POLICY

BESLUTSDATUM:	2022-12-19
BESLUT AV:	Direktionen
ANSVARIG AVDELNING:	AVS/SÄK
FÖRVALTNINGSANSVARIG:	Informationssäkerhetsansvarig/CISO
DIARIENUMMER:	2022-01402
HANTERINGSKLASS:	ÖPPEN

Informationssäkerhetspolicy

Innehåll och syfte

Syftet med policyn är att fastställa direktionens mål och säkerställa enhetlighet i hanteringen av informationssäkerhetsrisker i all verksamhet Riksbanken driver och ansvarar för.

Direktionens mål med Informationssäkerhet i Riksbanken är att tillämpa framstående standarder inom området, framförallt standarder som ISO27000, NIST CSF eller ISF Standard of Good Practice, samt att eftersträva en mognad i arbetet som är jämförbar eller bättre än andra centralbanker av samma storlek.

Målgrupp

Informationssäkerhetspolicyn riktar sig till samtliga som handhar Riksbankens information oaktat om de är anställda, inhyrda eller utför tjänster som underleverantör.

Innehållsförteckning

1 Inledning

Informationssäkerhetspolicyn är det dokument där direktionen anger riktning och nivåer för hur informationssäkerhetsarbetet ska bedrivas inom Riksbanken.

1.1 Ledningssystem för Informationssäkerhet

Ett ledningssystem ska finnas på plats och uppfylla kraven för ett strukturerat och metodiskt arbete av informationssäkerhet på Riksbanken. Ledningssystemet ska integreras med riskhanteringsprocesser, i de delar det finns effektivitetsfördelar, och utvärdera verksamhetens styrning av informationssäkerhet och relaterade risker. Resultatet av utvärderingen ska vägas mot den aktuella hotbilden mot Riksbanken och rapporteras till direktionen av informationssäkerhetsansvarig/CISO, minst årligen men oftare om så krävs.

Årscykeln för ledningssystemet ska vara anpassad till organisationens planerings- och budgetprocesser för att utgöra beslutsunderlag till verksamheternas planer för kommande år.

1.2 Bakomliggande regelverk

Riksbankens beslut rörande policys regleras i 4 § ”Instruktion för Sveriges riksbank” där Informationssäkerhetspolicyn ingår.

1.3 Definitioner

Informationssäkerhet – Bevarande av konfidentialitet, riktighet och tillgänglighet hos information, oberoende av form; talad, tryckt, elektronisk etc.

IT-säkerhet – Åtgärder för att upprätthålla informationssäkerhet i IT-system.

Cybersäkerhet – Tekniska och administrativa åtgärder för skydd mot fientliga eller illvilliga, externa IT-hot.

Säkerhetsskydd – Skydd mot spioneri, sabotage och andra brott som kan innebära hot mot Sveriges säkerhet, innefattande informationssäkerhet, tillträdeskontroll samt säkerhetsprövning.

Konfidentialitet – Egenskapen att information inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

Riktighet – Egenskapen att information är korrekt och fullständig.

Tillgänglighet – Egenskapen att information är åtkomlig och användbar på begäran från en behörig individ, objekt eller process.

2 Roller och ansvar

Samtliga medarbetare har ansvar för att upprätthålla en god informationssäkerhet i det dagliga arbetet genom att följa regler och rutinbeskrivningar inom området samt rapportera incidenter och händelser som kan innebära ett hot mot Riksbanken.

Följande funktioner har ett särskilt ansvar och påverkan på informationssäkerhetsarbetet i Riksbanken:

Direktionen fastställer denna policy samt beslutar om inriktning och tilldelar resurser via budget och verksamhetsplan. Direktionen informeras löpande om informationssäkerhetsläget och tar vid behov beslut om informationssäkerhetsfrågor som överlämnats från informationssäkerhetsansvarig/CISO.

Informationssäkerhetsansvarig/CISO ansvarar för att leda, samordna arbetet, samt dokumentera mål, inriktning och krav för verksamhetens övergripande informations- och cybersäkerhet. Ansvaret innefattar även att stödja och följa upp att kraven är implementerade. Det ligger på informationssäkerhetsansvarig/CISOs ansvar att lämna förslag till policy och regler samt att rapportera informationssäkerhetsläget för direktionen och ledningsgrupper.

Avdelningschefer ansvarar för att säkerställa att en ändamålsenlig informationssäkerhet tillgodoses och att medarbetare samt konsulter under deras ledning görs medvetna om sitt ansvar för informationssäkerhet som är relevant för arbetsuppgifterna.

Säkerhetschefen, tillika säkerhetsskyddschef ansvarar för Riksbankens säkerhetsskydd vilket även innefattar informationssäkerhet för de delar av Riksbankens verksamhet som är av vikt för Sveriges säkerhet. Säkerhetschefen samråder i dessa frågor med informationssäkerhetsansvarig/CISO.

IT-chefen ansvarar för att informations- och IT-säkerhet inkluderas vid utformandet av den övergripande IT-strategin samt för att säkerställa att IT-system och infrastruktur motsvarar verksamhetens krav avseende IT-säkerhet, oavsett om den bedrivs i egen regi eller är utkontrakterad.

IT-säkerhetsansvarig ansvarar för att leda och samordna det operativa IT-säkerhetsarbetet samt dokumentera och rapportera utifrån uppsatta mål. IT-säkerhetsa**n**svarig ska även stödja och följa upp att IT-säkerhetskraven är implementerade samt rapportera IT-säkerhetsläget för IT-ledning och informationssäkerhetsansvarig/CISO.

Informationsägare ansvarar för att klassificera information inom sitt verksamhetsområde och säkerställa att den hanteras i enlighet med regler för klassificering och hantering av Riksbankens information.

Objektägare ansvarar för att leda och organisera arbetet över förvaltningen av IT-stöd och ansvarar för att regelbundet säkerställa att data som finns i systemet är klassificerad och att skyddsnivån motsvarar informationsklassificering och riskanalyser.

3 Regler för informationssäkerhet

För att säkerställa att styrningen av informationssäkerhet upprätthålls i Riksbankens verksamheter bör regler utformas och antas av berörda avdelningschefer i Riksbankens ledningsgrupp. Målsättningen med reglerna är att tydliggöra kraven och uppfylla direktionens mål med informationssäkerhet. Alla avdelningschefer ansvarar för att tillse att kraven i reglerna implementeras, dokumenteras och är mätbara.

Följande områden behöver hanteras i regler:

- Regel om krav på klassificering och hantering av Riksbankens information syftar till att tydliggöra informationens egenskaper och behov av skydd utifrån konfidentialitet, riktighet och tillgänglighet.

- Regel om allmänna krav på informationssäkerhet där målsättningen är att tydliggöra roller och ansvar vid styrning och uppföljning av åtkomst till Riksbankens resurser, för både anställda och leverantörer. Regeln ska även innefatta krav om rutiner för hanteringen av informationssäkerhetsincidenter samt att en årlig granskning av informationssäkerhetsarbetet ska genomföras.

- Regel om IT-specifika krav på informationssäkerhet där målsättningen är att tydliggöra roller och ansvar för implementation och uppföljning av skyddsnivåer för Riksbankens information och informationsbehandlingsresurser. Skyddsnivåerna utvärderas, utformas och fastställs i förhållande till verksamhetens krav och består av tekniska kontroller samt uppföljningsrutiner.

4 Efterlevnad

CISO ansvarar för Riksbankens följsamhet mot denna policy och rapporterar löpande till direktionen eventuella avvikelser. CISO rapporterar minst årligen på efterlevnad och status gällande mognaden av kontroller enligt LIS *(Ledningssystem för Informationssäkerhet)* till direktionen.

5 Ikraftträdande och övergångsbestämmelser

Denna policy träder i kraft den 2022-12-19. Den tidigare versionen av denna policy (dnr 2020-01006) upphävs i och med att denna policy träder i kraft.

5.1 Versionshistorik

Senast granskad	Version	Kommentar till ändringar
2020-10-07	Dnr 2020-01006	Fastställd
2022-10-24	Dnr 2022-01402	Anpassning till ny mall