Regel

BESLUTSDATUM:	2014-03-24
BESLUT AV:	Anders Vredin
BEFATTNING:	Avdelningschef
ANSVARIG AVDELNING:	Stabsavdelningen
FÖRVALTNINGSANSVARIG:	Lars Andersson
HANTERINGSKLASS:	Ö P P E N
Senast granskad:	2017-11-15

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 2014-305-STA

Användning av Riksbankens IT-resurser

Inledning

I denna regel anges vad som gäller vid användning av Riksbankens IT-resurser (datorer, mobiltelefoner, nätverk och all annan kringutrustning). Reglerna gäller för alla medarbetare i Riksbanken samt konsulter och leverantörer med uppdrag på Riksbanken.

Syftet med denna regel är att ge ett stöd för den som använder Riksbankens IT-resurser, i arbetet eller vid begränsat privat bruk, genom att informera om hur dessa får användas och hur användningen kan komma att kontrolleras.

Användning av IT-resurser

Riksbankens IT-resurser ägs av Riksbanken och är avsedda att användas som arbetsredskap vid tjänsteutövning.

Viss användning för privata ändamål är tillåten i begränsad omfattning om dessa regler för användning respekteras. Detta gäller dock inte för samtal, SMS eller annan datatrafik från mobiltelefon när användaren befinner sig utanför EU/EES, där särskilda restriktioner finns.

Användning för privata ändamål ska ske med gott omdöme, och får inte inkräkta på det ordinarie arbetet. Den får inte heller menligt påverka datorns eller nätverkets funktionalitet, prestanda eller tillgänglighet.

Användning av Internet och e-post

Vid användning av Riksbankens adress på Internet representerar användaren Riksbanken. Användaren ska därför agera etiskt korrekt och i enlighet med svensk lag och Riksbankens etiska regler.

- En webbplats får inte avsiktligen besökas om den
    - har innehåll som är rasistiskt eller främlingsfientligt,

- har innehåll som uttrycker missaktning mot etniska, religiösa eller andra grupper eller mot personer med viss sexuell läggning eller livsstil,
- uppmanar till eller hyllar politiskt eller annat våld eller har terroristanknytning,
- har pornografiskt innehåll,
- har innehåll som uppmuntrar till användning av illegala droger,
- ger möjlighet att spela mot betalning,
- erbjuder en möjlighet att bryta mot upphovsrättsliga regler, eller
- har ett innehåll som i övrigt inte är etiskt försvarbart eller som strider mot svensk lagstiftning.

Riksbanken har ett s.k. ”surffilter” installerat, vilket avser att stoppa olämpliga webbplatser. En utebliven blockering ska dock inte tas som intäkt för att besök på webbplatsen är acceptabelt.

- Integritetskänsliga eller värderande uppgifter om enskild person får inte spridas över Internet. Personuppgifter får inte användas i strid med personuppgiftslagen, eller, från den 25 maj 2018, dataskyddsförordningen[1]. Stötande formuleringar i e-post får inte förekomma.

- Riksbankens egna lösningar för fjärråtkomst, webbmail eller distans-PC ska användas vid resa eller hemifrån. Uppgifter som omfattas av sekretess eller på annat sätt innehåller känslig information får, i enlighet med ”Regler för hantering av Riksbankens information”, inte sändas oskyddade via Internet.

- Riksbankens IT-resurser får inte användas för politiska eller kommersiella syften.

- Det är inte tillåtet att installera eller använda programvara som inte är godkänd av chefen för IT-avdelningen.

- Det är inte tillåtet att ladda ned programvara från Internet om det inte ingår i de tilldelade arbetsuppgifterna.

Reglerna kan inte täcka alla händelser. När man står inför ett etiskt problem kan det därför vara till hjälp att ställa sig följande frågor:

- Skulle jag tycka det vore pinsamt eller bli illa berörd om "detta" blev känt av mina arbetskamrater?

- Skulle "detta" på något sätt kunna skada Riksbanken om det skulle tas upp i massmedia?

Om du är tveksam i din bedömning bör du ta upp frågan med din närmaste chef. Frågor kan också ställas till riskenheten eller till juristerna på stabsavdelningen.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Användning av privat eller främmande utrustning

Utrustning som ansluts till Riksbankens nätverk och datorer måste vara rätt konfigurerad och skyddad för att inte utsätta verksamheten för oönskade risker.

En oskyddad dator som ansluts till nätverket kan överföra virus och annan skadlig kod till servrar och andra arbetsdatorer. I värsta fall kan felaktigt konfigurerad utrustning slå ut hela nätverket eller öppna upp nya oskyddade förbindelser med omvärlden. Främmande utrustning, exempelvis USB-minnen eller skrivare, som ansluts till bankens datorer, kan innehålla skadlig kod eller på annat sätt störa funktioner i datorerna om den programvara som behövs för utrustningens funktion inte följer Riksbankens säkerhetsstandard.

Endast utrustning som är godkänd av chefen för IT-avdelningen får anslutas till Riksbankens nätverk.

Undantag från denna huvudregel gäller för;

Främmande datorer som ansluts till Riksbankens trådlösa gästnät och där användaren har erhållit koder för inloggning.

Främmande utrustning får anslutas till Riksbankens datorer eller övrig utrustning, oavsett anslutningstyp (Ethernet, WLAN, Bluetooth, USB etc.) om stöd finns i Riksbankens utrustning och installationen kan göras utan att användaren får eller har utökade behörigheter.

Detta innebär t.ex. att en konsult eller leverantör inte utan tillstånd får ansluta en egen dator till nätverket. Det innebär också att privata mobiltelefoner, läsplattor, skrivare och liknande endast får anslutas till Riksbankens datorer om de drivrutiner och liknande programvara som behövs redan finns installerade på datorn.

Besöksmottagare ansvarar för att besökare i Riksbankens lokaler vid behov informeras om och följer dessa regler.

Lagring av privat information

Privat information ska normalt inte lagras i Riksbankens IT-miljö. Viss privat information, t.ex. sådan som är resultatet av privat användning av Internet och e-post enligt ovan, får dock lagras under begränsad tid och i begränsad omfattning.

Mediafiler, t.ex. musik, video och bilder, får inte lagras i Riksbankens utrustning med undantag för sådant som är arbetsrelaterat. Detta gäller oavsett om mediafilerna är upphovsrättsligt skyddade eller inte.

Övervakning och kontroll

Det kan finnas skäl för Riksbanken att följa upp och kontrollera hur IT-utrustning, e-post och Internet används. E-post och andra aktiviteter på Internet kan därmed komma att granskas.

Löpande övervakning

Vid användning av Internet (besök på webbplatser och e-posttrafik) uppkommer s.k. loggfiler. Loggningen omfattar uppgifter om avsändare och mottagare av e-post, besökta webbplatser och IP-adress på användarens dator. Nätverkstrafiken övervakas av tekniska och säkerhetsmässiga skäl av behörig personal hos Riksbanken och hos Riksbankens driftleverantör.

Normalt granskas inte vilka webbplatser enskilda medarbetare besökt. Vid misstänkta IT-säkerhetsincidenter såsom t.ex. virus, trojaner och onormala händelser i nätverket måste dock de som ska övervaka nätverkstrafiken kunna utreda händelserna ytterligare. Vid utredningen kan det i vissa fall finnas ett behov av att gå vidare och t.ex. också ta reda på vilken dator som har en viss IP-adress. Anledningen är att man kan behöva veta om den misstänkta IT-säkerhetsincidenten beror på avsiktligt eller oavsiktligt användande av datorn. De som löpande övervakar nätverkstrafiken får därför i dessa fall spåra datorn och också kontakta användaren för att utreda IT-säkerhetsincidenten.

Det finns i dessa fall ingen ursprunglig misstanke om missbruk av bankens informationssystem från användarens sida. I vissa fall kan utredningen dock leda till en sådan skälig misstanke om missbruk där en regelrätt kontroll av användaren kan ske enligt vad som anges nedan.

De som övervakar nätverkstrafiken ska dokumentera varje misstänkt IT-säkerhetsincident där vidare analys och utredning görs.

Kontroll

För att följa upp att reglerna följs kan kontroll också utföras av enskild medarbetares användande när det finns skälig misstanke om missbruk av bankens informationssystem, t.ex. besök på webbplatser som enligt dessa riktlinjer inte får besökas. Denna kontroll innebär att loggfiler över medarbetarnas Internetanvändning, inklusive e-post, granskas.

Särskild kontroll av innehållet i en enskild fil, t.ex. en användares privata dokument eller e-post, får dock endast ske om det är nödvändigt vid hot mot informationssäkerheten, t.ex. vid virus- och hackerangrepp, eller om det finns skälig misstanke om brott.

Riksbanken kan dessutom komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt för att uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet.

Beslut om kontroll

Beslut om kontroll får endast fattas av berörd medarbetares avdelningschef i samråd med chefsjuristen. Rör kontrollen en avdelningschef fattas beslutet av riksbankschefen. I samband med att beslutet om kontroll fattas ska de personer utses vilka ska genomföra kontrollen. Kontrollen ska utföras av två personer som ska arbeta tillsammans. IT-avdelningen ska bistå genom att tilldela de behörigheter som behövs för att kontrollen ska kunna genomföras. Avrapportering ska ske till den chef som beslutat om kontrollen. De användare som har kontrollerats ska också informeras om att en kontroll har genomförts, varför detta har skett och vilket resultat kontrollen gav, om inte syftet med kontrollen motverkas på ett allvarligt sätt av att sådan information lämnas.

Om det av kontrollerna framgår att reglerna överträtts kan ärendet komma att utredas av personalchefen i samråd med chefsjuristen. Vid allvarligt eller återkommande missbruk kan disciplinära åtgärder komma att vidtas.

Bevarande och gallring

Uppgifterna som ligger till grund för kontrollen av medarbetarnas Internet- och e-postanvändning gallras, senast efter sex månader. Om en utredning påbörjas kommer uppgifterna att bevaras så länge utredningen pågår.