Protokollsbilaga A3
Direktionens protokoll 2025-12-03, § 3

BESLUT

DATUM:	2025-12-03
AVDELNING:	Avdelningen för intern styrning och verksamhetsstöd/SÄK
HANDLÄGGARE:	Maria Emilsson
DIARIENUMMER:	2025- 01189
HANTERINGSKLASS:	ÖPPEN

Säkerhetspolicy

Riksbankens beslut

Riksbanken beslutar om Säkerhetspolicy i enlighet med bilaga. Genom policyn upphävs Säkerhetspolicy för Sveriges Riksbank (dnr 2024-01212).

Skälen för beslutet

En översyn har gjorts av befintlig säkerhetspolicy. Följande justeringar har genomförts:

- En organisationsförändring har skett på AIS/SÄK där rollen CISO nu är en separat befattning och därför flyttats från säkerhetschefens ansvar till en egen rollbeskrivning.
- I förra årets säkerhetspolicy togs några lagkrav bort som nu har lagts tillbaka.
- Mindre förtydliganden och justeringar.

Beslutet har fattats av direktionen (riksbankschefen Erik Thedéen, förste vice riksbankschefen Aino Bunge samt vice riksbankscheferna Per Jansson och Anna Seim) efter föredragning av compliance officer Anna Fjäll. I den slutliga handläggningen har tf. säkerhetschef Susanne Wintzell och informationssäkerhetsspecialist Maria Emilsson medverkat.

SÄKERHETSPOLICY

BESLUTSDATUM:	2025-12-03
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	Avdelningen för intern styrning och verksamhetsstöd
FÖRVALTNINGSANSVARIG:	Säkerhetschefen
DIARIENUMMER:	2025- 01189
HANTERINGSKLASS:	ÖPPEN

Säkerhetspolicy

Innehåll och syfte

Denna policy innehåller bestämmelser för Riksbankens säkerhetsarbete och utgör grunden för Riksbankens säkerhetsledningssystem (SLS).

Syftet är att tydliggöra Riksbankens inriktning och principer för säkerhetsarbetet samt att definiera ansvarsfördelningen inom banken.

Målgrupp

Policyn riktar sig till samtliga medarbetare inom Riksbanken. Med medarbetare avses såväl anställda som uppdragstagare.

Postadress: 103 37 Stockholm, **Besöksadress:** Brunkebergstorg 11
Telefon: 08-787 00 00, **Webb:** riksbank.se

Innehållsförteckning

Säkerhetspolicy		1
	Innehåll och syfte	1
	Målgrupp	1
1	Inledning	3
	1.1 Bakomliggande regelverk	3
	1.2 Definitioner	3
2	Roller och ansvar	4
3	Principer för säkerhetsarbetet	5
	3.1 Effektiv säkerhetsstyrning	5
	3.2 Högt säkerhetsmedvetande	6
	3.3 Ändamålsenlig säkerhetsorganisation	6
	3.4 Omvärldsbevakning	6
	3.5 God kontroll av säkerhetsrisker och hot	6
	3.6 Informationstillgångarna är kartlagda och skyddade	6
	3.7 Säkerhetsarkitektur i flera lager	7
	3.8 Stark it- och cybersäkerhetsförmåga	7
	3.9 Kontinuitetshantering	7
	3.10 Samverkan för förbättrad säkerhet	7
4	Efterlevnad	7
5	Ikraftträdande	8

1 Inledning

Säkerhetspolicyn är den policy där direktionen beskriver den övergripande inriktningen och principerna för säkerhetsarbetet inom Riksbanken.

Riksbanken bedriver verksamhet som har stor betydelse för samhället i allmänhet och det finansiella systemet i synnerhet. Att Riksbankens verksamhet bedrivs på ett säkert sätt är en förutsättning för förtroendet för myndigheten och för samhällets stabilitet. Riksbanken ska därför bedriva ett aktivt säkerhetsarbete.

Säkerhetsarbetet ska vara en integrerad del av den ordinarie verksamheten. Det ska möjliggöra för verksamheten att nå de övergripande målen och den strategiska förflyttningen, under såväl normala förhållanden som under fredstida krissituationer och höjd beredskap.

1.1 Bakomliggande regelverk

Följande författningar och ramverk styr Riksbankens säkerhetsarbete.

- Lagen (2022:1568) om Sveriges riksbank
- Lagen (2019:109) om säkerhetsskydd i riksdagen och dess myndigheter
- Säkerhetsskyddslagen (2018:585)
- Skyddslagen (2010:305)
- Sveriges riksbanks arbetsordning
- SS-EN ISO/IEC 27001:2022, Ledningssystem för informationssäkerhet
- SS-EN ISO/IEC 27002:2022, Riktlinjer för styrning av informationssäkerhetsåtgärder

1.2 Definitioner

Säkerhet innebär skydd av medarbetare, information, system, lokaler, tillgångar och verksamhet.

Säkerhetsledningssystem (SLS) är ett ramverk som styr Riksbankens säkerhetsarbete och inkluderar personalsäkerhet, informationssäkerhet (inkluderar it- och cybersäkerhet), säkerhetsskydd och fysisk säkerhet.

Säkerhetsskydd handlar om att skydda information och verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot.[1]

[1] Lagen (2019:109) om säkerhetsskydd i riksdagen och dess myndigheter, 2§.

Säkerhetskänslig verksamhet är verksamhet som har betydelse för Sveriges säkerhet eller omfattas av ett för Sverige internationellt åtagande om säkerhetsskydd.

Övriga termer och uttryck som används i denna policy har samma betydelse och tillämpningsområde som Myndigheten för samhällsskydd och beredskaps (MSB) termbank för informationssäkerhet.[2]

2 Roller och ansvar

Alla **medarbetare** har ansvar att följa regler och rutiner inom säkerhetsområdet. Medarbetarna ska vara uppmärksamma på och rapportera incidenter och säkerhetsbrister som kan påverka säkerheten eller som kan innebära ett hot mot Riksbanken.

Alla **chefer** har ansvar för säkerheten inom sitt ansvarsområde. Det innebär att de ansvarar för att regler och rutiner följs, samt att deras medarbetare får den information och utbildning som krävs för att uppnå en god säkerhet.

Följande roller har ett utökat ansvar:

Direktionen har det övergripande ansvaret för säkerheten på Riksbanken. Direktionen informeras löpande om säkerhetsläget och de tar vid behov beslut om säkerhetsfrågor som föredras av säkerhetschefen.

Säkerhetschefen ansvarar för styrning, samordning, stöd och uppföljning av Riksbankens säkerhetsarbete inklusive övergripande kravställning inom it- och cybersäkerhet. Säkerhetschefen ansvarar även för Riksbankens SLS och för att rapportera säkerhetsläget för direktionen och ledningsgruppen. Säkerhetschefen är även **säkerhetsskyddschef** och ansvarar för Riksbankens säkerhetsskydd. Detta ansvar kan inte delegeras.[3]

Informationssäkerhetschefen (CISO) ansvarar för att leda och utveckla informationssäkerhetsarbetet, säkerställa att informationssäkerhetskrav är implementerade och efterlevs. Informationssäkerhetschefen ska även samordna informationssäkerhetsrelaterade aktiviteter inom banken och stödja informationsägare i deras ansvar.

Avdelningscheferna ansvarar för att säkerställa att en ändamålsenlig säkerhet bedrivs i enlighet med SLS. Avdelningschefen är **informationsägare** för information inom sitt verksamhetsområde. Det innebär att de ansvarar för att klassificera, skydda och hantera informationen enligt gällande regler och rutiner, genom hela dess livscykel.

Chef för avdelningen för it och digitaliseringen (AID) ansvarar för att styra och leda arbetet med it- och cybersäkerhet utifrån övergripande kravställning i Riksbankens

[2] https://termbank-informationssakerhet.msb.se/

[3] Lagen (2019:109) om säkerhetsskydd i riksdagen och dess myndigheter, 4 a §.

SLS. Chefen för AID ansvarar för att it-system och infrastruktur uppfyller kraven, oavsett om de bedrivs i egen regi eller är utkontrakterade.

It-säkerhetschefen ansvarar för att leda och samordna det operativa it-säkerhetsarbetet utifrån Riksbankens SLS samt ta fram rutiner och rapportera utifrån uppsatta mål. It-säkerhetschefen ska även stödja och följa upp att it-säkerhetskraven är implementerade samt rapportera it-säkerhetsläget för it-ledning och CISO.

3 Principer för säkerhetsarbetet

Riksbankens säkerhetsarbete ska vara systematiskt och riskbaserat. Vi ska ha ett proaktivt förhållningssätt med fokus på ständiga förbättringar. Säkerhetsarbetet ska integreras med Riksbankens befintliga styrningsprocesser.

Riksbankens medarbetare, information, system, tillgångar, verksamhet och lokaler ska skyddas mot identifierade risker och hot, som kan orsaka skada. Det gäller oavsett om de är avsiktliga eller oavsiktliga, interna eller externa.

Riksbanken ska eftersträva ett balanserat skydd. Det innebär att de kostnader för skyddsåtgärder som vidtas ska stå i rimlig proportion dels till den aktuella hotbilden, dels till risk för verksamheten vid eventuell skada. Riksbanken ska uppnå en skyddsnivå i enlighet med svensk författning och som är jämförbar med den på andra centralbanker, myndigheter eller organisationer med liknande förutsättningar.

De tio säkerhetsprinciper som beskrivs nedan ska tillämpas inom Riksbanken.

3.1 Effektiv säkerhetsstyrning

Riksbanken ska ha en integrerad systematisk och riskbaserad säkerhetsstyrning genom ett aktuellt, dokumenterat och förankrat SLS baserat på ISO/IEC 27000-serien.

Styrning och arbetssätt ska utformas, och lämpliga säkerhetsåtgärder ska implementeras, för att möta risker och hot. Riksbanken ska följa upp, utvärdera och förbättra säkerhetsarbetet löpande.

Årscykeln för SLS ska samordnas med verksamhetens planerings- och budgetcykler för att ge underlag till kommande års verksamhetsplaner.

Säkerhetsskyddsarbetet styrs utifrån säkerhetsskyddsanalysen och tillhörande säkerhetsskyddplaner, vilka leds av säkerhetsskyddschefen, i enlighet med gällande lagstiftning och interna styrande dokument.

3.2 Högt säkerhetsmedvetande

Riksbankens medarbetare ska ha en hög grundkompetens och vara medvetna om säkerhet. Medarbetarna ska ha den information och den kunskap som krävs för att på ett effektivt sätt skydda Riksbankens information och verksamhet.

3.3 Ändamålsenlig säkerhetsorganisation

För att säkerhetsarbetet ska vara effektivt ska Riksbanken ha tydligt definierade roller och ansvar för säkerhetsfrågor, inom alla delar av organisationen. Arbetet präglas av tillit, samverkan och förtroende mellan verksamhetens avdelningar.

Varje avdelning ska förstå vilket säkerhetsansvar den har utifrån de säkerhetsrisker och hot som finns. Avdelningarna ska ha den kompetens och de resurser som krävs inom säkerhetsområdet för att kunna bidra till att Riksbankens strategiska mål uppnås. Riksbanken ska uppfattas som en attraktiv arbetsplats, som lockar de bästa inom säkerhetsområdet, där bra ledarskap, medarbetarskap och kompetensutveckling är centrala.

3.4 Omvärldsbevakning

För att arbeta proaktivt och kunna hantera potentiella hot och utmaningar ska Riksbanken bedriva en systematisk omvärldsbevakning av de hot och trender som kan påverka verksamheten. För att kunna göra rätt avvägningar ska Riksbankens säkerhetsorganisation ha en djupgående kunskap om den egna verksamhetens och den finansiella sektorns utmaningar, trender och mönster. Riksbanken ska bevaka hur ny teknik utvecklas för att dra lärdomar och bemöta framtida säkerhetshot.

3.5 God kontroll av säkerhetsrisker och hot

Säkerhetsarbetet ska vara riskbaserat för att skapa underlag till att leda och fatta väl avvägda beslut. Det innebär att risker och hot löpande identifieras och hanteras för att minimera sårbarheter i verksamheten. När säkerhetsrisker och hot identifierats ska de kommuniceras, analyseras och hanteras inom hela Riksbanken.

Säkerhetsskyddsarbetet ska vara konsekvensdrivet vilket innebär att analys av hot och deras potentiella konsekvenser styr säkerhetsskyddsarbetet.

3.6 Informationstillgångarna är kartlagda och skyddade

Riksbankens information ska skyddas så att korrekt information lämnas till rätt person vid rätt tillfälle. Informationstillgångar, informationssystem, processer och säkerhetskänslig verksamhet ska vara kartlagda.

Ett balanserat skydd för bankens information och informationssystem ska säkerställas, genom att information klassificeras och hanteras utifrån Riksbankens regler och

rutiner. Det ska finnas utsedda informationsägare som är ansvariga för att information är identifierad, informationsklassificerad, dokumenterad och skyddad utifrån dess värde.

3.7 Säkerhetsarkitektur i flera lager

Kompletterande skyddsåtgärder ska användas för att minska risken för att ett enskilt fel kan skada hela system eller verksamheten. Säkerhetsarkitekturen ska utformas med flera skyddslager med effektiva skyddsåtgärder för att kunna identifiera, skydda, upptäcka, agera och återställa verksamheten från hot och attacker. Både den tekniska och den fysiska miljön ska ha flera skyddslager. Riksbanken ska använda moderna säkerhetsverktyg som ligger i framkanten av den tekniska utvecklingen.

3.8 Stark it- och cybersäkerhetsförmåga

Riksbanken ska ha it- och cybersäkerhetsförmågor för att möta aktuella hot samt kunna identifiera, skydda, upptäcka, agera och återställa verksamheten från angrepp.

It- och cybersäkerhetsarbetet ska ske inom ramen för Riksbankens SLS. It-arkitekturen och de proaktiva och reaktiva förmågorna ska vara dimensionerade i proportion till den aktuella hotbilden som finns mot Riksbanken och den risk som direktionen beslutat att acceptera.

3.9 Kontinuitetshantering

Riksbanken ska implementera och regelbundet testa säkerhetsåtgärder och kontinuitetsplaner för att effektivt hantera befintliga hotbilder och oförutsedda händelser. Genom noggrann planering, övning och etablerade rutiner skapas förutsättningar att upprätthålla säkerhetsskyddet samt hantera allvarliga säkerhetsincidenter.

3.10 Samverkan för förbättrad säkerhet

Riksbanken ska upprätthålla och etablera både interna och externa samverkansforum inom säkerhetsområdet, både nationellt och internationellt. Syftet med dessa forum är att nätverka, utbyta erfarenheter och underrättelser samt att genomföra gemensamma övningar. Detta arbete syftar till att stärka både samhällets och Riksbankens robusthet.

4 Efterlevnad

Säkerhetschefen tillika säkerhetsskyddschefen följer upp säkerhetsarbetet på Riksbanken och rapporterar löpande eventuella avvikelser till direktionen. Minst en gång per år rapporterar säkerhetschefen till direktionen om arbetet med SLS, om dess

effektivitet och efterlevnad. Säkerhetschefen ska också rapportera vilka aktuella säkerhetsrisker som finns och vilka resurser som behövs.

5 Ikraftträdande

Denna policy träder i kraft den 1 januari 2026. Genom policyn upphävs Säkerhetspolicy för Sveriges Riksbank (dnr 2024-01212).