BESLUT

DATUM:	2024-12-10
AVDELNING:	AIS/SÄK
HANDLÄGGARE:	Maria Emilsson
DIARIENUMMER:	2024-01212
HANTERINGSKLASS:	ÖPPEN

Säkerhetspolicy för Sveriges Riksbank

Riksbankens beslut

Riksbanken beslutar om Säkerhetspolicy för Sveriges riksbank i enlighet med bilaga. Genom policyn upphävs informationssäkerhetspolicy (dnr 2022-01402), säkerhetspolicy (dnr 2022-00515) samt Riksbankens informations- och cybersäkerhetsstrategi (dnr 2023-01211-2).

Skälen för beslutet

För att minska antalet styrande dokument, hålla samman styrningen av säkerhetsarbetet och förenkla för medarbetare och chefer ersätts nuvarande *Informationssäkerhetspolicy*, *Säkerhetspolicy* samt *Riksbankens Informations- och Cybersäkerhetsstrategi* med en ny policy, det vill säga *Säkerhetspolicy för Sveriges riksbank*.

Syftet är att få en gemensam uppdaterad säkerhetspolicy som omfattar samtliga discipliner inom säkerhetsområdet.

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

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

SÄKERHETSPOLICY FÖR SVERIGES RIKSBANK

BESLUTSDATUM:	2024-12-10
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	Avdelningen för intern styrning och verksamhetsstöd
FÖRVALTNINGSANSVARIG:	Säkerhetschefen
DIARIENUMMER:	2024-01212
HANTERINGSKLASS:	ÖPPEN

Säkerhetspolicy för Sveriges riksbank

Innehåll och syfte

I denna policy finns de bestämmelser som är av strategisk betydelse för Riksbankens säkerhetsarbete. Policyn är en del av Riksbankens säkerhetsledningssystem (SLS).

Syftet med den här policyn är att beskriva Riksbankens övergripande inriktning, principer samt ange de roller som har ansvar för säkerhetsarbetet, och beskriva vilket ansvar som ingår i rollerna.

Målgrupp

Säkerhetspolicyn 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

1 Inledning

Säkerhetspolicyn är det dokument 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 banken 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)
- Sveriges riksbanks arbetsordning
- Ledningssystem för informationssäkerhet, SS-ISO/IEC 27001:2022
- Riktlinjer för styrning av informationssäkerhetsåtgärder, SS-ISO/IEC 27002:2022

1.2 Definitioner

Säkerhet innebär att Riksbanken ska skydda medarbetarna, informationen, systemen, lokalerna och utrustningen.

Säkerhetsledningssystem (SLS) omfattar 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.

Säkerhetskänslig verksamhet. En verksamhet är säkerhetskänslig om den är av betydelse för Sveriges säkerhet eller om den omfattas av ett internationellt åtagande om säkerhetsskydd som Sverige måste genomföra.

Övriga termer och uttryck som används i denna policy har samma betydelse och tillämpningsområde som Myndigheten för samhällsskydd och beredskaps (MSB) termbank för informationssäkerhet[1].

2 Roller och ansvar

Alla **medarbetare** har ansvar att följa och tillämpa regler och rutiner inom säkerhetsområdet. Medarbetarna ska även 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.

Direktionen har det övergripande ansvaret för säkerheten på Riksbanken och fastställer den här policyn. Direktionen informeras löpande om säkerhetsläget, och de tar vid behov beslut om säkerhetsfrågor, som föredragits av säkerhetschefen.

Säkerhetschefen är tillika **informationssäkerhetschef (CISO)** samt ansvarar för styrning, samordning 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.

Avdelningscheferna ansvarar för att säkerställa att en ändamålsenlig säkerhet tillgodoses i enlighet med SLS, och att medarbetare under deras ledning görs medvetna om sitt ansvar för säkerhet. Avdelningschefen är **informationsägare** för information inom sitt verksamhetsområde. Det innebär att de ansvarar för att klassificera informationen, och att de ansvarar för att informationen skyddas och hanteras 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 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.

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

3 Principer för säkerhetsarbetet

Riksbankens säkerhetsarbete ska vara systematiskt och riskbaserat. Vi ska ha ett proaktivt förhållningssätt och ständigt sträva efter förbättringar. Säkerhetsarbetet ska integreras med Riksbankens befintliga lednings- och styrningsprocesser. För Riksbanken tillämpliga författningar inom säkerhetsområdet ska följas, och säkerhetskraven i SLS ska efterlevas i alla Riksbankens verksamheter.

Riksbankens medarbetare, information, system, lokaler och utrustning 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 vara en trygg arbetsplats.

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 konsekvenser och risk för verksamheten vid eventuell skada. När Riksbanken bedömer konsekvenser ska skador på person, förtroende och anseende särskilt beaktas. Riksbankens skyddsnivå ska överensstämma 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. Ledningssystemet baseras på de internationella standarderna i ISO/IEC 27000-serien, i vilka styrande regler och rutiner samverkar för att ständiga förbättringar ska omhändertas i verksamheten.

SLS utgör en grundläggande säkerhetsnivå och ingår som en del av Riksbankens övergripande styrning. Det kännetecknas av väldefinierade säkerhetskrav och processintegrerade arbetssätt, som utgör ett stöd för Riksbankens medarbetare.

Riksbanken ska arbeta kontinuerligt med att identifiera och analysera potentiella risker och hot, utforma styrning och arbetssätt, implementera lämpliga säkerhetsåtgärder, följa upp, utvärdera och förbättra säkerhetsarbetet.

Årscykeln för SLS ska vara anpassad till verksamhetens planerings- och budgetprocesser. Det här för att SLS:et ska kunna utgöra ett beslutsunderlag till verksamheternas planer för kommande år.

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. Alla medarbetare ska känna sig trygga på arbetet, och det ska vara lätt att göra rätt.

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 de har utifrån de säkerhetsrisker och hot som finns. Avdelningarna ska ha den kompetens och de resurser som krävs inom säkerhetsområdet för att på ett säkert sätt kunna uppnå Riksbankens strategiska mål. 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 vara i framkant och kunna hantera potentiella hot och utmaningar ska Riksbanken bedriva en systematisk omvärldsbevakning av de hot och trender som kan påverka verksamheten. Omvärldsbevakningen sker både internt och externt. 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

Riksbanken ska vara medveten om bankens hotmiljö och bankens säkerhetskänsliga verksamhet, så att lämpliga avhjälpande åtgärder kan vidtas. 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.

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

Genom att använda flera olika kompletterande skyddsåtgärder minskar risken för att ett enskilt fel kan kompromettera hela systemet eller verksamheten. Säkerhetsarkitekturen ska utformas med flera skyddslager med effektiva skyddsåtgärder. Det här för att kunna identifiera, skydda, upptäcka, agera och återställa verksamheten från både dagens och morgondagens 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 ska beredskap säkerställas för att upprätthålla säkerhetsskyddet samt hantera allvarliga säkerhetsincidenter, krissituationer och höjd beredskap.

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 rapporterar löpande eventuella avvikelser till direktionen, och minst en gång per år hur effektivt SLS är och om det efterlevs. Säkerhetschefen ska också rapportera vilka aktuella säkerhetsrisker som finns och vilka resurser som behövs.

Interna och externa revisioner utförs för att säkerställa efterlevnaden av säkerhetspolicyn.

5 Ikraftträdande

Denna policy träder i kraft den 1 januari 2025. Genom policyn upphävs informationssäkerhetspolicy (dnr 2022-01402), säkerhetspolicy (dnr 2022-00515) samt Riksbankens informations- och cybersäkerhetsstrategi (dnr 2023-01211-2).