Styrdokument

Informationssäkerhetspolicy för Katrineholms kommun

Övergripande anvisningsdokument

Senast reviderad av kommunfullmäktige 2013-12-16, § 203

Giltighetstid 2020-01-01 - 2020-06-30

Beslutshistorik

Gäller från 2013-09-16—2015-12-31

2010-08-18 Revision enligt beslut av KS 2010-05-26 version 1.1
2013-05-14 Revision hopslagning IT policy och informationssäkerhetspolicy

Antagen av kommunfullmäktige 2013-09-16.

Ändrad av kommunfullmäktige
2013-12-16, § 203

Förlängd giltighetstid beslutat av kommunstyrelsen 2019-12-18 § 212

Ägare[1]

Kommunstyrelsen

Förvaltarskap[2]

IT-chefen

Uppföljning

Hur: -

När: Revideras juni 2015

[1] Ägarskapet innebär ansvar för att styrdokumentet beaktas i beslutsprocessen samt för att efterfråga och ta del av uppföljning. Vidare att vid behov besluta om förändringar.

[2] Förvaltarskapet innebär ansvar för att
- dokumentet efterlevs
- är tillgängligt
- följa eventuellt ändrade förutsättningar för dokumentet
- dokumentet följs upp och revideras
- dokumentet är aktuellt och uppdaterat

Katrineholms kommuns informationssäkerhetspolicy

Innehåll

Definitioner

Informationssäkerhet

- rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt
- det är möjligt att spåra vem som tagit del av högt säkerhetsklassad information
- informationen är och förblir riktig

System

- mjukvara för inmatning, bearbetning och lagring av data.
- kan användas av en eller flera användare och vara installerat lokalt eller på en server.

Med **informationssystem** avses alla processer och system som innehåller information.

Med **information** avses det innehåll eller de meddelanden som överförs vid kommunikation, oberoende av i vilken form eller miljö den förekommer. Information finns exempelvis tryckt på papper, lagrad elektroniskt, överförs med post, e-post eller via integrationer samt visas på film eller nämns i ett samtal.

Med **kommunikation** avses överföring av information mellan människor eller apparater.

6900 är benämningen på IT-kontorets servicedesk. Följande kontaktinformation gäller:

- kontakt via e-post är 6900@katrineholm.se
- kontakt via telefon är 0150-(5) 6900

Med **intrång** menas att man tillgodogör sig information som:

- ej är relevant för just nu rådande arbetssituation
- saknas samtycke till

SPAM

- Reklam med e-post som skickas till många personer samtidigt men som mottagarna inte har beställt.

Med **incident** avses en tillfällig händelse, ett tillbud eller ett missöde.

BITS Plus

- system framtaget av Myndigheten för samhällsskydd och beredskap, som kartlägger informationssäkerhetsnivån för verksamhetssystem (MSB).

DISA

- datorstödd informationssäkerhetsutbildning för användare via webben (http://disa.msb.se/)

Omfattning

Vad omfattas

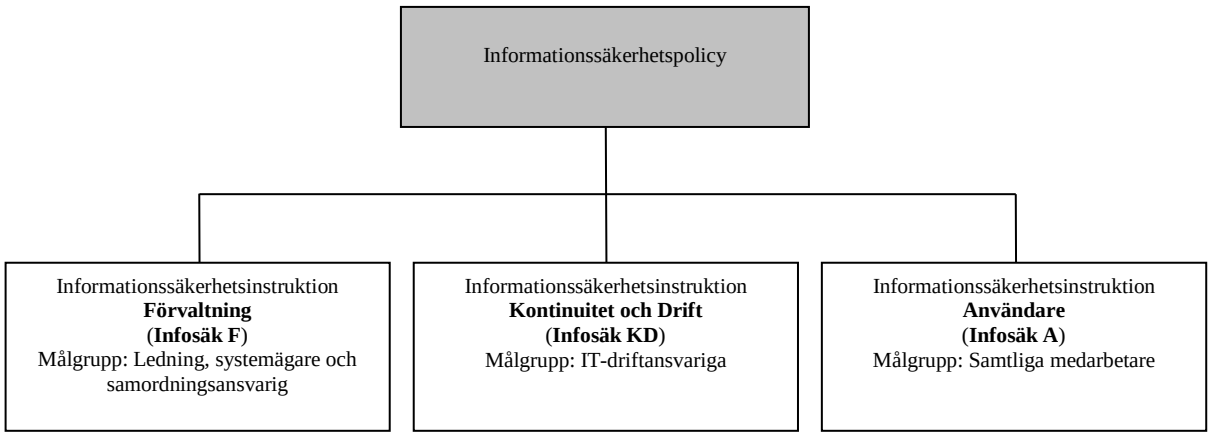
Informationssäkerheten omfattar kommunens alla informationstillgångar som finns i kommunens besittning. Exempel på informationstillgångar kan vara:

- information som finns i datorer eller på servrar
- information som skickas med e-post, chatt eller liknande
- information som finns på mobila enheter ex telefoner och surfplattor
- information som finns lagrad på externt media ex USB-minne m.m.
- information som visas på webbsidor eller via sociala medier
- information som överförs muntligt via ett samtal med telefon, direkt eller annat media
- information som finns i skriftlig form

Vem omfattas

Samtliga anställda, förtroendevalda, elever inom skola/förskola/vuxenutbildning och uppdragstagare som arbetar med kommunens information omfattas av informationssäkerhetspolicyn.

Policyns roll i informationssäkerhetsarbetet



Informationssäkerhetspolicyn redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet. Policyn konkretiseras i informationssäkerhetsinstruktioner. Policyn är framtagen enligt rekommendation från Myndigheten för samhällsskydd och beredskap (MSB).

Informationssäkerhet är den del av kommunens lednings- och kvalitetsprocess som handlar om hur verksamheten hanterar information. Informationssäkerhetspolicyn och särskilda informationssäkerhetsinstruktioner styr kommunens arbete kring informationssäkerhet.

Allmänt om informationssäkerhet och IT

Information är en av Katrineholms kommuns viktigaste tillgångar. Utgångspunkter i kommunens säkerhets- och policyarbete inom informationsteknologi är:

- lagar, förordningar och föreskrifter
- krav uppsatta av Katrineholms kommun
- avtal
- överenskommelse
- öka effektiviteten genom rätt IT-stöd i förvaltningarna
- ge bättre förutsättningar för ledning, styrning, uppföljning, utvärdering och resursfördelning

Hanteringen av informationen är en viktig del i risk- och sårbarhetsanalyser.

Överordnade chefer har rätt att, efter kontakt med personalkontor och en skriftlig begäran till IT-kontoret, få tillgång till information, inklusive e-post och hemkataloger på en medarbetare vid misstanke om oegentligheter.

I det fall det rör en förtroendevald politiker har kommunstyrelsens ordförande efter kontakt med personalkontoret samt kommunjuristen rätt att, efter en

skriftlig begäran till IT-kontoret, få tillgång till den förtroendevaldes e-post och hemkatalog vid misstanke om oegentligheter.

Skulle det röra kommunstyrelsens ordförande eller kommunfullmäktiges ordförande, som inte har någon chef över sig, har de möjlighet att via personalkontoret göra en anmälan för varandra.

Informationssäkerhet är en integrerad del av vår verksamhet. Samtliga chefer ansvarar för att all sin personal är väl insatta i informationssäkerhetspolicyn och efterlever denna. Alla som hanterar informationstillgångar ansvarar för att upprätthålla informationssäkerheten.

Samtliga som omfattas av denna policy ska vara uppmärksamma på, och rapportera händelser som kan påverka säkerheten för kommunens informationstillgångar. Rapportering ska ske till systemägaren som i sin tur rapporterar till informationssäkerhetssamordnaren inom organisationen. Lokala avvikelser från denna policy inom organisationen är tillåtet, dock reglerar denna policy en miniminivå på informationssäkerheten. Disciplinära åtgärder i enighet med arbetsrätten eller motsvarande kan vidtas mot den som använder informationstillgångarna på ett sätt som strider mot informationssäkerhetspolicyn.

Mål

Att ha ett säkert informationsflöde med rätt skydd för informationen så att den är:

- säkrad mot förlust
- säkrad mot skada
- säkrad mot sabotage
- säkrad mot stöld
- säkerhetsställd gällande riktighet

säkrad mot otillbörlig åtkomst

Dessa mål hanteras och bör följas upp i respektive verksamheters verksamhetsplan.

Ansvar

Kommunstyrelsen har det övergripande ansvaret för informationssäkerheten. Informationssäkerhetssamordnaren har det operativa ansvaret för samordning av informationssäkerhetsarbetet.

Varje facknämnd utser systemägare för informationssystem inom nämndens ansvarsområde.

Systemägare bör vara den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer. Systemägare utser även systemförvaltare för respektive informationssystem.
Beskrivning av roller och ansvar framgår av Infosäk F.

Generella krav

Kommunens informationssystem

Samtliga informationssystem ska vara identifierade och förtecknade på central plats (http://system.katrineholm.se).
Informationssystem som är av vikt, viktigheten beslutas av systemägare, ska genomgå en riskanalys. Riskanalysen genomförs med stöd av kommunens verktyg för analys av informationssäkerhet (BITS Plus). Underlaget från riskanalysen ska ligga till grund för driftnivå av informationssystemen.

Informationssäkerhetsutbildning

All personal ska regelbundet genomgå utbildning i informationssäkerhet för att informationssäkerheten ska upprätthållas.

Informationsklassning

Information som hanteras på myndigheten ska klassificeras med avseende på sekretess, riktighet och tillgänglighet enligt kommunens klassningsmodell i Infosäk A.

Internet

Förutsättningar och restriktioner för användandet av Internet dokumenteras i Säkerhetsinstruktion för användare.

E-post

Förutsättningar och restriktioner för användandet av e-post dokumenteras i Säkerhetsinstruktion för användare.

Kontinuitetsplanering

Kontinuitetsplaneringen krävs för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. En kontinuitetsplan ska även finnas för driften av IT-verksamheten baserad på de olika informationssystemens samlade krav och vara integrerade med Katrineholms kommuns gemensamma kontinuitetsplan.

Revidering

Revideringstid av informationssäkerhetspolicy och underdokument

- informationssäkerhetspolicyn ska ses över vid revidering av kommunplanen eller vid behov.
- informationssäkerhetsinstruktionerna revideras vid behov eller vid förändringar i informationssäkerhetspolicyn som påverkar informationssäkerhetsinstruktionerna.

Revideringsansvar

IT-chef är revisionsansvarig för informationssäkerhetspolicyn med underliggande dokument.

Beslutsinstans och referensgrupper

Informationssäkerhetspolicyn beslutas av Kommunstyrelsen, Informationssäkerhetsinstruktioner beslutas av IT-chef på delegation från kommunstyrelsen, IT-rådet är referensgrupp i revisionsarbetet.

Revidering och uppföljning

Uppföljning är en viktig del i informationssäkerhetsarbetet för att säkerhetsställa att:

- beslutade åtgärder är genomförda
- årliga mål är uppfyllda
- policy följs
- att policy, säkerhetsinstruktioner och riskanalyser vid behov revideras

Referenser

Katrineholms kommuns författningssamling

http://www.katrineholm.se/Om-kommunen/Styrdokument-och-planer/Forfattningssamling1

KOMMUNLEDNINGSFÖRVALTNINGEN

Datum
2013-09-16

Säkerhetsinstruktion för förvaltning

Revisionshistoria:
2010-05-04 SITHS-projektet Version 1
2013-07-01 Reviderad 2.0

Innehållsförteckning

Inledning

Med *informationssäkerhet* avses den samlade effekten av de skyddsåtgärder som tillsammans minskar eller eliminerar effekterna av hot och risker som riktar sig mot IT-stödets och informationsresursernas tillgänglighet, riktighet, sekretess och spårbarhet.

Med *information* avses här all information oberoende av i vilken form eller miljö den förekommer - den kan vara muntlig, skriven, tryckt eller elektronisk. Då datorer och IT-system idag har en så central roll som bärare av information blir denna instruktion dominerad av frågor rörande detta.

Styrande dokument för arbetet med informationssäkerhet i Katrineholms kommun är informationssäkerhetspolicy med tillhörande instruktioner.

Denna Informationssäkerhetsinstruktion för förvaltning (**Infosäk F**) redovisar:

- de olika rollernas ansvar
- riktlinjer för områden av särskild betydelse
- regler för systemutveckling, systemunderhåll och hantering av incidenter

Organisation och ansvar

Ledningen

Kommunstyrelsen beslutar om hur informationssäkerhetsarbetet ska bedrivas. Ansvarets omfattning framgår av BITS. BITS är ett verktyg för informationssäkerhetsanalys enligt BITS-konceptet från Myndigheten för samhällsskydd och beredskap (MSB).

IT-råd

IT-rådets syfte är att som samverkande organ, med deltagare från samtliga förvaltningar, verka för en IT-verksamhet som är kommungemensam, verksamhetsstyrd och kostnadseffektiv.

IT-rådets mål är att IT-ärenden ska behandlas utifrån kommunens befintliga styrdokument och att revidera IT-strategin, så att den stödjer IT-visionen.

Informationssäkerhetssamordnaren

Informationssäkerhetssamordnaren stödjer arbetet med att uppnå målen för informationssäkerhetspolicyn samt ansvarar för att de delar av IT-stödet som är gemensamma för hela verksamheten analyseras. Analyserna ska genomföras med stöd av BITS Plus. Informationssäkerhetssamordnaren stödjer och följer upp systemägarnas arbete med att genomföra säkerhetsanalyser av verksamhetssystem.

Systemägare

I enlighet med kommunfullmäktiges beslut att varje facknämnd utser systemägare för informationssystem inom nämndens ansvarsområde.

Systemägaren har det yttersta ansvaret för systemet och ansvarar bl.a. för:

- se till att genomföra analyser av systemets säkerhet med stöd av verktyget BITS Plus
- utse systemförvaltare, samt för att ge systemförvaltaren stöd i dennes roll som utförare av vissa moment inom systemdriften
- att lagar och förordningar följs ex personuppgiftslagen (PUL)
- informationen i systemet är i enighet med informationssäkerhetspolicyn
- att det finns en SNÖ (ServiceNivåÖverenskommelse) med IT-kontoret för reglering av driftansvaret
- att information och utbildning ges till berörd personal
- att systemet utvecklas i linje med kommunens IT-vision, IT-strategi och informationssäkerhetspolicy
- att hålla kontakt och utbyta information med IT-kontoret och IT-råd
- att godkänna nya versioner av systemet
- att licenser finns i erforderlig mängd och att en överlämning sker av licenserna och programvara till IT-kontoret vid installation
- att fastställa felhanteringsrutinen för varje system

Systemförvaltare

Systemförvaltaren utses av Systemägaren och ansvarar, i samverkan med IT-kontoret, för den dagliga driften och förvaltning av aktuellt system.

Systemförvaltarens roll är bl.a. att:

- verkställa beslut som systemägaren fattar
- informera sig om och bli väl förtrogen med programmets innehåll, struktur och termer
- upprätta, införa och utvärdera systemförvaltarrutiner
- se till att uppgifterna i systemet är aktuella och korrekta
- se till att användarna/grupperna har rätt behörighet i systemet
- tillhandahålla aktuell användarhandledning
- ansvara för användarsupporten rörande verksamhetsrelaterade frågor i systemet
- rapportera och förbereda ärenden och beslut som skall hanteras av systemägaren
- rapportera fel, brister, regelbrott och oegentligheter till systemägaren och informationssäkerhetssamordnaren
- hantera felanmälningar från kommunens gemensamma Servicedesk och åtgärda eller vidarebefordrar problemet till leverantören
- ge förslag till ändringar/utveckling av systemet
- ansvara för arbetet med säkerhetsfrågor som rör systemet

- ansvara för planering av datum för produktionssättning inför nya releaser/ versioner i samråd med IT-kontoret
- ansvara för att samtliga användare i systemet är informerade om planerade driftavbrott
- ansvara för tester vid uppdateringar och felrättningar
- ansvara för att kontroll och uppföljning av SNÖ följs
- se till att reservrutiner, serviceavtal mm, finns så att systemägarens krav på lägsta tillåtna avbrottstid kan tillgodoses
- se till att det finns lättillgänglig användardokumentation och handböcker till systemen, samt att dessa hålls aktuella och väl spridda hos användarna
- tillse att organisationens systemförteckning[1] är uppdaterad med relevant information

IT-chef

IT-chefen ansvarar för avveckling, uppgradering, utökning och implementering av IT-system samt utrustning i syfte att nå kostnadseffektiva lösningar för Katrineholms kommun inom ramen för antagna mål och ekonomiska ramar och i enlighet med Katrineholms kommuns delegationsordning.

IT-chef är systemägare för kommungemensamma system. IT-chef har ansvaret för att dessa fungerar. IT-chef ansvarar för att en analys av dessa genomförs med stöd av BITS Plus.

IT-chef ansvarar för att Informationssäkerhetsinstruktionerna Infosäk A, Infosäk F samt Infosäk KD upprättas och underhålls. Infosäk KD ska vara samordnad med myndighetens gemensamma kontinuitetsplan.

Systemadministratör

Systemadministratören tillhör IT-kontoret och har den tekniska kompetensen. Systemadministratören ansvarar tillsammans med systemägaren och systemförvaltaren för att den dagliga driften upprätthålls enligt SNÖ.

Regler och rutiner

Ansvar för IT-utrustning

All IT-utrustning ska vara förtecknad och stöldmärkt. Undantag från stöldmärkning kan beslutas av IT-chef. Av en förteckning ska framgå utrustningens placering, användare och datornamn. Omflyttning och överlåtelse av utrustning får inte ske utan samråd med IT-kontoret.

Anskaffning av IT-utrustning, görs i samråd med IT, se tjänstekatalog.

[1] http://system.katrineholm.se

Flyttning av IT-kommunikation

Förvaltningarna har skyldighet att i god tid kontakta IT-kontoret när det avser flytt. Verksamheter som flyttar utan att planera och meddela IT-kontoret före budgetplaneringen betalar kostnaden för flytt och kommunikation själva fram till nästa budgetperiod.

Utbildningsansvar

Systemägaren ansvarar för att:

- användare ges grundläggande informationssäkerhetsutbildning före tilldelning av behörighet i nätverket
- användarhandledning för aktuellt system finns
- medarbetare har tillräckliga kunskaper om säkerhetsreglerna för de informationssystem de behöver för de egna arbetsuppgifterna

Information och utbildning av anställda ska omfatta:

- informationssäkerhetens betydelse för verksamheten
- innehållet i Informationssäkerhetspolicyn
- Informationssäkerhetsinstruktion för Användare (Infosäk A)
- Kortversion av användarinstruktion och ansvarsförbindelse ska skrivas på av den anställda och skickas in till IT-kontoret

Säkrade utrymmen

Känslig information från informationssystem ska lagras på resurser i datorhallar som ska vara försedda med kontrollsystem för in- och utpassering.
Utrymmen med konsolutrustning ska vara låsta när de är obemannade.
Utrymmen med kopplingspunkter ska vara låsta och enbart behörig personal ska ha tillträde.
Känslig information som inte hanteras i informationssystem ska förvaras i brandklassade säkerhetsskåp.
Servicepersonal, städpersonal m.fl. ska övervakas i dessa utrymmen.

IT-chef/Informationssäkerhetssamordnaren beslutar om och när tillträde till säkrade utrymmen tillåts.

Utbyte av information

Om media som innehåller information som klassats som ”mycket hög nivå” måste transporteras fysiskt ska IT-chef/Informationssäkerhetssamordnaren kontaktas för beslut om tillvägagångssätt.

Övervakning

För informationssystemsloggar ska systemägaren besluta:

- Vad som ska loggas
- Hur ofta loggarna ska analyseras
- Vem som ansvarar för analyser av dem
- Hur länge de ska sparas
- Hur de ska förvaras

Styrning av användares åtkomst

För att säkerställa att endast behöriga användare har tillgång till nätverket ska åtkomst till nätverket beställas enligt anvisningar som finns på Intranätet under IT.

Innan användaren får konto i nätverket måste en ansvarsförbindelse för kommunens IT-resursers skrivas under och lämnas till IT-kontoret.

Samma tillvägagångssätt gäller även när konsulter eller andra utför arbete i informationssystem. Leverantörslösenord och behörigheter ska förvaras inlåsta.

Styrning av åtkomst till information

Användare ska bara ges tillgång till den information som krävs för arbetet.

Särskild hänsyn ska tas till PUL.

Styrning av åtkomst till nätverk

IT-chefen beslutar om

- autentisering vid externa anslutningar
- anslutning av utrustning till nätverket
- anslutning av externa nätverk till kommunens eget nät med ingående säkerhetsfunktioner, autentisering etc.
- anslutning av trådlösa nät
- säkerhet vid Internetanslutning

IT-chefen ansvarar för

- att en översikt av säkerhetsarkitekturer för interna nätverket och kommunikationsanslutningar upprättas
- administrationen av brandväggen samt besluta om vad som ska loggas i den, vem som ansvarar för uppföljningen av loggarna, hur ofta uppföljning ska ske och hur länge loggarna ska sparas
- att upprätta underlag för fullmäktiges beslut om kommunikationstjänster

Styrning av åtkomst till operativsystem

IT-chefen beslutar i vilken utsträckning användning av administrationsverktyg eller systemhjälpmedel som kan förbigå system- och tillämpningsspärrar ska användas.

Kontroll och revision av programlicenser

IT-kontoret ansvarar för de kommungemensamma licenserna såsom Office och Adobe. Därutöver har varje förvaltning ansvar för att antalet programinstallationer överensstämmer med antalet inköpta licenser på sin förvaltning. Varje förvaltning ansvarar för att köpa in sina egna programlicenser till respektive förvaltnings system. Villkoren för slutanvändning av licenserna ska uppfyllas. Vid en programvarurevision ska förvaltningen kunna visa upp aktuell dokumentation på antalet licenser och installationer. IT-kontoret kan vid behov göra sticksprovkontroll.

Kommunen måste kunna visa upp giltiga licenser för installerade program på samtliga kommunala datorer närhelst det begärs. Detta innebär att IT-kontoret kan komma att göra inventeringar.

Externa utövare

Beställare av utomstående leverantörers tjänster ska följa upp och granska att säkerhetsöverenskommelser följs. Om extern personal, t.ex. konsulter, ska ges tillgång till kommunens olika system, så ska det ske via utrustning som kommunen tillhandahåller. Undantag kan medges av IT-chef vid särskilda behov, t.ex. vid outsourcing av drift eller underhåll.

Anskaffning av informationssystem och övrig utrustning

Inför nyanskaffning och införande av ett informationssystem ska IT rådet informeras, därefter ska förvaltningschef, eller av denne utsedd person, i samarbete med Informationssäkerhetsansvarig och IT-kontorets förvaltningskontakt utforma en projektplan över införandet.

Denna **projektplan** ska minst omfatta:

- verksamhetens **beskrivning av behov och mål** med anskaffningen
- en utsedd **systemägare**
- en inledande **systemsäkerhetsanalys** med stöd av BITS Plus beroende på systemets betydelse. Analysen syftar till att klarlägga säkerhetskraven på det system som planeras att införas och den utökas därefter med en **kravspecifikation** som minst omfattar:
  - integrationskrav med andra system
  - krav på test
  - tidplan
  - personella och ekonomiska resurser
  - klarlägga behov av användarutbildning

Ansvarig för nyanskaffningsprojekt förbereder överlämnandet från test och utveckling till drift och förvaltning tillsammans med den tilltänkte **systemägaren**. Beslut om tidpunkt från vilken systemet övergår från projekt till förvaltning fattas av systemägaren. I och med detta övergår ansvaret till systemägaren som då också övertar all dokumentation samt upprättar **SNÖ-avtal** och en **systemsäkerhetsanalys**.

Klassning av information

Information som hanteras i IT-baserade informationssystem

För information som lagras i informationssystem måste inte bara sekretessaspekten beaktas, utan även kraven på riktigheten i informationen och tillgängligheten till den.

Säkerhets-aspekt / Kravnivå	Sekretess (konfidentialitet)	Riktighet	Tillgänglighet
Mycket hög nivå	Information som kan medföra mycket allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra mycket allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som ska vara åtkomlig inom högst 2 timmar inom kontorstid för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person
Hög nivå	Information som kan medföra allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som inte behöver vara åtkomlig inom 2 timmar, men inom högst 8 timmar inom kontorstid för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person
Basnivå	Information som kan medföra mindre allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den röjs för obehörig	Information som kan medföra mindre allvarliga negativa konsekvenser för egen eller annan organisations verksamhet eller för enskild person om den är felaktig	Information som inte behöver vara åtkomlig inom 8 timmar inom kontorstid för att inte medföra oacceptabla konsekvenser för egen eller annan organisations verksamhet eller för enskild person

Anm: Följande typ av information hanteras utanför klassningsmodellen:

- Information som avser rikets säkerhet. Sådan information ska hanteras enligt särskilda bestämmelser.
- Information som har extrema krav på sig att vara tillgänglig.
- Information som inte bedöms ha krav på sig vare sig avseende sekretess (konfidentialitet), riktighet eller tillgänglighet.

De åtgärder som ska vidtas för att uppfylla säkerhetskraven på respektive informationssystem framgår av analys av dessa med BITS Plus.

Säkerhet i utvecklings- och underhållsprocesser

Förslag om önskemål på förändringar i systemen lämnas till systemägaren. Arbetet bedrivs enligt Katrineholms kommuns modell för införande och utveckling av informationssystem.

Hantering av informationssäkerhetsincidenter

Vid misstanke om intrång eller andra incidenter ska användare agera enligt informationssäkerhetsinstruktion för Användare (Infosäk A)

Informationssäkerhetssamordnaren ska sammanställa och rapportera till IT-chef:

- intrång och försök till intrång
- brott mot lagstiftning och internt regelverk
- incidenter som orsakar eller skulle kunna orsaka betydande avbrott och störningar
- konsekvenser och förslag till åtgärder efter intrång eller funktionsfel

Efterlevnad av rättsliga krav

Anvisningar för skydd av register och handlingar ska följas, se Infosäk A.

Miljö och IT

Katrineholms kommun ska vara ett föredöme när det gäller att ta ansvar för miljön och människors hälsa och ska därför så långt det är möjligt välja de ur miljösynpunkt bästa alternativen vid inköp och upphandlingar. De leverantörer som används vid inköp av IT-utrustning är valda för att uppfylla detta syfte.

IT-utrustning och el skrot lämnas till återvinning för att användbara delar ska tas tillvara och övrig sorteras med tanke på vårt ansvar för miljön.

Revidering

IT-chef reviderar fortlöpande detta dokument med IT-rådet som referensgrupp. Giltighet av detta dokument följer Informationssäkerhetspolicyn.

Referenser

Katrineholms kommuns Informationssäkerhetspolicy, KS 2010/311

Basnivå för Informationssäkerhet – BITS, http://www.msb.se

KOMMUNLEDNINGSFÖRVALTNINGEN

Datum
2013-09-16

Informationssäkerhetsinstruktion för användare

Revisionshistoria:
2010-04-21 SITHS-projektet Version 1
2010-08-19 Version: 1.1
2011-01-25 Version: 1.2
2013-07-01 Reviderad: 2.0

Innehållsförteckning

Inledning

Med *informationssäkerhet* avses den samlade effekten av de skyddsåtgärder som tillsammans minskar eller eliminerar effekterna av hot och risker som riktar sig mot IT-stödets och informationsresursernas tillgänglighet, riktighet, sekretess och spårbarhet.

Med *information* avses här all information oberoende av i vilken form eller miljö den förekommer - den kan vara muntlig*, skriven, tryckt eller elektronisk. Då datorer och it-system idag har en så central roll som bärare av information blir denna instruktion dominerad av frågor rörande detta.

Styrande dokument för arbetet med informationssäkerhet i Katrineholms kommun är informationssäkerhetspolicy med tillhörande instruktioner.

Denna Informationssäkerhetsinstruktion för användare (**Infosäk A**) redovisar hur användaren ska agera för att upprätthålla god säkerhet.

Syfte

För att skydda de värden informationen representerar krävs ett säkerhetsmedvetande hos alla. Användarinstruktionen ska hjälpa dig leva upp till de säkerhetskrav som ställs och ge kunskap om vilket ansvar du har.

Efterlevnad

Vid underlåtenhet att följa eller medvetet bryta mot användarinstruktionen görs en utredning i samråd med it-kontoret och personalkontoret. Efter utredning kan rätten att använda it-resurser begränsas eller återkallas och arbetsrättsliga åtgärder som disciplinpåföljd bli aktuella.

* Muntligen överförd information ges inte mycket utrymme i denna instruktion. Samtidigt kan vi konstatera att vi inom det området har några av de största hoten mot vår informationssäkerhet. Det är viktigt att var och en tänker på *var* man pratar och med *vem*. Ett stort ansvar vilar på den enskilde kring de sekretessbelagda uppgifter man tar del av i sitt arbete.

Din arbetsplats

Med din arbetsplats menar vi din fysiska arbetsplats och den IT-utrustning du hanterar i ditt arbete.

Programvaror

Med programvara menar vi datorprogram som är avsedda att installeras på din dator och användas i syfte att underlätta dina arbetsuppgifter.

Respektive programvaras licensavtal bestämmer hur programvaran får hanteras. De program som krävs för att du ska kunna utföra ditt arbete på ett tillfredställande sätt ska finnas installerat på datorn. Beslut gällande detta fattas av din chef i samråd med IT-kontoret. Giltig licens erfordras.

Om du lämnar arbetsplatsen

När du lämnar arbetsplatsen för dagen ska du alltid stänga av din dator av miljö- och säkerhetsskäl. Datorn ska däremot alltid vara ansluten till strömuttag och nätverk eftersom underhåll av datorn och program kan ske nattetid via nätverket. Datorer som ej är anslutna kommer uppdateras/installeras vid nätanslutning.

Blåtand (bluetooth)

Blåtand eller bluetooth är en standard för trådlös kommunikation mellan olika enheter, som te.x. en dator och ett tangentbord.

Blåtand på din IT-utrustning ska generellt ska vara avstängd då du inte använder den. Tänk på att byta till ett personligt lösenord. När blåtand är påslagen bör du iaktta försiktighet.

Trådlöst nät (WLAN)

Det trådlösa nätet på din IT-utrustning ska generellt vara avstängd då du inte använder det. Tänk på att information som skickas över oskyddat nätverk kan vara synligt för andra.

Katrineholms kommuns, administrativa och pedagogiska, trådlösa nätverk kräver att det finns ett certifikat på datorn. Det publika trådlösa nätverket kräver inloggningsuppgifter och ger endast tillgång till Internet.

Användarens ansvar

Du ska

- ha antivirusprogram installerat och uppdaterat på din pc, smartphone och läsplatta
- vid installationer av ”appar” på läsplatta och smartphone noga kontrollera appens åtkomstbehörigheten
- ha skärmlås aktiverat på din dator, smartphone och läsplatta
- låsa ditt rum eller lägga in akter i dokumentskåp när du lämnar rummet, om du hanterar handlingar med sekretessuppgifter
- låsa din dator när du lämnar rummet (Ctrl+Alt+Del och välj Lås datorn)

Kontakta Service Desk, 6900, vid:

- fysiska ingrepp på din IT-utrustning
- felanmälan av IT-utrustning
- beställning av installation och konfiguration på IT-utrustning
- kassering av IT-utrustning
- återställning av backup

Du får inte

- installera egna programvaror på datorer som är anslutna till kommunens nätverk

Tänk också på att

Du lämnar spår efter dig när du är inloggad och arbetar i systemen. Systemen kan därför spåra bland annat obehörig åtkomst. Syftet med att kunna spåra användandet av systemen är att skydda informationen och för att undvika att oskyldiga misstänks, om oegentligheter inträffar.

Loggar är allmän handling och innebär att de ska lämnas ut på begäran från myndigheter, allmänhet eller media.

Tänk på att flyttbara lagringsmedia som t.ex. CD, USB-minnen, mobiltelefoner, m.m., kan innehålla skadlig kod (t.ex. virus). Rådfråga Service Desk, 6900, om du är osäker.

När du får besök av it-tekniker för hjälp med datorn, be dem gärna att legitimera sig så att du vet var de kommer ifrån.

Du bör ha samma säkerhetstänkande när du hanterar papper och pärmar, som när du hanterar information med hjälp av datorer och telefoner.
Vid utskrift av känslig information var noga med att direkt gå och hämta utskrifter.

För att en bärbar dator ska vara så säker som möjligt, ska du kontinuerligt (minst en gång per vecka) ansluta den till Katrineholms kommuns nätverk. Då blir virusskydd och andra säkerhetsprogram uppdaterade.

Åtkomst till information

Dina arbetsuppgifter avgör vilka behörigheter du har och beslut om behörighet fattas av din chef eller informationsägaren.

Inloggning till datorn/nätverket

Innan du första gången loggar in i nätverket får du ett användarnamn och lösenord av din närmaste chef eller av denne utsedd person.
Vid första inloggningen blir du uppmanad att byta lösenordet. Lösenordet ska uppfylla punkterna nedan. Lösenord är personliga och ska hanteras därefter.

Katrineholms kommuns lösenordsstandard

- ska vara minst nio tecken långt
- ditt nya lösenord måste innehålla minst **3** av följande teckengrupper:
  - 1 stor bokstav
  - 1 liten bokstav
  - 1 siffra (0-9)
  - 1 specialtecken (= + # % & / (!) ? < > | @ $ { [ ] } \ ' * , ; . _: -)
- kan inte vara samma som något av dina tidigare 24 lösenord
- måste skilja sig från ditt förra lösenord med mer än bara sista tecknet
- kan inte vara samma som användarnamnet
- kan bara bytas av användaren en gång per dygn, 24 timmarsperiod
- efter 10 misslyckade inloggningsförsök så låses kontot,
  efter 30 min så låses kontot upp igen och man får yttligare 10 nya inloggningsförsök.

Byte av lösenord

I det administrativa nätverket ska byte av lösenord ske var 90:e dag. 10 dagar innan det är dags att byta lösenord visas en dialogruta på ditt datorskrivbord samt e-post skickas till tillhörande e-postlåda.
Lösenordet ska omedelbart bytas om du misstänker att någon annan känner till ditt lösenord.

Lösenord i verksamhetssystem

Lösenord till respektive verksamhetssystem administreras av systemägare eller av denna utsedd person. Tidsintervallet beslutas av respektive systemägare.
Rekommendation är att dessa lösenord följer samma regelverk som lösenord i det administrativa nätverket.

Användarens ansvar

Du ska:

- ha ett lösenord som består av minst 9 tecken enligt Katrineholms kommuns lösenordsstandard

Du får inte:

- lämna (låna) ut kontot till någon annan
- utnyttja någon annans konto

Tänk också på att
Använd inte samma lösenord på publika tjänster på Internet som du använder hos kommunen.

Om du läser eller ändrar uppgifter som du inte har rätt till och till exempel utan medgivande använder någon annans lösenord görs en utredning av personalkontoret och åtalsanmälan för dataintrång kan aktualiseras hos åklagarmyndighet.

Lagring av information

Varje användare i Katrineholms kommun är ansvarig för att informationen lagras på tilldelat diskutrymme. Den information du lagrar på våra gemensamma utrymmen säkerhetskopieras. Information bör ej sparas på lokal disk (C:\).

Lagra information efter åtkomstbarhet enligt följande:

- G:\ (Gemensam) är en enhet för lagring av information som du och medarbetarna på din förvaltning har tillgång till.
- H:\ (Hemkatalog) är din personliga enhet som du kan använda för lagring av eget arbetsmaterial. Om du väljer H-enheten kommer dina medarbetare inte åt informationen.
- K:\ (Kommungemensam) är en enhet för lagring av information som du och dina medarbetare gemensamt inom kommunen har tillgång till, tänk på att det passerar myndighetsgränsen på denna enhet.

Lagring av information på olika media

Följande krav gäller:

Krav på sekretess	**Åtgärder**
Mycket hög nivå (Informationen får inte röjas)	Förvaring - Förvaras inlåsta - Endast CD-R eller DVD-R får användas för data Kopiering - Får kopieras endast med godkännande från systemägaren för systemet som informationen kommer ifrån Återanvändning - Får inte återanvändas Destruktion - Papper och OH-film destrueras i papperstugg - IT-chef/Informationssäkerhetssamordnaren kontaktas för beslut om tillvägagångssätt för datamedia.
Hög nivå (Informationen kan ge negativa konsekvenser för organisationen eller enskild person om den röjs)	Förvaring - Ej förvaras synligt - Endast CD/DVD-skiva eller USB-media får användas för data Kopiering - Får kopieras i samråd med systemets förvaltare/administratör Återanvändning - Tillåten Destruktion - Papper och OH-film destrueras i papperstugg - Datamedia lämnas till 6900 för destruktion
Basnivå (Informationen kan inte ge negativa konsekvenser för organisationen eller enskild person om den röjs)	Förvaring - Inga krav Kopiering - Tillåten Återanvändning - Tillåten Destruktion - Krävs ej

Användarens ansvar

Du får inte

- lagra sekretesshandlingar på din egen dator, USB-minne eller CD-skiva eller andra mobila/bärbara enheter
- lagra allmänna handlingar eller verksamhetskritisk information på en extern lagringsplats där det inte finns avtal med kommunen som reglerar villkoren (Hotmail, Facebook, Youtube, etc).

Tänk också på att
Vissa verksamheter ställer extra höga krav på hanteringen av sekretesshandlingar (hälso- och sjukvården och socialtjänsten). Den som uppsåtligen eller av oaktsamhet röjer sekretessbelagd uppgift kan dömas till brott mot tystnadsplikten.

Information lokalt på datorarbetsplatsen säkerhetskopieras inte. Därför kommer informationen försvinna vid dataförlust i samband med service, stöld, haverier eller liknande. IT-kontoret har inget ansvar för förlorad information lokalt på datorarbetsplatsen.
Sekretessbelagd information får endast lagras på server.

Internet

När du använder Internet kan säkerheten i kommunens lokala nätverk påverkas negativt beroende på ditt beteende, till exempel beroende på vilka sidor du besöker.

När du surfar på Internet representerar du Katrineholms kommun och bör därför agera enligt Katrineholms kommuns värdegrund (RÖTT).

På datorerna finns ett skydd mot barnpornografi (NetClean) installerat. Programmet genomsöker datorerna och vid upptäckt skickas rapport till IT-kontoret varvid en polisanmälan sker.

Internet ska ses som ett arbetsredskap där medarbetarna kan hämta information och tjänster som är till nytta och stöd i arbetet. Privat användning i begränsad omfattning är tillåten om det inte påverkar arbetet på ett negativt sätt.

Användarens ansvar

Du får inte
- besöka oetiska sidor så som sidor med rasistiskt, pornografiskt eller olagligt innehåll*
- ladda ner och själv installera programvara från Internet

Tänk också på att
Du lämnar spår i en fil som loggar internettrafiken på kommunen. Denna loggfil är allmän offentlig handling (det innebär att vem som helst har rätt att veta vilka sidor du besökt på jobbet) och visar vilka webbplatser du har besökt.

Bilder och annat material kan vara upphovsrättsskyddat (Copyright)

E-post

E-post är ett hjälpmedel i arbetet men minneskapaciteten för att spara e-post är begränsad. Underhåll därför regelbundet mapparna ”Inkorgen”, ”Skickat”, och ”Borttaget” för att frigöra utrymme. Din e-post spärras om minnet blir fullt. Spara meddelanden, bifogade filer med mera, på samma sätt som du lagrar annan information.

Så väl personliga e-postlådor som myndighetsbrevlådor ska kontrolleras varje vardag för att bedöma inkommen e-post utifrån om diarieföring är nödvändlig.

Användarens ansvar

Du ska

- vid sjukdom eller frånvaro (mer än 1 dag) se till att din brevlåda stängs eller hanteras av ett av dig utsett ombud, om du inte har möjlighet att själv bevaka den.
- ha en e-postsignatur som är utformad i enighet med den för verksamheten gällande grafiska profilen
- kontakta din chef om du får hotbrev
- kontakta Service Desk, 6900, om du misstänker att det kommit in virus via e-postsystemet
- låta registrera allmänna handlingar oavsett om de inkommer med e-post eller vanlig post

* Undantag kan finnas om syftet är uppenbart arbetsrelaterat.

Du får inte

- skicka sekretessbelagd eller annan integritetskänslig information via e-post.
- skriva någon känslig information i ämnesraden
- använda e-post för att sända spam eller kedjebrev
- öppna en bifogad fil eller länk om du är tveksam på dess innehåll

Tänk också på att

Det är viktigt att tänka på att meddelande via e-post omfattas av bestämmelser om offentlighet och sekretess på samma sätt som mer traditionella handlingar.
Samma regler gäller för diarieföring av e-post som för vanliga brev.

Du uppträder som representant för kommunen när du använder kommunens e-post.

Ange alltid ett relevant ämne i ämnesraden för meddelandet, för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-posten.

Kontrollera vilka som är medlemmar på sändlistor innan du använder dem, sändlistor innebär risk att känslig information når fel mottagare.
För att minska risken för så kallat SPAM bör du tänka på hur du sprider din e-postadress.

E-postsystemet är ett arbetsverktyg och bör inte användas för privat bruk.

Incidenter, virus m.m.

En it-incident är en oönskad och oplanerad störning som drabbar eller påverkar ett it-system. Som incident räknas även upptäckt av otillåten användning och obehörigt intrång i it-system samt upptäckt av misstänkt ”skadliga koder” (virus, trojaner m.m.).

Skadlig kod förekommer i otaliga varianter och nya kommer fortlöpande, mer eller mindre dagligen med illvilliga avsikter att infektera och skada ett system eller dator. Virusprogram uppdateras för att klara nya virus men kan aldrig bli 100 % säkra.

Säkraste skyddet mot virusangrepp är att ***inte*** ladda ner filer från Internet och att ***inte*** öppna bilagor i e-posten från okända avsändare.

It-kontoret har ansvar för att din dator har ett virusskydd som är aktiverat och uppdaterat. Detta förutsätter dock att du är inloggad i nätverket.

Katrineholms kommun rapporterar IT-incidenter till identifierad användares närmsta chef. Om incidenten beror på kriminell handling, gör Katrineholms kommun en polisanmälan efter samråd med personalchefen.

Användarens ansvar

Du ska

om du misstänker att du varit utsatt för någon typ av incident:

- notera när du senast var inne i IT-systemet
- notera när du upptäckte incidenten
- omedelbart anmäla förhållandet till Service Desk, 6900, och din chef.
- dokumentera alla iakttagelser i samband med upptäckten och försök fastställa om din information har påverkats.

vid misstanke om virus:

- dra ut nätverkskabeln och stänga av den trådlösa uppkopplingen, men låta datorn vara på.
- kontakta Service Desk, 6900, via telefon. Inte e-post.

Tänk också på att

Aldrig vidarebefordra e-post med misstänkt virus i, inte ens till Service Desk, 6900. En stor källa till virusspridning är just e-post, antingen via bifogade filer eller länkar i e-posten.

Handdatorer, digitala kameror, mobiltelefoner, skrivare, läs- och surfplattor med mera kan lätt bli virusbärare eftersom du kan mellanlagra information mellan olika datorer i dessa. Var noga med att den dator du ansluter sådan kringutrustning till har ett uppdaterat antivirusprogram.

Om du upptäcker fel och brister i de system du använder ska du rapportera dessa till systemägaren.

Vid anställningens upphörande

När du slutar din anställning ansvarar du för att rådgöra med din chef, eller utsedd person, om vilket av ditt arbetsmaterial som ska sparas. Notera att all information du framställer eller sparar, på av Katrineholms kommun ägd utrustning, under arbetstid anses vara Katrineholms kommuns egendom. Det innebär att information inte får tas med utan chefs godkännande.

Stöd och hjälp i it – frågor

Kontakt Service Desk
Telefon 0150-(5) 6900
E-post 6900@katrineholm.se

Öppettider Service Desk
Måndag-Fredag 07:00-17:00

Vid frågor som rör specifika verksamhetssystem kontaktar du din systemansvarige.

Stöd och hjälp kan också ges av it-samordnaren på din förvaltning.

Frågor kring denna instruktion eller om informationssäkerhet, kontakta
IT-kontoret på epost: ITK@katrineholm.se