inom internrevisionen. Arbetet innefattar bland annat årlig självutvärdering av internrevisionsprocessen med stöd av ESV:s årliga enkät om myndigheters internrevision, självutvärdering utifrån internrevisionsstandards samt årlig utvärdering av Internrevisionens arbete genom en enkät till revisionsutskottet.

Resultatet av den interna kvalitetssäkringen presenteras för Revisionsutskottet, samt rapporteras till universitetsstyrelsen genom avlämnandet av Internrevisionens årsrapport.

Extern kvalitetssäkring

Internrevisionens verksamhet ska genomgå kvalitetsutvärdering av en extern part vart femte år. Internrevisionschefen ska ta initiativet till en extern utvärdering i samråd med revisionsutskottet.



Handläggare:
Clara Ersson
Verksamhetscontroller
Rektors kansli

Rektors yttrande över internrevisionens granskning av universitetets informations- och IT-säkerhetskultur

Internrevisionen har under 2025 granskat universitetets informations- och IT-säkerhetskultur. Syftet med granskningen har varit att bedöma om universitetet har en intern styrning och kontroll som säkerställer en god informations- och IT-säkerhetskultur i enlighet med krav i lag, föreskrifter och interna styrdokument.

Den samlade bedömningen är att den interna styrningen och kontrollen inom området är *bristfällig*.

Internrevisionens iakttagelser och rekommendationer från granskningen sammanfattas i rapporten ”Granskning av informations- och IT-säkerhetskultur” (dnr SU FV-0003-25, daterad 17 oktober 2025). Rapporten är ställd till universitetsstyrelsen och ger en övergripande bild av utfört granskningsarbete och resultat.

Internrevisionens rekommendationer

Med anledning av granskningen rekommenderar internrevisionen följande:

1. Etablera ansvar och aktiviteter för att höja personalens kunskap och medvetenhet inom informations- och IT-säkerhet.
2. Utveckla incidentrapporteringen avseende process samt uppföljning och rapportering.
3. Beakta identifierade utvecklingsområden utifrån genomfört manipulationstest.

Rektors yttrande

Rektors yttrande över rapporten, som avges i samråd med universitetsdirektören, följer nedan.

Rektor konstaterar att det är av största vikt att universitetet har en god informationssäkerhet, och internrevisionens granskning och rekommendationer är ett värdefullt stöd i det fortsatta arbetet.

Mot bakgrund av internrevisionens granskning av IT-säkerhet som diskuterades i universitetsstyrelsen den 28 april beslutade rektor innan sommaren att uppdra till

universitetsdirektören att ta fram en plan i syfte att långsiktigt höja nivån på IT-säkerhetsarbetet och säkerställa en god IT-säkerhetsmiljö. Åtgärdsplanen som är under framtagande omfattar både informations- och IT-säkerhet och de ingående aktiviteternas prioritering bygger på aktuella riskanalyser. Åtgärdsplanen kommer sträcka sig fram till 2028, och inkluderar flera planerade åtgärder som syftar till att flytta fram positionerna avseende det systematiska förbättringsarbetet inom informations- och IT-säkerhetsområdet, höja personalens kunskap och minska sårbarheter. Grundprincipen för arbetet med åtgärdsplanen är att de allvarligaste bristerna ska prioriteras och åtgärdas först, varför rektor inte avser att ge specifika tidsatta uppdrag för åtgärder som planeras att omhändertas inom ramen för planen. Åtgärdsplanen kommer i enlighet med uppdraget att presenteras för styrelsen vid sammanträdet den 22 april 2026.

Parallellt med arbetet med att ta fram åtgärdsplanen arbetar universitetet bland annat med att stärka det operativa IT-säkerhetsarbetet, vilket innefattar både förstärkning av personella resurser, att hantera operativa ärenden mer systematiskt, och förbättra stödet till kärnverksamheten i frågor som inte kan hanteras centralt.

En biträdande informationssäkerhetschef har rekryterats och börjar i januari vilket innebär en förstärkning på både operativ och strategisk nivå. Rekrytering pågår av två IT-säkerhetsspecialister som kommer att stärka universitetets operativa IT-säkerhetsarbete ytterligare.

För att ge ett bättre och mer effektivt stöd till kärnverksamheten har sektionen för informations- och IT-säkerhet förändrat sitt arbetssätt. Arbetet är nu organiserat i produktområden som fokuserar på olika delar av ledningssystemet för informationssäkerhet (LIS), exempelvis utbildning. Varje produktområde har en utsedd kontaktperson som ansvarar för samordning och samverkan med verksamheten. Produktområdena är utformade för att möta kärnverksamhetens behov och främja en kultur där informations- och IT-säkerhet är en naturlig del av arbetet.

Vidare pågår ett flertal åtgärder med anledning av tidigare granskningar av fysisk säkerhet i IT-utrymmen respektive IT-säkerhet. Bland annat förväntas flera styrdokument om informations-säkerhet fastställas före jul. Förslag som nu är på internremiss omfattar bland annat regler för fysisk säkerhet i IT-utrymmen samt universitetets besluts- och delegationsordning. Dessutom vidtas åtgärder för att införa ett mer systematiskt arbetssätt vid hantering av bristfälliga säkerhetsinställningar och konfigurationer. En annan prioriterad åtgärd för att stärka IT- och cybersäkerheten vid universitetet är att införa tvåfaktorsautentisering (MFA) i den centrala identitetsplattformen SUKAT. Införandet är planerat till första kvartalet 2026.

1. Internrevisionens rekommenderar:

Etablera ansvar och aktiviteter för att höja personalens kunskap och medvetenhet inom informations- och IT-säkerhet.

Rektors yttrande

Internrevisionen bedömer att interna styrdokument brister i reglering av ansvar för åtgärder i syfte att etablera en säkerhetskultur och kunskap hos medarbetare.

Rektor konstaterar att behovet av kompetensutveckling varierar beroende på medarbetarens bakgrund, arbetsuppgifter och verksamhetens specifika förutsättningar.

Det är en del av chefernas ansvar att säkerställa att medarbetarna har den kunskap som krävs för att utföra sitt arbete utifrån verksamhetens behov. Chefer förväntas verka för att gällande regelverk följs, ge sina medarbetare möjlighet att tillgodogöra sig nödvändig kunskap exempelvis genom att delta i relevanta utbildningar som erbjuds vid universitetet och informera nyanställda om var viktig information finns.

Prefekter och andra chefer inom kärnverksamheten förväntas ta del av det stöd som universitetsförvaltningen erbjuder och bidra till erfarenhetsutbyte inom organisationen. Det är dock viktigt att tydliggöra att prefekter och andra chefer inom kärnverksamheten inte förväntas att själva utveckla utbildningar inom informationssäkerhet.

Universitetsförvaltningen har ansvar för att tillhandahålla utbildningstillfällen, inklusive introduktionsutbildning för nyanställda. Medarbetare har också ett eget ansvar att inhämta den kunskap som krävs för att utföra sitt arbete.

I praktiken låter ansvaret för säkerhetskulturen sig inte lätt definieras i ett styrdokument. Istället krävs samverkan mellan chefer, medarbetare och specialister vid universitetsförvaltningen i frågor som rör utbildning, informationsinsatser, erfarenhetsutbyte och stöd.

Ansvaret för olika aspekter av informations- och IT-säkerhetsarbetet har nyligen förtydligats i *Handläggningsordning för ansvarsfördelning och vägledning avseende säkerhetsåtgärder i informationssystem vid Stockholms universitet*¹. Inom ramen för åtgärdsplanen som är under framtagande övervägs ytterligare förtydliganden av ansvar för vissa specifika roller såsom systemägare och incident manager.

Inom ramen för åtgärdsplanen som är under framtagande planeras ett utbildningspaket utvecklas, där medarbetare kan erhålla en rollanpassad utbildning inom informations- och IT-säkerhet.

Rektor instämmer i internrevisionens bedömning att Nimblr och dess utbildningsinnehåll är ett bra verktyg, och att det vore värdefullt om uppföljningen av utbildningen kunde stärkas. För att

¹ Fastställt 2025-04-16, dnr SU FV-1582-25

möjliggöra en mer effektiv uppföljning bör det utredas om det är möjligt att utveckla systemet så att prefekter/motsvarande kan få tillgång till statistik för genomgången utbildning för sina medarbetare. Det är vidare viktigt att säkerställa att alla anställda inkluderas i utbildningen. Nimblr bör integreras med Stockholms universitets centrala identitetsplattform så att alla anställda inkluderas i utbildningen per automatik.

Arbetet med att utveckla Nimblr är påbörjat. Ett inledande möte om den kommande utvecklingen har redan genomförts tillsammans med Nimblr. Integrationen mellan Nimblr och universitetets identitetsplattform innebär att både Nimblr och universitetet behöver genomföra ett utvecklingsarbete. Syftet med integrationen är att säkerställa att medarbetare automatiskt får tillgång till Nimblr-utbildningar vid anställning och att behörigheter tas bort vid avslutad anställning. En förbättrad integration möjliggör även att Nimblr automatiskt kan tillhandahålla sammanställningar om medarbetares kursdeltagande till prefekter och avdelningschefer. Målsättningen är att integrationen ska genomföras under det andra kvartalet 2026, men tekniska utmaningar kan uppstå som kan komma att påverka förutsättningarna för arbetet.

Åtgärd: Rektor avser att uppdra till universitetsdirektören att fortsätta arbetet med hur uppföljning av den webbaserade IT-säkerhetsutbildningen med kursmoduler kan utvecklas, samt att integrera utbildningsplattformen i Stockholms universitets centrala identitetsplattform.

2. Internrevisionens rekommenderar:

Utveckla incidentrapporteringen avseende process samt uppföljning och rapportering.

Rektors yttrande

Ett utvecklingsarbete avseende rapportering av incidenter har genomförts de senaste åren, och incidentrapporteringsrutiner enligt ITIL² finns på plats. Informationen om hur informations- och IT-säkerhetsincidenter rapporteras har under hösten förtydligats på medarbetarportalen och inuti Serviceportalen. Inom ramen för åtgärdsplanen som är under framtagande diskuteras möjligheter att stärka uppföljningen ytterligare. Grundprincipen för arbetet med åtgärdsplanen är dock att de allvarligaste bristerna ska prioriteras och åtgärdas först. I nuläget har universitetsförvaltningen bedömt att andra åtgärder har högre prioritet.

Åtgärd: Rektor avser att uppdra till universitetsdirektören att genomföra insatser för att öka kännedomen om hur informations- och IT-säkerhetsincidenter ska rapporteras.

² ITIL (Information Technology Infrastructure Library) är ett vedertaget ramverk för att hantera IT-tjänster.

3. Internrevisionens rekommendarar:

Beakta identifierade utvecklingsområden utifrån genomfört manipulationstest.

Rektors yttrande

Rektor ser med stor oro på resultaten från internrevisionens nätfiskekampanj där ett stort antal medarbetare klickat på länken.

För att underlätta identifiering av misstänkta mejl bedömer rektor att det vore värdefullt att aktivera funktionen för varningsbanner för mejl från externa avsändare ("external sender tag") i universitetets mejltjänst.

Avseende noteringen att programvaruuppdatering inte var gjorda kan nämnas att det mot bakgrund av internrevisionens granskning av IT-säkerhet som diskuterades i universitetsstyrelsen den 28 april pågår ett arbete för att åtgärda brister i mjukvaruuppdateringar. Detta inkluderar införande av automatiska uppdateringar där det är tekniskt möjligt för universitetens gemensamma infrastrukturer. Rektor har även gett universitetsdirektören i uppdrag att utreda förutsättningarna för att genomföra regelbundna sårbarhetsskanningar vid universitetet.

Internrevisionen påpekar att incidentrapporteringen till IT-avdelningen var mycket låg. I praktiken rapporteras nätfiske sällan av enskilda medarbetare, utan av institutionernas dator- och systemansvariga. I det här fallet uppmärksammade dessa funktioner snabbt att mejlet kom från internrevisionen och detta spreds även bland kollegor, vilket sannolikt påverkat rapporteringsgraden och gör att den inte kan ses som representativ för en verklig attack.

Åtgärd: Rektor avser att uppdra till universitetsdirektören att utreda förutsättningarna för att konfigurera funktionen varningsbanner i universitetets mejltjänst.

Rektors yttrande, övrigt

Rektor noterar att det finns ett missförstånd i rapporten avseende bakgrundskontroller vid rekrytering (sid. 12). Vid universitetet sker rekryteringsprocesser med intervjuer och referenstagning. För lärare är processen än mer gedigen med sakkunnigutlåtanden vad gäller akademiska meriter. När det finns lagstadgad skyldighet att genomföra säkerhetsåtgärder t.ex. vid säkerhetsskydd och strålskydd, så hanteras detta av säkerhetsfunktionen. I rekryteringar är det viktigt att kontroller av potentiella medarbetare är nödvändiga, proportionerliga och har en tydlig rättslig grund i förhållande till de arbetsuppgifter som ska genomföras. Därmed bedöms Stockholms universitets rekryteringsförfarande uppfylla MSB:s föreskrift och allmänna råd rörande säkerhetsåtgärder vid rekrytering.

Uppdragen ska återrapporteras till rektor senast den 30 juni 2026.

Internrevisionen

Granskning av informations- och IT-säkerhetskultur

Revisionsrapport från Internrevisionen

Universitetsstyrelsen den 5 december 2025

Sammanfattning och rekommendationer

Internrevisionen (IR) har i enlighet med internrevisionsplanen för 2025 granskat universitetets informations- och IT-säkerhetskultur. Syftet med granskningen har varit att bedöma om universitetet har en intern styrning och kontroll som säkerställer en god informations- och IT-säkerhetskultur i enlighet med krav i lag, föreskrifter och interna styrdokument.

IR:s sammantagna bedömning är att universitetets interna styrning och kontroll är *bristfällig*¹ och behöver stärkas i syfte att säkerställa en god informations- och IT-säkerhetskultur i enlighet med krav i lag, föreskrifter och interna styrdokument. På en övergripande nivå bedöms det saknas tillräcklig styrning för att säkerställa efterlevnad till MSBFS 2020:6 och det bedöms även saknas en tillräcklig intern styrning och kontroll för att säkerställa följsamhet till regelverk. IR lämnar emellertid inga nya rekommendationer rörande det övergripande systematiska informationssäkerhetsarbetet. Tidigare granskningar har fångat utvecklingsbehov rörande systematiskt informationssäkerhetsarbete och IR är medveten om att utvecklingsarbete pågår i relation till tidigare lämnade rekommendationer inom området.

På en övergripande nivå bedöms Nimblr och dess utbildningsinnehåll vara ett bra verktyg för att höja medvetenheten och säkerhetskulturen men det behöver kompletteras med fler åtgärder och dess genomförande och uppföljning behöver stärkas. IR bedömer att befintliga rutiner för genomförande av säkerhetsåtgärder i syfte att uppnå kunskap och mognad hos medarbetare inom informations- och IT-säkerhetsområdet är bristfälliga. IR bedömer att det finns risk för att nuvarande insatser inte är tillräckliga för att uppnå en godtagbar kunskap och säkerhetskultur. Det mognadstest som genomförts inom ramen för granskningen påvisar att universitetet har en förhöjd risk för både ekonomisk skada och förtroendeskada om informationssäkerhetshot riktas mot medarbetare.

IR lämnar följande rekommendationer i syfte att stärka den interna styrning och kontrollen inom det granskade området:

1. Etablera ansvar och aktiviteter för att höja personalens kunskap och medvetenhet inom informations- och IT-säkerhet.
2. Utveckla incidentrapporteringen avseende process samt uppföljning och rapportering.
3. Beakta identifierade utvecklingsområden utifrån genomfört manipulationstest.

Tobias Bjöörn
Internrevisionschef

¹ Internrevisionen använder följande fyra nivåer i sin bedömning av den interna styrningen och kontrollen: tillfredställande, förbättringsmöjligheter, bristfällig samt otillfredsställande.

Innehåll

SAMMANFATTNING OCH REKOMMENDATIONER	2
1. INLEDNING	4
1.1 Bakgrund och syfte	4
2. OMFATTNING OCH METOD	5
2.1. Avgränsning och revisionskriterier.....	5
3. GRANSKNINGSRESULTAT.....	7
3.1. Interna regelverk inom informationssäkerhet	7
3.1.1 Ansvar för intern styrning och kontroll inom Stockholms universitet	7
3.1.2 Säkerhetspolicy och informationssäkerhetspolicy	7
3.1.3 Handläggningsordning för informationssäkerhet.....	8
3.1.4 Regler för organisation och genomförande av dataskydd.....	8
3.1.5 Digitaliseringsplan.....	8
3.1.6 Ansvarsfördelning inom informationssäkerhet enligt interna styrdokument	8
3.1.7 Bedömning.....	9
3.2. Kunskap och mognad hos medarbetare inom informations- och IT-säkerhet.....	10
3.2.1 Rutiner och arbetssätt för att etablera kunskap och mognad	10
3.2.2 Genomförande av utbildningsinsatser	10
3.2.3 Uppföljning av insatser	12
3.2.4 Säkerhetsåtgärder vid rekrytering	12
3.2.5 Bedömning.....	12
3.3 Incidenthantering	13
3.3.1 Incidenthanteringsrutiner.....	13
3.3.2 Bedömning.....	14
3.4 Socialt manipulationstest.....	14
3.4.1 Bedömning.....	15
3.5 Sammanfattande bedömning och rekommendationer	17
Bilaga 1 Sammanställning över granskad dokumentation	18

1. Inledning

1.1 Bakgrund och syfte

Informationssäkerhet och IT-säkerhet har fått allt större fokus de senaste åren i samhället. I regleringsbrev för universitet och högskolor 2025 ställs även krav på redogörelse hur lärosätet har arbetat för att förvalta och utveckla sin informationssäkerhet. Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) reglerar att myndigheter ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001 och 27002. I föreskriftens § 9 regleras åtgärder som myndigheten ska vidta för att säkerställa att personal behandlar information på ett säkert sätt. Bland annat framgår att bakgrundskontroller ska göras samt att kompetens behöver säkerställas och hållas uppdaterad genom utbildning, informationsinsatser och övning.

Inom universitetet hanteras värdefulla informationstillgångar. Forskare och forskargrupper samarbetar ofta med forskare i andra länder och kontaktytorna utnyttjas i allt högre grad av fientliga intressen som kan stjäla, förvanska eller förstöra forskningsdata. En svag informations- och IT-säkerhetskultur kan leda till att forskning går förlorad, och kan även medföra att forskningsfinansierare kan ifrågasätta universitetets skydd och hantering av data.

Sedan 2023 har ett flertal webbaserade utbildningsmoduler genomförts inom ramen för Stockholm universitets IT-säkerhetsutbildning. Syftet har varit att minska riskerna för IT-angrepp och öka personalens medvetenhet om IT-säkerhet.

Utifrån områdets omfattning och de risker som Internrevisionen bedömt föreligger har en granskning rörande informations- och IT-säkerhetskultur föreslagits i revisionsplanen 2025 som beslutades av universitetsstyrelsen 25 november 2024².

Syftet med granskningen har varit att bedöma om universitetet har en intern styrning och kontroll som säkerställer en god informations- och IT-säkerhetskultur i enlighet med krav i lag, föreskrifter och interna styrdokument.

Följande revisionsfrågor ingår för att besvara syftet:

1. Reglerar interna styrdokument hur ansvaret för informations- och IT-säkerhetsområdet inom universitetet är fördelat?
2. Har universitetet etablerade rutiner för genomförande och uppföljning för att uppnå kunskap och mognad hos medarbetare inom informations- och IT-säkerhetsområdet?
3. Finns kännedom om rapporteringsrutiner vid misstänkta eller inträffade incidenter kopplade till medarbetares användning av digitala system?
4. Bedöma nivå på universitetets mognad avseende informations- och IT-säkerhet.

² Stockholms universitet, *Internrevisionsplan 2025*, beslutad av universitetsstyrelsen 2024-10-31, Dnr SU FV-0495- 24.

2. Omfattning och metod

Internrevisionen har genomförts genom dokumentstudier, intervjuer samt ett socialt manipulationstest.

- Dokumentstudier har omfattat analys av tillämpliga interna regelverk och internt framtaget material inom informationssäkerhetsområdet. Se bilaga 1 för sammanställning av dokumentation.
- Intervjuer har genomförts med chef IT-avdelningen, personalchef, informationssäkerhetschef (CISO), dataskyddsbud och universitetsjurist, enhetschef IT-avdelningen med ansvar för service och support samt funktion inom IT-avdelningen med ansvar för utbildning. Ett urval av intervjupersoner från två institutioner har gjorts. Funktioner som deltagit har varit professor tillika föreståndare och administrativ chef för Stockholms Resilienscentrum. För Institutionen för slaviska och baltiska språk, finska, nederländska och tyska har professor tillika prefekt samt administrativ chef intervjuats.

Samtliga intervjuade har givits möjlighet att faktagranska ett utkast av rapporten innan färdigställandet.

- I syfte att testa säkerhetsmedvetenhet och säkerhetskultur ingår i revisionen ett socialt manipulationstest. Detta innebär att internrevisionen skickar ut ett mejl med en länk för att se hur många medarbetare hos universitetet som klickar på länken, öppnar meddelandet, lämnar uppgifter samt eventuellt incident-rapporterar händelsen. Resultatet av testet utgör underlag för bedömning av revisionsfråga fyra. Resultatet av testet utgör underlag för bedömning av revisionsfråga fyra.

Granskningen har genomförts i samverkan mellan IR och upphandlade konsulter från KPMG³.

2.1. Avgränsning och revisionskriterier

Revisionskriterier för granskningen har utgjorts av:

- Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter 2020:6 §4, §5, §9
- ISO 27002 avsnitt 6, Personrelaterade säkerhetsåtgärder (i tillämpliga delar)
- Förordning (2007:603) om intern styrning och kontroll
- Universitetets styrdokument, rutiner samt beslut
- Föreskrifter för statliga myndigheter inom informationssäkerhet

³ Enligt de villkor och under de förutsättningar som framgår av ramavtalet SU FV-0849-25 och avropsförfrågan SU FV-1427-25.

Granskningen har inriktats på universitets medarbetare och inte dess studenter.

Stockholms universitet har inom informationssäkerhetsområdet att förhålla sig till de av Myndigheten för samhällsskydd och beredskap utfärdade föreskrifterna MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter och MSBFS 2020:7 föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter. Dessa föreskrifter innehåller bestämmelser om säkerhetskrav som avses i 19 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Ett grundkrav för alla organisationer enligt föreskrifterna är att Myndigheten ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav och SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder eller motsvarande.

Föreskriften tydliggör kraven på åtgärder för att säkerställa att personal behandlar information på ett säkert sätt. Enligt 9 § i MSBFS 2020:6 framgår att Myndigheten ska:

1. anpassa bakgrundskontroller av egen och inhyrd personal utifrån vilken information personalen ska få åtkomst till
2. hålla egen och inhyrd personal informerad om relevanta interna regler, arbetssätt och stöd
3. utvärdera att interna regler, arbetssätt och stöd används på avsett sätt
4. säkerställa att egen och inhyrd personal med utpekade roller i informationssäkerhetsarbetet har tillräcklig kompetens för att kunna utföra sina arbetsuppgifter
5. utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet genom utbildning, informationsinsatser och övning

I ISO 27002 som preciserar kontroller för samtliga säkerhetsåtgärder används terminologin *Personalrelaterade säkerhetsåtgärder* som utgör ett eget avsnitt i standarden (avsnitt sex). De områden som ingår speglar delvis ovan nämnda krav enligt MSB:s föreskrifter men är mer detaljerade. De områden som beskrivs i kontrollerna är; Bakgrundskontroller, Anställningsvillkor, Medvetenhet och utbildning inom informationssäkerhet, Disciplinära processer, Ansvar efter upphörande eller ändring av anställning, Avtal om konfidentialitet och sekretess, Distansarbete samt Rapportering av informationssäkerhetsincidenter. Universitetets CISO har valt att bedriva informationssäkerhetsarbetet enligt NIST⁴ vilket IT-avdelningen bedömt likvärdigt vad gäller krav på systematik och säkerhetsåtgärder.

⁴ NIST står för National Institute of Standards and Technology och är en amerikansk statlig myndighet som utvecklar standarder och ramverk, framförallt inom cybersäkerhet

3. Granskningsresultat

3.1. Interna regelverk inom informationssäkerhet

3.1.1 Ansvar för intern styrning och kontroll inom Stockholms universitet

I universitetets arbetsordning fastställd av styrelsen⁵ finns en hänvisning till högskoleförordningen 2 kap. 2 § om att ska universitetsstyrelsen säkerställa att det vid högskolan finns en intern styrning och kontroll som fungerar på ett betryggande sätt. Samma hänvisning framgår av rektors fastställda besluts- och delegationsordning⁶. Rektor har också fastställt en handläggningsordning för intern styrning och kontroll⁷ som bland annat innehåller hänvisningar till internrevisionsförordningen, förordning om intern styrning och kontroll samt myndighetsförordningen. I detta dokument anges att processen för intern styrning och kontroll är integrerad i ordinarie styrning som regleras genom olika styrdokument bland annat universitetets arbetsordning och besluts- och delegationsordningar.

3.1.2 Säkerhetspolicy och informationssäkerhetspolicy

Det finns interna regelverk som reglerar arbetet med informationssäkerhet. Bland annat finns en Säkerhetspolicy⁸ som uppges vara det övergripande styrdokumentet för informationssäkerheten och den fysiska säkerheten vid Stockholms universitet. Enligt säkerhetspolicyn konkretiseras denna genom Riktlinjer för informationssäkerhet och Riktlinjer för fysisk säkerhet. Nu gällande Säkerhetspolicy har enligt uppgift i dokumentet aktualitetsgranskats under 2024 med planerad revidering senare under 2024. Revideringen har enligt uppgift senarelagts för att ge den nya ledningen möjlighet att sätta sin prägel på arbetet. Vid tidpunkten för granskningen var revideringen pågående.

Vi har tagit del av Informationssäkerhetspolicy⁹. Denna ska enligt uppgift i underlaget ersätta Riktlinjer för informationssäkerhet som Säkerhetspolicyn ovan hänvisar till. Informationssäkerhetspolicyn är enligt underlaget en del av Stockholms universitets ledningssystem för informationssäkerhet. Syftet med policyn är att lägga grunden för ett systematiskt arbete med informationssäkerhet som ger ett ändamålsenligt och välavvägt skydd och kvalitet i universitetets informationshantering. Policyn beskriver mål, organisation, övergripande roller och ansvar inom informationssäkerhetsområdet.

⁵ Arbetsordning vid Stockholms universitet, fastställd av universitetsstyrelsen 2024-11-25 att gälla fr.o.m. 2025-01-01 (dnr: SU FV-3298-24).

⁶ Besluts- och delegationsordning för Stockholms universitet, 2024-12-19 (dnr: SU FV-4158-24).

⁷ Handläggningsordning för intern styrning och kontroll, 2024-12-04 (dnr: SU FV-3412-24).

⁸ Beslut 2017-01-26, Dnr SU FV-2.11.2-1922-16, framgår ej av underlaget vem som beslutat, dock finns rektors beslutsprotokoll som styrker att policyn beslutats av rektor.

⁹ Beslutad av rektor 2023-06-01

3.1.3 Handläggningsordning för informationssäkerhet

En handläggningsordning finns för att tydliggöra kravbild med grund i MSBFS 2020:7 föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter.

Enligt intervjuade syftar handläggningsordningen till att tydliggöra de gemensamma krav som samtliga universitetsverksamheter har att efterleva vad gäller de tekniska säkerhetsåtgärderna (IT-säkerhet). Detta som en följd av att flera institutioner tillhandahåller egen IT-utrustning, system och digitala verktyg.

Vi noterar vid dokumentgranskning att denna inte reglerar säkerhetsåtgärder i syfte att etablera kunskap och säkerhetskultur. Däremot tydliggörs ansvar till viss del i handläggningsordningen.

3.1.4 Regler för organisation och genomförande av dataskydd

Vid universitetet finns en samordningsgrupp för säkerhetsfrågor som ska verka för ett effektivt och systematiskt säkerhetsarbete inom områdena informations- och IT-säkerhet, fysisk säkerhet, dataskydd, säkerhetsskydd och kris- och kontinuitetshantering. Samordningsgruppen ska bland annat se till att samordning sker av styrdokument och handlingsplaner och säkerställa att universitetets incidenthantering är samordnad och effektiv. Samordningsgruppen består av säkerhetschef (ordförande), informationssäkerhetschef, gruppchef för arbetarskydd och dataskyddsombud. Ytterligare funktioner kan adjungeras till gruppen.¹⁰

3.1.5 Digitaliseringsplan

Digitaliseringsplan för Stockholms universitet 2024–2026¹¹ inkluderar ett delmål om att all personal på universitetet behöver ha en grundläggande kompetens i och ska erbjudas förutsättningar för att kunna använda digital teknik på ett säkert, effektivt och ansvarsfullt sätt.

3.1.6 Ansvarsfördelning inom informationssäkerhet enligt interna styrdokument

Enligt interna regelverk¹² har rektor det övergripande ansvaret för informationssäkerheten och den fysiska säkerheten vid Stockholms universitet. Ansvaret är därutöver en integrerad del i verksamhetsansvaret och följer universitetets besluts- och delegationsordning. Det innebär att chefer för verksamhet också ansvarar för säker hantering av verksamhetens information. Informationsägare är en term som används inom informationssäkerhetsområdet. Rollen innehas främst av prefekt/föreståndare eller avdelningschef.

Vad gäller säkerhetskultur framgår av informationssäkerhetspolicyn att arbetet ska vara en integrerad del av medarbetarens ansvar för den egna verksamheten. Den viktigaste delen i att

¹⁰ Avsnitt 6.9 i Regler för organisation och genomförande av dataskydd vid Stockholms universitet, sid 14. 2024-12-19 (dnr: SU FV-3115-24)

¹¹ Beslutad av rektor 2024-02-08 (Dnr SU FV-0431-23)

¹² Säkerhetspolicy samt Informationssäkerhetspolicy

skapa en säker informationshantering är alltid medarbetarnas kunskap, medvetenhet och motivation. Ett av målen med informationssäkerhetsarbetet är enligt informationssäkerhetspolicyen att universitetet ska ha en utvecklad säkerhetsmedvetenhet och uppmuntra till engagemang hos alla medarbetare och därtill följa gemensamma regler. Medarbetare eller andra informationshanterare ska vara utbildade och kunniga i informationssäkerhet i relation till sin roll.

Det finns en intern föreskrift från 2014 för användning av information och informationshanderande resurser¹³ som riktar sig till anställda vid Stockholms universitet samt till personer som arbetar på uppdrag av universitetet. I föreskriften framgår regler och förhållningssätt. Det framgår också i föreskriften att fel, brott och brister mot föreskriften eller lagområden ska anmälas. Prefekt eller motsvarande har mandat att besluta om anmälan ska göras till personalansvarsnämnden eller anmälas till åtal. I övriga ärenden kan funktionen för informationssäkerhet besluta om åtgärder såsom avstängning av konto samt tillgång till universitetets informationshanderande resurser i avvaktan på vidare utredning. Baserat på genomförda intervjuer är kännedom om denna föreskrift svag och dess nyttjande har inte kunnat verifieras. Enligt uppgift ska undertecknade ansvarsförbindelser skickas till personalavdelningen som ska förvara dessa. Enligt representant från personalavdelningen så är det inget som de ansvarar för. I intervju hänvisas frågeställningen vidare till IT-avdelningen eller institutionerna. Representanter som deltagit i granskningen känner inte till att föreskriften signeras av medarbetare. Det saknas därtill kännedom om ansvar och tillvägagångssätt vid bristande hantering och avvikelser där intervjuade inte känner till några disciplinära åtgärder vid överträdelser.

3.1.7 Bedömning

IR bedömer att informations- och IT-säkerhetsområdet inom universitetet är fördelat i interna styrdokument och säkerhetskultur ingår i delvis, dock avser detta främst ansvar på en övergripande nivå. Interna styrdokument brister i reglering av ansvar för åtgärder i syfte att etablera säkerhetskultur och kunskap hos medarbetare samt riktlinjer för hur detta ska uppnås. Den samlade bedömningen i denna del är att området är bristfälligt.

IR bedömer att nuvarande styrdokument inte i tillräcklig grad når upp till de krav som finns på ledningssystem för informationssäkerhet i enlighet med MSBFS 2020:6. Nuvarande omfattning kan innebära risk för att det saknas styrning och stöd för att arbetet på helheten ska nå upp till att vara systematiskt och riskbaserat i enlighet med föreskrifter och av universitet beslutad informationssäkerhetspolicy. IR ser positivt på att det upprättats en handläggningsordning som tydliggör krav i enlighet med MSBFS 2020:7. IR noterar samtidigt att det saknas uppdaterade interna styrdokument för att ändamålsenligt stödja ansvariga att bedriva ett systematiskt informationssäkerhetsarbete.

¹³ Daterad 2014-11-28 med ansvar IT-avdelningen (Dnr SU FV-1.1.2-3513-14)

IR noterar att Säkerhetspolicyn inte har reviderats enligt ursprunglig plan. Policyn hänvisar delvis till föräldrad lagstiftning och föreskrifter inom informationssäkerhet som ersatts. En revidering pågick emellertid vid granskningstillfället.

3.2. Kunskap och mognad hos medarbetare inom informations- och IT-säkerhet

Enligt 9 § p.5 i MSBFS 2020:6 Säkerhetsåtgärder för att säkerställa att personal behandlar information på ett säkert sätt ska myndigheterna utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet genom utbildning, informationsinsatser och övning. Därtill ingår krav om att hålla egen och inhyrd personal informerad om relevanta interna regler, arbetssätt och stöd samt att utvärdera att interna regler, arbetssätt och stöd används på avsett sätt.

3.2.1 Rutiner och arbetssätt för att etablera kunskap och mognad

Ovan konstaterades en otydlighet i interna styrdokument rörande reglering av ansvar för åtgärder i syfte att etablera säkerhetskultur och kunskap hos medarbetare samt krav på hur detta ska uppnås. I intervju framhålls att det i uppgifterna för informationssäkerhetschef/CISO ingår att samordna, stödja och säkerställa att det finns tillfällen för anställda att få utbildning. På institutionsnivå är uppfattningen att ansvar för säkerhetskultur inte har tydliggjorts vilket lett till otydlighet över om det förväntas ingå i prefektens verksamhetsansvar. Denna otydlighet har bidragit till en passiv hållning rörande säkerhetskulturen.

3.2.2 Genomförande av utbildningsinsatser

Enligt uppgift har varken centrala funktioner eller institutionerna genomfört någon systematisk och dokumenterad analys över de anställdas behov av utbildning inom informationssäkerhet kopplat till roller eller arbetsuppgifter.

Samtidigt framkommer i intervjuerna att det finns stor variation i behov av informationssäkerhetsutbildning för olika funktioner och roller och därigenom olika behov hos medarbetare utifrån organisatorisk tillhörighet samt roll och funktion.

Introduktionsutbildning

Enligt personalavdelningen har det tagits fram ett introduktionspaket för nyanställda där informationssäkerhet ska vara en del. Planen är att detta ska genomföras första gången under hösten 2025. Delen om informationssäkerhet ska ha utformats av IT-avdelningen. IR har efterfrågat program och innehåll för introduktionspaketet men något sådant fanns ännu inte framtaget vid tidpunkten för intervjuerna. Innan rapportens färdigställande har vi kunnat ta del av programmet för introduktionsdagen för nyanställda och där ingå ett pass om IT-säkerhet.

Intervjuade institutioner har inte etablerat interna utbildningar som informationssäkerhet. Intervjuade institutioner har inte heller kunnat svara på hur medarbetare regelbundet får information eller anvisning om de interna regelverk som finns inom informationssäkerhetsområdet. Hänvisning görs till att information finns tillgängligt på *Medarbetarwebben*.

Digital grundutbildning (Nimblr)

Utbildningar om informationssäkerhet riktade till medarbetare sker främst genom en digital plattform (Nimblr) inom ramen för Stockholm University Security Awareness Training.

På medarbetarwebben finns information om denna utbildning, ”*Samtliga medarbetare bör genomföra denna utbildning för att minska risken för digitalt intrång, sabotage, skadlig kod och bedrägeri. Ansvaret för att genomföra utbildningen ligger på dig som medarbetare och det kommer följas upp av din närmsta chef*”.

Vi har tagit del av en sammanställning av de kurser som ingår i plattformen vilka är 52 till antalet. I sammanställningen framgår vilken typ av medvetenhet som kursen förväntas bidra med, exempelvis beteenden, bedrägeri eller skadlig kod. Upplägget är enligt uppgift inte att alla medarbetare ska gå alla kurser utan dessa anpassas automatiskt beroende av behov och hotbild.

Det saknas dock tydlighet i vem som ansvarar för tilldelningen av utbildningarna så att anställda får del av de utskick som sker. Det saknas även tydlighet över vem som ansvarar för uppföljningen. Enligt uppgift är detta en helt manuell process där nya medarbetares mejladresser behöver skickas till systemleverantören som därefter kan registrera att de är aktuella för utskick. Exempel finns dock där nyanställda ännu inte erhållit några utskick trots anställning i början av 2025. Det finns systemstöd för utdata ur systemet men det saknas attribut om organisatorisk placering vilket gör att uppföljning på avdelnings/institutionsnivå försvårats. Detta har i sin tur medfört en bristfällig uppföljning.

Övriga utbildnings- och informationsinsatser

Informationssäkerhetsfunktionen har under året genomfört en insats med informationsklassning av informationsmängder inom institutionerna. I samband med dessa tillfällen, som hade representation från delar av verksamheterna, erbjöds även inledande utbildning och information inom informationssäkerhet. Därtill har medarbetare som tilldelats access till MS365 erbjudits en kortare utbildning inom informationssäkerhet för de verktyg som ingår i plattformen. Det tillhandahålls riktade utbildningar för vissa tjänster som hanterar känslig information, till exempel för katalogansvariga där det bedöms finnas förhöjd risk för potentiellt missbruk. Det har även genomförts utbildning riktad till nya doktorander kring forskningsdata samt personalhandläggare, exempelvis inom dataskyddsfrågor.

3.2.3 Uppföljning av insatser

Uppföljning av utbildning genomförs av informationssäkerhetschef till universitetsdirektören månadsvis i samband med IT-styrgruppsmöten. Den uppföljning som presenteras är antal deltagare totalt samt hur många som genomfört första steget, grunden, i Nimblr (Introduktion).

IR har tagit del av sammanställning av genomförande för kurserna som ingår i Nimblr. Kurserna har genomförts av mellan 1446 och 4381 medarbetare med ett genomsnitt på 2615. Introduktionskursen har genomförts av 4381 medarbetare vilket enligt uppföljningen är 77 % av de som erhållit kursen via mejl. Genomförandet som helhet varierar dock: 26 av de 52 kursmomenten har genomförts av färre än 100 medarbetare.

Av de 20 kurserna som flest medarbetare genomfört är medelantalet 2615.

Varken centralt eller lokalt finns förteckning eller sammanställningar över vilka anställda som genomgått olika utbildningar fördelat på organisatorisk tillhörighet eller roll/funktion. Enligt uppgift går det ännu inte att sammanställa utdata ur Nimblr eftersom systemet inte är fullt integrerat med universitetets personalkatalog eller Active Directory (där alla användarkonton för medarbetare registreras).

I dagsläget genomförs ingen strukturerad utvärdering av Nimblr och huruvida utbildningarna uppnår sina syften. Den preliminära återkopplingen IT-avdelningen får från medarbetarna är att många är nöjda med utbildningarna. Enligt genomförda intervjuer med IT-avdelningen uppfyller Nimblr grundkraven på den kompetensnivå universitetsanställda bör hålla.

3.2.4 Säkerhetsåtgärder vid rekrytering

Enligt 9 § p.1 i MSBFS 2020:6 Säkerhetsåtgärder för att säkerställa att personal behandlar information på ett säkert sätt ska myndigheterna anpassa bakgrundskontroller av egen och inhyrd personal utifrån vilken information personalen ska få åtkomst till.

Enligt uppgift saknas strukturer vid universitet idag för anpassade bakgrundskontroller med koppling till vilken information som en anställd eller konsult kommer att få. På förfrågan kände ingen heller till om det finns fastställda förfaranden rörande sekretess eller konfidentialitetsavtal, reglering av aspekter rörande informationssäkerhet i anställningsavtal, eller om det är reglerat hur information ska hanteras vid avslut eller ändrad anställning. Från personalavdelningen påpekas dock att, om det finns lagstadgad skyldighet att genomföra säkerhetsåtgärder t.ex. vid säkerhetsskydd och strålskydd, så hanteras detta av säkerhetsenheten.

3.2.5 Bedömning

Baserat på genomförda intervjuer finnas det utrymme att anpassa delar av universitetets styrdokument och rutiner för att öka följsamheten till 9 § p.1 och p.5 i MSBFS 2020:6 och området bedöms vara *bristfälligt*.

Sammantaget bedömer internrevisionen att nuvarande rutiner för genomförande och uppföljning för att uppnå kunskap och mognad hos medarbetare inom informations- och IT-säkerhetsområdet är bristfälligt. Detta stöds av att institutionsnivå uppfattar att ansvar för säkerhetskultur är otydligt vilket bidrar till en osäkerhet om vilka uppgifter som förväntas ingå i prefektens verksamhetsansvar. Denna otydlighet uppfattas ha bidragit till en passiv hållning rörande säkerhetskulturen

Interna styrdokument är ej tydliga rörande ansvar för att utveckla och upprätthålla kompetens hos egen personal avseende informationssäkerhet genom utbildning, informationsinsatser och övning. Det är därtill ett utvecklingsområde att medarbetare vid anställning erhåller information och kunskap om myndighetens förhållningssätt och regler inom informationssäkerhetsområdet. Detta så att medarbetare får förutsättningar att efterleva regelverk och inte utgöra risk i informationshanteringen.

SU bedöms vara i behov av att utveckla och implementera strukturer som säkerställer att alla anställda erhåller regelbunden lämplig utbildning och träning utifrån respektive roll, funktion och ansvar. Det bör också övervägas att analysera om befintlig utbildningsplattform via Nimblr tillgodoser myndighetens behov och om eventuella kompletterande insatser kan vara nödvändiga. Det är en brist att lämpliga utdata är svåra att tillhandahållas ur Nimblr för ändamålsenlig uppföljning och utvärdering.

3.3 Incidenthantering

Enligt 11 § i MSBFS 2020:6 Åtgärder för att hantera incidenter och avvikelser, ska myndigheterna

1. skyndsamt upptäcka och bedöma incidenter och avvikelser,
2. återställa manipulerad eller förlorad information, och
3. bedöma om inträffad incident ska rapporteras externt.

Enligt 12 § ska myndigheten, om en incident eller avvikelse inträffat, identifiera grundorsaker till incidenten eller avvikelsen och vidta åtgärder för att motverka att liknande incidenter och avvikelser inträffar på nytt.

3.3.1 Incidenthanteringsrutiner

På intranätet finns information och vägledning för hur medarbetare ska gå till väga för att rapportera en incident. Internrevisionen har dock inte erhållit någon beslutad rutin eller process för hantering av incidenter. Enligt beskrivna strukturer på intranätet ska incidenter rapporteras via Serviceportalen. Rapportering sker i nuläget via portalen, samtal eller mejl. Samtliga inkomna ärenden registreras dock i Serviceportalen där funktioner vid IT-avdelningen bedömer inkomna ärenden. Inom IT-avdelningen finns interna rutiner baserade på ITIL¹⁴ som är kända och etablerade hos ansvariga funktioner. Vid IT-avdelningen finns det även en roll, incident

¹⁴ ITIL (Information Technology Infrastructure Library) är ett vedertaget ramverk för att hantera IT-tjänster. De vanligaste rutinerna är Change, Problem och Incident.

manager, med uppgift att säkerställa hantering, uppföljning och åtgärder utifrån rapporterade incidenter.

Hur välkänd incidenthanteringsprocessen är bland medarbetarna är delvis oklart. Baserat på utfall i granskningens manipulationstest (se avsnitt 3.5 nedan) så kan vi konstatera att det till viss del finns kännedom om incidentrapporteringsrutiner, men kan samtidigt konstatera att endast ett fåtal medarbetare rapporterade phishing-mejlet som incident.

Det saknas en samlad dokumentation och utvärdering av inträffade incidenter. Enskilda incidenter utvärderas som del i IT-avdelningens rutiner. Allvarligare incidenter eskaleras enligt fastställd eskaleringskedja som ingår i incidentrutinen enligt ITIL.

3.3.2 Bedömning

IR:s sammantagna bedömning är att det finns *förbättringsmöjligheter* rörande kännedom om rapporteringsrutiner vid misstänkta eller inträffade incidenter kopplade till medarbetares användning av digitala system.

IR bedömer vidare att processen för hantering av IT-incidenter bör formaliseras på behörig nivå och kommuniceras ut i organisationen. Det finns därtill behov av att införa rutiner för att dokumentera och följa upp inträffade incidenter på myndighetsövergripande nivå då incidenter är en viktig informationskälla för arbetet med ständiga förbättringar. Förslagsvis kan en sådan sammanställning inkluderas i momentet ledningens genomgång (minst årlig uppföljning och rapportering till högsta ledningen) vilket är ett krav i det systematiska informationssäkerhetsarbetet.

3.4 Socialt manipulationstest

Som en del i internrevisionens granskning genomfördes ett socialt manipulationstest, så kallad nätfiskekampanj. Syftet var att undersöka samt höja medvetenheten gällande informationssäkerhet bland universitetets anställda. Resultatet av testet redovisas översiktligt i rapporten.

Målgrupp för testet var medarbetare inom såväl universitetsförvaltning som de två vetenskapliga områdena. Sammantaget skickades testet till 5328 mottagare inom universitetet.

Nätfiskekampanjen påbörjades 2025-08-25 07:30 och avslutades 2025-08-28 15:01. I genomförandet av nätfiskekampanjen användes specifika verktyg och strategier för att simulera en realistisk attack. Nätfiskekampanjen innefattade utskick av mejlmeddelanden som var designade för att efterlikna legitima kommunikationer inom universitetet. Meddelandena innehöll uppmaningar att klicka på en länk, vilket var en central del i kampanjens syfte. Under kampanjens gång samlades data in för att mäta hur många som mottog, öppnade och klickade på länken i mejlen. Dessa mätvärden gav en indikation på hur effektivt nätfiskemeddelandet var i att fånga mottagarnas uppmärksamhet och få dem att klicka på länken.

Vissa begränsningar fanns i spårningen, detta då verktyget som användes för att genomföra kampanjen, inte möjliggjorde spårning av hur många som rapporterade mejlen som misstänkta. För att komplettera denna information kontaktades IT-avdelningen efter kampanjens genomförande. Vi har i granskningen erhållit data över antal som kontaktade IT-avdelningen. Denna information bidrog till en mer komplett bild av kampanjens genomslag och hur medarbetarna reagerade på de misstänkta meddelandena.

Område	Skickade mejl	Öppnat mejl	Klickat på Länkar	Rapporterat till IT
Alla områden (sammanställda)	5328	3128 (58%)	1916 (35%)	13 (0.42%)
Universitetsförvaltningen	705	444 (62%)	275 (39%)	
Naturvetenskapliga området	1814	1028 (56%)	600 (33%)	
Humanvetenskapliga området	2809	1656 (58%)	1041 (37%)	

Resultaten från nätfiskekampanjen visar att en stor andel av mottagarna som öppnade mejlet också klickade på länkarna. Detta indikerar att en verklig angripare sannolikt hade kunnat orsaka betydande skada för universitetet. Universitetets resultat ligger sämre än jämförbara organisationer, både generellt och inom utbildningssektorn. Som riktmärke anses 5–10 % klickfrekvens vara acceptabel, 10–20 % mindre bra och >20 % dåligt. I denna kampanj översteg klickfrekvensen markant 20 %, vilket tyder på bristande säkerhetsmedvetenhet och behov av förstärkt utbildning och tydligare kommunikation. Därtill var rapporteringen av misstänkta mejl mycket låg, vilket tyder på bristande medvetenhet och/eller otydliga eller ineffektiva rutiner för att identifiera och rapportera nätfiske.

Resultatet av testet identifierade flera områden som ökar risken för säkerhetsbrister. Externa mejl saknar tydlig märkning, vilket gjorde det svårt för användare att identifiera om avsändaren var någon utanför organisationen. Detta ökade risken för felaktiga klick på misstänkta länkar. Därtill saknades funktion i universitetets mejl-program där användare enkelt kan direktrapportera misstänkta mejl till mottagare på IT-supporten. Detta försvårar rapporteringsprocessen och riskerar att fördröja hanteringen av potentiella säkerhetshot. I testet identifierades även tekniska säkerhetsbrister i de operativsystem och webbläsare som medarbetare använder.

3.4.1 Bedömning

IR gör mot bakgrund av genomförd nätfiskekampanj bedömningen att universitetet har en låg mognad inom informationssäkerhet gällande området medarbetarnas kunskap och säkerhetskultur vilket bedöms vara *otillfredsställande*. Trots genomförda utbildningsinsatser i syfte att

ge medarbetarna kunskap och medvetenhet för att reagera på motsvarande hot via mejl så visar testet att en stor andel öppnade mejl och klickade på länkar. Detta indikerar en betydande risk för skada vid verkliga nätfiskeattacker. Den låga rapporteringsgraden av misstänkta mejl understryker behovet av förbättrad medvetenhet och effektivare rutiner för hantering av säkerhetsincidenter. IR noterar även brister gällande uppdatering av operativsystem och webbläsare då sårbarheter i dessa identifierades i testet, vilka skulle kunna nyttjas av en faktisk hotaktör.

Identifierade utvecklingsområden utifrån manipulationstestet:

- *Utvecklingsområde – tydlig märkning av externa avsändare:*
En viktig säkerhetsfunktion som saknades var en tydlig markering för mejl som kommer från externa avsändare. En sådan markering, ofta kallad "External sender tag" eller en varningsbanner, syftar till att visa att mejlet kommer utanför organisationen. I Microsoft 365/Outlook kallas det "External"-taggen, och vissa organisationer väljer att lägga till [EXTERNAL] i ämnesraden via en mejl flow-regel. Implementeringen av denna funktion skulle kunna hjälpa anställda att snabbt identifiera potentiellt misstänkta mejl från externa källor.
- *Utvecklingsområde – ingen enkel rapportering i Outlook:*
Det fanns inget smidigt sätt för anställda att rapportera misstänkta mejl direkt inuti Outlook. För att förbättra detta, rekommenderas att universitetet implementerar ett tillägg som gör det enkelt att rapportera sådana mejl, samt att tydligt kommunicera hur det kan användas.
- *Utvecklingsområde - Föråldrade operativsystem och webbläsare:*
Även om detta inte var huvudfokus för nätfiskekampanjen visade insamlade data att många av universitetets datorer, mobiler och surfplattor använder gamla operativsystem och webbläsare. Det innebär en stor säkerhetsrisk, eftersom äldre programvara inte längre får säkerhetsuppdateringar från tillverkaren. När sårbarheter blir kända kan angripare enkelt utnyttja dem om systemen inte är uppdaterade. IR rekommenderar därför att universitetet säkerställer regelbundna uppdateringar av både operativsystem och webbläsare för alla enheter. På så sätt minskar risken för att angripare lyckas ta sig in genom kända svagheter.
- *Utvecklingsområde – Utbildning och testning:*
Att SU själva överväger att göra sådana phisingtester regelbundet som träning/test, något som är relativt vanligt i många organisationer idag.

3.5 Sammanfattande bedömning och rekommendationer

IR:s sammantagna bedömning är att universitetets interna styrning och kontroll är *bristfällig* och behöver stärkas i syfte att säkerställa en god informations- och IT-säkerhetskultur i enlighet med krav i lag, föreskrifter och interna styrdokument. På en övergripande nivå bedöms det saknas tillräcklig styrning för att säkerställa efterlevnad till MSBFS 2020:6 och det bedöms även saknas en tillräcklig intern styrning och kontroll för att säkerställa följsamhet till regelverk. IR lämnar emellertid inga nya rekommendationer rörande det övergripande systematiska informationssäkerhetsarbetet. Tidigare granskningar har fångat utvecklingsbehov rörande systematiskt informationssäkerhetsarbete och IR är medveten om att utvecklingsarbete pågår i relation till tidigare lämnade rekommendationer inom området.

På en övergripande nivå bedöms Nimblr och dess utbildningsinnehåll vara ett bra verktyg för att höja medvetenheten och säkerhetskulturen men det behöver kompletteras med fler åtgärder och dess genomförande och uppföljning behöver stärkas. IR bedömer att befintliga rutiner för genomförande av säkerhetsåtgärder i syfte att uppnå kunskap och mognad hos medarbetare inom informations- och IT-säkerhetsområdet är bristfälliga. IR bedömer att det finns risk för att nuvarande insatser inte är tillräckliga för att uppnå en godtagbar kunskap och säkerhetskultur. Det mognadstest som genomförts inom ramen för granskningen påvisar att universitetet har en förhöjd risk för både ekonomisk skada och förtroendeskada om informationssäkerhetshot riktas mot medarbetare.

IR lämnar följande rekommendationer i syfte att stärka den interna styrning och kontrollen inom det granskade området:

1. Etablera ansvar och aktiviteter för att höja personalens kunskap och medvetenhet inom informations- och IT-säkerhet.
2. Utveckla incidentrapporteringen avseende process samt uppföljning och rapportering.
3. Beakta identifierade utvecklingsområden utifrån genomfört manipulationstest.



Bilaga 1 Sammanställning över granskad dokumentation

MSBFS 2020:6 Föreskrifter om informationssäkerhet för statliga myndigheter

Arbetsordning vid Stockholms universitet, styrelsen 2025-01-01 (dnr: SU FV-3298-24)

Besluts- och delegationsordning, 2024-12-19 (dnr: SU FV-4158-24)

Föreskrift för anställda och personal som arbetar på uppdrag av Stockholms universitet avseende användning av information och informationshanterande resurser 2014-12-03 (dnr: SU FV-1.1.2-3513-14)

Säkerhetspolicy vid SU, 2017-01-26 (dnr SU FV-2.11.2-1922-16)

Informationssäkerhetspolicy, 2023-06-01 (dnr: SU FV-2209-23)

Riktlinjer för informationssäkerhet vid Stockholms universitet, 2017-01-26 (dnr: SU FV-2.11.2-1923-16)

Digitaliseringsplan, 2024-02-08 (dnr: SU FV-0431-23)

Regler för organisation och genomförande av dataskydd vid Stockholms universitet, 2024-12-19 (dnr: SU FV-3115-24)

Handlägningsordning för ansvarsfördelning och vägledning avseende säkerhetsåtgärder i informationssystem vid Stockholms universitet, 2025-04-16 (dnr: SU FV-1582-25)

Handlägningsordning för intern styrning och kontroll, 2024-12-04 (dnr: SU FV-3412-24)

Handlägningsordning för de registrerades rättigheter enligt den allmänna dataskyddsförordningen, 2024-12-19 (dnr: SU FV-3116-24)

Ansvarsförbindelse systemadministratör

Intranät: Informationssäkerhet - allmän information.