Policy

BESLUTSDATUM: 2008-12-08
ANSVARIG AVDELNING: ADM
BESLUT AV: Direktionen

FÖRVALTNINGSANSVARIG: Anton Granlund
HANTERINGSKLASS: ÖPPEN

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR 2008-915-ADM

Riksbankens säkerhetspolicy

1. Inledning

Riksbanken bedriver verksamhet av stor betydelse för samhället i allmänhet och det finansiella systemet i synnerhet. Att Riksbankens verksamhet fungerar säkert är en förutsättning för förtroendet för banken och för samhällets stabilitet.

Riksbanken ska därför bedriva ett aktivt säkerhetsarbete. Det ska vara en del av den ordinarie verksamheten och stödja bankens huvuduppgifter under såväl normala förhållande som påfrestningar och kris.

2. Säkerhetsarbetets inriktning

Riksbankens tillgångar i form av medarbetare, information, informationssystem, värden och egendom ska skyddas mot identifierade risker och hot, avsiktliga eller oavsiktliga, interna eller externa, som kan orsaka skada. Skyddet ska också omfatta icke anställda i Riksbanken och tillgångar ägda av annan, då dessa finns i Riksbankens lokaler.

Riksbanken ska eftersträva ett balanserat skydd där kostnaden för skyddsåtgärderna står i rimlig proportion dels till den aktuella hotbilden och dels till konsekvenser för verksamheten vid skada.

Vid bedömning av konsekvenser ska skador på förtroende och anseende särskilt beaktas. Riksbanken ska också beakta vad som är vedertagen skyddsnivå hos andra centralbanker eller organisationer med liknande förutsättningar.

3. Ansvar

Avdelningschef ansvarar för att identifierade risker som är förknippade med avdelningens verksamhet hanteras genom att de begränsas, undviks, överförs eller accepteras. Säkerhetschefen ansvarar för inriktning, samordning och uppföljning av säkerhetsarbetet.

Administrativa avdelningen ansvarar för att fastställa regler för hur denna policy ska uppfyllas. Det är varje medarbetares ansvar att följa dessa regler, samt att vara uppmärksam på och rapportera händelser som kan påverka säkerheten.

Varje chef ansvarar för att medarbetarna får den information och utbildning som krävs för att uppnå en god säkerhet.

SENAST GRANSKAD AV: DATUM:

4. Skyddsområden

4.1 Personskydd

Målet med personskyddet är att Riksbankens medarbetare ska känna trygghet på sin arbetsplats och på tjänsteresor samt att besökare ska känna trygghet när de vistas i Riksbankens lokaler.

Säkerhetschefen ansvarar för det övergripande personskyddsarbetet och beslutar om vilka medarbetare som behöver förhöjt skydd samt hur säkerhetsåtgärder ska sättas in. Detta gäller även när Riksbanken bedriver verksamhet utanför sina egna lokaler. Vid akuta händelser eller förhöjd hotbild ska personskyddsnivån kunna höjas och anpassas efter rådande omständigheter. Vid riskbedömning ska skydd av person alltid prioriteras.

En hotbild för enskilda eller grupper av medarbetare ska regelbundet tas fram av en analysgrupp med bred representation från verksamheten. Denna ska ligga till grund för säkerhetschefens riskbedömningar.

4.2 Informationssäkerhet

Målet med informationssäkerheten är att säkerställa ett tillräckligt skydd för bankens information och informationssystem.

Skyddet av informationstillgångar och informationssystem som Riksbanken äger eller förvaltar ska vara utformat så att verksamhetens krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet uppfylls. Detta gäller också när Riksbankens information eller informationssystem hanteras av extern part.

Riksbankens information ska ha ett balanserat skydd som säkerställer krav på öppenhet och transparens likaväl som sekretess och konfidentialitet. Arbetet ska bedrivas i enlighet med vedertagna internationella standarder.

Varje informationssystem ska ha en ägare. Den som är systemägare ska godkänna systemet före driftsättning och vid större förändringar. Godkännandet ska baseras på att systemet uppfyller verksamhetens krav på funktionalitet och säkerhet.

Avdelningschefer och systemägare har ansvar för att beakta nya risker som kan uppstå till följd av teknisk utveckling. Detta ställer krav på en kontinuerlig riskhantering, det vill säga att hot och risker löpande identifieras och att information och informationssystem tilldelas ett lämpligt skydd.

Alla medarbetare som hanterar information har ansvar för att upprätthålla informationssäkerheten.

4.3 Egendomsskydd

Målet med egendomsskyddet är att minimera risken för skada på personer, värden, information, informationssystem och byggnader.

Skyddet ska bestå av robust fysisk säkerhet och av effektiva säkerhetsanläggningar som omedelbart kan detektera försök till obehörigt intrång, brand eller sabotage. Tillträde till Riksbankens lokaler ska vara strängt kontrollerat och besökare ska registreras.

Skyddet ska ha en sådan nivå att ett brottsligt angrepp, vare sig det kommer från egna medarbetare eller utomstående, inte ska lyckas . Skyddet ska därigenom ha en avhållande effekt. Bankens lokaler ska vara uppdelade i skyddszoner där varje nivå har specifika krav på fysisk säkerhet, säkerhetsanläggningar och brandskydd.

Möjlighet till snabba åtgärder från polis eller säkerhetspersonal vid allvarliga händelser ska vara väl tillgodosedd. Alla säkerhetsanläggningar ska vara i drift dygnet runt och det ska finnas beredskapssystem eller likvärdiga åtgärder tillgängliga vid underhållsarbeten och funktionsstörningar.

Skyddet ska fördröja olovligt intrång under minst så lång tid som det tar för medarbetarna att sätta sig i säkerhet och som det tar för polis eller säkerhetspersonal att anlända för att antingen förhindra intrång eller för att förhindra angripare att nå zoner med högre skyddsnivå. Vid misstanke om brott ska möjlighet att rekonstruera händelseförlopp vara väl tillgodosedd.

Utveckling av egendomsskyddet är resurskrävande och ska därför ha ett långsiktigt perspektiv.