Katrineholm

Informationssäkerhets-policy för Katrineholms kommun

Dokumentinformation

Beslutshistorik
Antagen av kommunfullmäktige 2010-06-21 § 106

Senast ändrad av kommunfullmäktige
2013-12-16 § 203

2021-06-14 § 95

Senast ändrad av kommunstyrelsen 2023-09-27, § 204 (förlängd giltighetstid)

Inlagda bilagor ses som verkställighetsdokument och hanteras på tjänstemannanivå.

Giltighet
Gäller från och med 2021-06-14

Gäller till och med 2027-12-31

Förvaltarskap[1]
Inom kommunstyrelsens ansvarsområde

Kategori
- Anvisningsdokument

Uppföljning
Hur:

När:

[1] 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

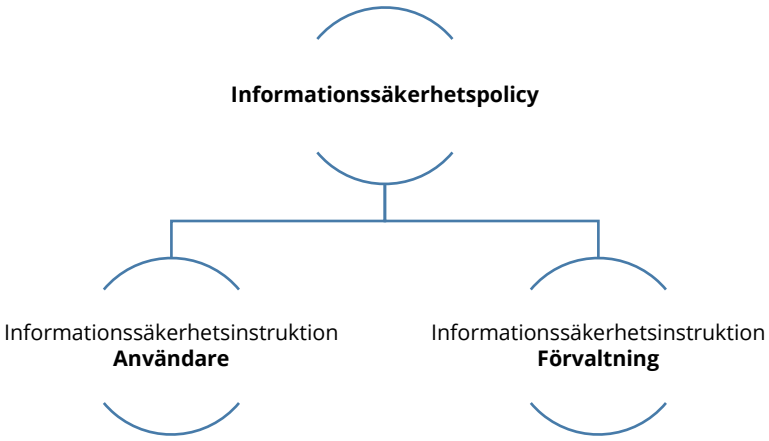
Innehåll

Informationssäkerhetspolicy för Katrineholms kommun

Informationssäkerhet är den del i organisationens lednings- och kvalitetsprocess som avser hantering av verksamhetens information. Informationssäkerhetspolicyn och särskilda informationssäkerhetsinstruktioner styr kommunens informationssäkerhetsarbete.

Policyns roll i informationssäkerhetsarbetet

Styrande dokument för informationssäkerhetsarbetet är Katrineholms kommuns informationssäkerhetspolicy och informationssäkerhetsinstruktionerna för användare och förvaltning.



Informationssäkerhetsinstruktion - Användare redovisar:

- hur en användare ska verka för att upprätthålla en god säkerhet.

Målgruppen för instruktionen är samtliga medarbetare vid kommunen samt andra parter som får tillgång till kommunens informationstillgångar.

Informationssäkerhetsinstruktion Förvaltning redovisar:

- det ansvar som ingår i de olika rollerna,
- hur informationssäkerhetsarbetet ska bedrivas,
- de riktlinjer som gäller för områden av särskild betydelse, samt
- regler för systemutveckling, systemunderhåll och incidenthantering.

Målgruppen för instruktionen är kommunens ledning, förvaltningsledning, systemägare och eventuell samordningsansvarig.

Allmänt om informationssäkerhet

Information är en av Katrineholms kommuns viktigaste tillgångar och hanteringen av den är en viktig del i arbetet med kommunens risk- och sårbarhetsanalys.

Utgångspunkter i Katrineholms kommuns arbete med informationssäkerhet är:

- lagar, förordningar och föreskrifter,

- krav uppsatta av Katrineholms kommun,
- avtal,
- att ge bättre förutsättningar för ledning, styrning, uppföljning, utvärdering och resursfördelning.

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer.

Informationssäkerheten omfattar kommunens informationstillgångar utan undantag. Med informationssäkerhet avses:

- att informationen endast delges behöriga personer (**konfidentialitet**), samt att informationen levereras vid rätt tidpunkt och till skäliga kostnader,
- att informationen är riktig, komplett och aktuell (**riktighet**),
- att information som efterfrågas och som kommunen har ett ansvar att tillhandahålla finns och inte medvetet eller omedvetet förstörs utan stöd i lag eller gallringsbeslut (**tillgänglighet**), och
- att eftersökande, förändring eller borttagning av information går att spåra (**spårbarhet**).

Informationssäkerheten är en integrerad del av Katrineholms kommuns verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det omfattar samtliga anställda, förtroendevalda, myndiga elever inom skola/vuxenutbildning och uppdragstagare som arbetar med kommunens information. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till säkerhetsarbetet.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för Katrineholms kommuns informationstillgångar. Rapporteringen ska ske till närmsta chef samt Informationssäkerhetsansvarig.

Alla delar inom kommunen är bundna av denna informationssäkerhetspolicy. Lokala avvikelser från denna policy inom organisationen är tillåtet, dock reglerar denna policy en miniminivå för hur informationssäkerhetsarbetet ska bedrivas. Eventuella lokala avvikelser får inte obefogat begränsa tillgången till information.

Den som använder Katrineholms kommuns informationstillgångar på ett sätt som strider mot denna policy kan bli föremål för disciplinära åtgärder.

Mål

För Katrineholms kommuns informationssäkerhetsarbete ska gälla att:

- all personal har kunskap om gällande informationssäkerhetsregler,
- att informationsförsörjningen är säker, effektiv och bidrar till ökat skydd och stöd för medarbetare, andra användare, samverkande partners och tredje man,
- ingångna avtal är kända och följs,
- krishanteringsförmågan upprätthålls,
- det finns tillgång till en gemensam, säker och väl definierad infrastruktur för extern och intern datakommunikation,
- hotbilden för varje enskilt informationssystem som är av vikt för Katrineholms kommuns verksamhet analyseras fortlöpande,
- händelser i informationssystemen som kan leda till negativa konsekvenser förebyggs, såsom förlust, skada, sabotage, förvanskning av information och otillbörlig åtkomst,
- årliga mål för arbetet beslutas i och framgår av verksamhetsplaneringen,

- Katrineholms kommun når sina övergripande visioner, strategier och mål.

Principer och arbetssätt

Katrineholms kommun ska arbeta med informationssäkerhet på ett sätt så att ovanstående mål uppfylls. Arbetet med informationssäkerhet ska gentemot kommunens verksamheter vara normerande, stödjande och kontrollerande.

Viktiga förmågor i det arbetet är att kunna identifiera hot, sårbarheter och risker rörande Katrineholms kommuns informationstillgångar samt att kunna utforma och införa säkerhetsåtgärder som reducerar dessa risker till en acceptabel nivå.

Arbetet med informationssäkerhet inom Katrineholms kommun ska:

- bygga på en helhetssyn som utgår från information, men som också innefattar processer, människor och teknik,
- vara systematiskt och bygga på den etablerade standardserien SS-ISO/IEC 27000 och dokumenteras i ett ledningssystem för informationssäkerhet,
- löpande ses över och förbättras, eftersom Katrineholms kommun och dess omvärld, inklusive hotbild, är under ständig förändring,
- vara förebyggande och proaktivt, men också ha en god förmåga att kunna hantera incidenter, allvarliga störningar och kriser som ändå kan inträffa,
- bygga på Katrineholms kommuns värderingar och ta hänsyn till verksamheters behov, externa krav samt rådande hotbild,
- vara väl kommunicerat till verksamheten; all personal ska fortlöpande få information och utbildning för att nå och upprätthålla ett högt säkerhetsmedvetande och för att kunna leva upp till denna policy och underliggande riktlinjer för informationssäkerhet,
- ske i aktiv samverkan med det omgivande samhället såsom myndigheter, företag och nätverk, särskilt sådana som är normgivande inom informationssäkerhet som till exempel SKR (Sveriges kommuner och regioner), MSB (Myndigheten för samhällsskydd och beredskap), SIS (Svenska institutet för standarder) och IMY (Integritetsskyddsmyndigheten).

Verksamhetsdriven informationssäkerhet genom informationssäkerhetsklassning

Verksamheter har ansvar för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras informationsmängder är, och därmed informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheter utifrån informationens skyddsvärde ställer krav på de aktörer som hanterar informationen, exempelvis användare, systemansvariga samt drifts- och systemleverantörer.

För detta ändamål ska informationsklassning tillämpas, där information klassas med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Därigenom kan en anpassad och effektiv informationssäkerhet skapas.

Katrineholms kommun ska tillämpa en enhetlig modell för informationsklassning som anger olika nivåer av skyddskrav vari information ska klassas baserat på interna och externa krav på informationens **konfidentialitet, riktighet, tillgänglighet** och **spårbarhet.**

Roller och ansvar

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet

Nedan beskrivs informationssäkerhetsansvaret för ett antal roller. Ansvaret och tillhörande åligganden för respektive roller beskrivs utförligare i Informationssäkerhetsinstruktion Förvaltning och Informationssäkerhetsinstruktion Användare.

Kommunstyrelsen har ägandeskapet för informationssäkerhetspolicyn och det övergripande ansvaret för informationssäkerheten. Kommunstyrelsen ansvarar även för att vid behov besluta om förändringar.

Nämnderna har det yttersta ansvaret inom respektive verksamhetsområde. Det innebär ansvar för att styrdokumentet beaktas i beslutsprocessen samt för att efterfråga och ta del av uppföljning.

Arkivmyndigheten/Arkivmyndigheterna leder arbetet med framtagande av dokumenthanteringsplaner, instruktioner för arkivering av digital/manuell information

Informationssäkerhetssansvarig har det operativa ansvaret för samordning av informationssäkerhetsarbetet i Katrineholms kommun. Det innebär ansvar för att dokumentet efterlevs, att det finns tillgängligt, att följa eventuellt ändrade förutsättningar för dokumentet, att dokumentet följs upp och revideras samt att dokumentet är aktuellt och uppdaterat. Informationssäkerhetsinstruktioner beslutas av Informationssäkerhetsansvarig. Referensgruppen i revisionsarbetet består av kommunjurist, säkerhetsansvarig, säkerhetsskyddsansvarig.

IT-säkerhetsansvarig samordnar arbetet med säkerheten i Katrineholms kommuns IT-miljö. IT-säkerhetsansvarig har tillsynsansvar för att IT-miljön är tillförlitlig och motsvarar interna och externa krav.

Dataskyddsombud kontrollera att dataskyddsförordningen (GDPR) följs inom Katrineholms kommun genom att utföra kontroller samt genomföra informations- och utbildningsinsatser.

Systemägaren är den som har ansvaret för den verksamhet som aktuellt informationssystem stödjer. Varje facknämnd utser systemägare för informationssystem inom nämndens ansvarsområde. Denna policy upphäver inte det normala linjeansvaret. Det är alltid nämnden/styrelsen som har det övergripande ansvaret för informationen i ett IT-system. Systemägaren ansvarar för att basnivån för informationssäkerheten uppnås.

Systemförvaltarna utses av respektive systemägare och ansvarar för den dagliga användningen av informationssystemen.

Medarbetare, förtroendevald och myndig elev i skola/vuxenutbildning har ett ansvar att följa Informationssäkerhetspolicyn, Säkerhetsinstruktion Förvaltning och Säkerhetsinstruktion Användare.

Revidering och uppföljning

Revidering:

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

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

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

Katrineholm

Informationssäkerhetsinstruktion

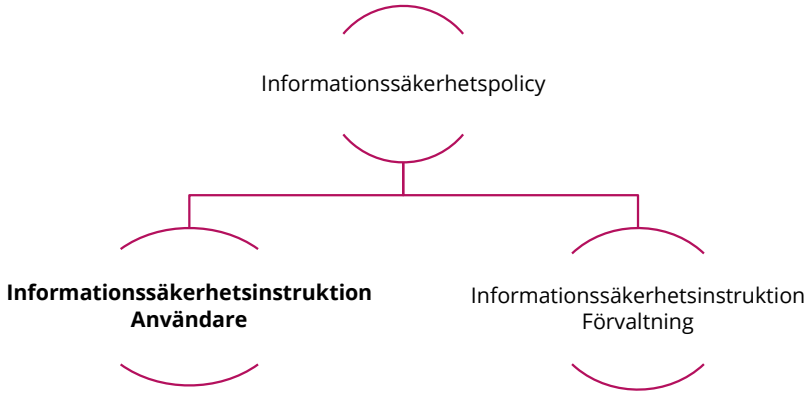
Användare

Katrineholms kommun

Innehåll

1. Instruktionens roll i informationssäkerhetsarbetet

Styrande dokument för informationssäkerhetsarbetet är Katrineholms kommuns informationssäkerhetspolicy och informationssäkerhetsinstruktionerna för användare, förvaltning samt kontinuitet och drift.



Informationssäkerhetspolicyn redovisar Katrineholms kommuns viljeinriktning och mål för informationssäkerhetsarbetet och syftar till att klarlägga:

- organisation och roller för informationssäkerhetsarbetet, och
- krav på riktlinjer för områden av särskild betydelse.

Informationssäkerhetsinstruktion Användare redovisar hur en användare ska verka för att upprätthålla en god säkerhet. Målgruppen för instruktionen är samtliga medarbetare vid kommunen samt andra parter som får tillgång till kommunens IT-system.

Informationssäkerhetsinstruktion Förvaltning redovisar:

- det ansvar som ingår i de olika rollerna,
- hur informationssäkerhetsarbetet ska bedrivas,
- de riktlinjer som gäller för områden av särskild betydelse, samt
- regler för systemutveckling, systemunderhåll och incidenthantering.

Målgruppen för instruktionen är kommunens ledning, förvaltningsledning, systemägare och eventuell samordningsansvarig.

Information gällande organisation och ansvar för drift av informationssystemenen, samt regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering framgår i avtal rörande IT-drift.

1.1 Definitioner

Med ***informationssäkerhet*** avses den samlade effekten av de skyddsåtgärder som tillsammans minskar eller eliminerar effekterna av hot och risker som riktar sig mot informationens konfidentialitet, riktighet, tillgänglighet 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 central roll som bärare av information blir denna instruktion dominerad av frågor rörande detta.

Med ***IT-resurser*** avses exempelvis (men är inte begränsat till) datorer, mobiler, nätverk, programvara, lagringsmedia samt applikationer som är till för att stödja medarbetaren i det dagliga arbetet.

2. Användarens ansvar

Som användare (medarbetare, förtroendevald och myndig elev i skola/vuxenutbildning) av Katrineholms kommuns IT-system och nätverk har du ett ansvar att läsa och följa Informationssäkerhetspolicyn, Informationssäkerhetsinstruktion Förvaltning och Informationssäkerhetsinstruktion Användare.

Information är en av Katrineholms kommuns viktigaste tillgångar. För att skydda denna krävs ett säkerhetsmedvetande hos alla användare och som användare har du ett stort ansvar för säkerheten i all informationshantering.

Vid eventuella oklarheter om vad som gäller för dig som användare vid din användning av Katrineholms kommuns IT-system och nätverk så kontaktar du din chef eller Digitaliseringsavdelningen för vägledning.

3. Din arbetsplats

Med din arbetsplats menas din fysiska arbetsplats och den IT-utrustning, nätverk, program och system som du hanterar i ditt arbete.

3.1 Utrustning

För den utrustning som du förfogar över, d.v.s. stationär, dockningsbar PC/Mac och/eller bärbar PC/Mac med tillhörande utrustning, smartphone, surfplatta gäller:

- Fysiska ingrepp får endast utföras av ServiceDesk, 569 00.
- Fel ska omgående anmälas till ServiceDesk, 569 00.
- All installation och konfiguration får endast utföras av ServiceDesk, 569 00.
- Har du en bärbar dator ska den anslutas till Katrineholms kommuns nätverk minst en gång per vecka för att virusskydd och andra säkerhetsprogram ska bli uppdaterade.

3.2 Programvaror

- Programvaror ska godkännas och installeras av ServiceDesk eller av ServiceDesk anvisad/godkänd person.
- Egna program kan inte, och får inte, installeras i Katrineholms kommuns datorer.
- Det är inte tillåtet att kopiera eller använda Katrineholms kommuns program utanför kommunens verksamhet.
- Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din chef.
- Vid installationer av appar på läsplatta och smartphone ska du vara noga med att kontrollera appens åtkomstbehörigheter.
- Du får endast installera appar som kommer från App Store, Google Play eller Windows Store.

3.3 Service på utrustning

Vid service som innebär att din utrustning lämnas till någon utanför Katrineholms kommun ska känslig information tas bort innan utlämnande.

Om du får besök av en It-tekniker för hjälp med datorn eller annan utrustning, be om legitimation så att du vet vem det är och varifrån personen kommer.

Om en It-tekniker efterfrågar ditt lösenord ska du inte lämna ut det

3.4 Kassering av utrustning

Kontakta ServiceDesk, 569 00, för destruktion.

3.5 Om du lämnar arbetsplatsen

Vid tillfällen när du inte har uppsikt över arbetsstationen ska du låsa den tillfälligt. Detta kan du göra med kortkommandot (Endast Windows): Ctrl + Alt + Del och välj ”Lås datorn”.

Din dator, telefon eller surfplatta ska alltid ha skärmlåset aktiverat.

Om du hanterar handlingar med sekretessuppgifter ska du när du lämnar ditt rum alltid låsa rummet eller lägga in akter i dokumentskåp.

När du lämnar arbetsplatsen för dagen ska du låta din dator vara i gång. Den ska 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.

3.6 Blåtand (Bluetooth)

Blåtand är en standard för trådlös kommunikation mellan olika enheter, som till exempel en dator och ett tangentbord.

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

3.7 Trådlöst nät (WLAN/WiFi)

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.

För att använda Katrineholms kommuns, administrativa och pedagogiska, trådlösa nätverk krävs att ServiceDesk försett datorn eller surfplattan med en nätverksnyckel. Publika trådlösa nätverket (exempelvis ”Anslutning Katrineholm”) kräver inga inloggningsuppgifter och ger endast tillgång till internet. Du ska inte använda ”Anslutning Katrineholm” för verksamhetsrelaterade arbetsuppgifter.

4. Åtkomst till information

4.1 Behörighet

Katrineholms kommuns informationssystem är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och avgörs av din chef.

Du får ej låta någon annan nyttja dina inloggningsuppgifter och därmed få del av det du är behörig till. Detta gäller även om den andra personen befinner sig på samma eller högre behörighetsnivå som den du eventuellt tillhör.

Alla inloggningar i kommunens system loggas, loggar är allmän handling och innebär att de lämnas ut på begäran från myndigheter, allmänhet eller media.

4.2 Inloggning

Innan du loggar in första gången ska du läsa och följa Informationssäkerhetspolicyn, Informationssäkerhetsinstruktion Förvaltning och Informationssäkerhetsinstruktion Användare.

Du får du ett lösenord av din chef eller ServiceDesk, 569 00, för åtkomst till Katrineholms kommuns interna IT-nätverk. Lösenordet ska du byta till ett personligt lösenord efter första inloggningen. Samma förfarande gäller för enskilda informationssystem som kräver lösenord för åtkomst.

Lösenord är strängt personliga och ska hanteras därefter. Du lämnar spår efter dig när du är inloggad och arbetar i systemen. De loggningsfunktioner som finns i systemen används för att spåra obehörig åtkomst. Detta för att skydda informationen och för att undvika att oskyldiga misstänks om oegentligheter inträffar.

Om lösenordet är bortglömt ta kontakt med ServiceDesk, 569 00, för att få ett nytt engångslösenord.

4.3 Typ av lösenord

När det är möjligt använd lösenord som:

- består av minst 16 tecken och
- är sammansatt av minst fem olika ord, gärna blandad storlek på bokstäver samt siffror och specialtecken.

4.4 Byte av lösenord

Byte av lösenord är aktuellt:

- Omedelbart om du misstänker att någon annan känner till det eller att du misstänker att någon loggat in på ditt personliga konto.
- För enskilda system administreras lösenord av systemägare eller någon som systemägaren utsett. Tidsintervallet beslutas av respektive systemägare. Rekommendationen är att dessa lösenord följer samma regelverk som lösenord i det administrativa nätverket.

4.5 Hantering av lösenord

Du får inte:

- Skriva upp lösenordet och förvara det i anslutning till dator, telefon eller plånbok.
- Lämna ut lösenordet till någon annan.
- Nyttja någon annans lösenord för att använda dennes konto.

5. Klassning och hantering av information

5.1 Klassning av information

Informationssystem inom Katrineholms kommun klassas utifrån den information som hanteras i systemet. Klassning görs från aspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet. Med detta menas:

Konfidentialitet: Att informationen skyddas från obehörig insyn.

Riktighet: Att informationen inte ändras på ett obehörigt sätt.

Tillgänglighet: Att informationen finns tillgänglig för rätt person vid rätt tillfälle.

Spårbarhet: Att eftersökande, förändring eller borttagning av information går att spåra.

Tas information ut ur systemet och lagras på andra media, eller används i ett annat sammanhang, måste den klassas där den används och hanteras därefter.

Även information i arbetsmaterial måste klassas.

Katrineholms kommuns klassningsmatris framgår av bilaga *Klassningsmatris*.

5.2 Lagring

Den information du lagrar på Katrineholms kommuns gemensamma utrymmen säkerhetskopieras automatiskt. Du kan välja att lagra på enheterna G:, K:, OneDrive, SharePoint och Teams samt i de olika verksamhetssystemen som används inom kommunen. Inom Bildningsförvaltningen och skolorna används även Google for Education med tillhörande Google Drive för lagring. Kommunen säkerhetskopierar inte information som lagras i Googles verktyg och tjänster.

G: (Gemensam) är en enhet för lagring av information som du och medarbetarna på din förvaltning har tillgång till. Användningen av **G:** ersätts av **SharePoint** med undantag för sekretessbelagd information som ska lagras i speciella kataloger på **G:**

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 myndighetsgränser på denna enhet och att viss information inte får föras över sådana gränser. Användningen av **K:** för lagring av information som kan delas inom hela kommunen över myndighetsgränser ersätts av **SharePoint**.

OneDrive är din personliga enhet som du kan använda för lagring av personligt arbetsmaterial. Om du väljer **OneDrive** kommer dina medarbetare ej åt informationen om du inte explicit väljer att dela informationen med någon/några kollegor. **Du får inte lagra eller bearbeta sekretessbelagd information i OneDrive.**

SharePoint är en enhet för lagring av information som du och medarbetarna på din förvaltning har tillgång till. Här lagras även information som delas av hela kommunen eller mellan förvaltningar. **Du får inte lagra eller bearbeta sekretessbelagd information i SharePoint.**

Teams i Teams kan du lagra och dela filer med kollegor i samma Teams-grupp. **Du får inte lagra eller bearbeta sekretessbelagd information i Teams.**

I förekommande fall kan också ytterligare enhetsbeteckningar finnas.

Om du lagrar information och filer på din lokala hårddisk i datorn är du personligen ansvarig för säkerhetskopiering. När du lagrar information på din lokala hårddisk riskerar du att förlora information som inte kan återskapas till rimliga kostnader, vid till exempel en diskkrasch. Undvik därför att lagra på den lokala hårddisken.

Om du använder en av Katrineholms kommuns bärbara datorer för hem- eller distans-arbete ska du tänka på att den kan utgöra en säkerhetsrisk och att du därför **inte får lagra sekretessbelagd eller för verksamheten känslig information på den. Du får inte lagra sekretessbelagd eller verksamhetskritisk information på en extern lagringsplats, såsom i molnet.**

Sekretessbelagd information får ej heller lagras på mobiler eller andra bärbara enheter.

Tänk på att flyttbara lagringsmedia som till exempel CD, USB-minnen, mobiltelefoner, med mera, kan innehålla skadlig kod (till exempel virus). Rådfråga ServiceDesk, 569 00, om du är osäker. Anslut aldrig en okänd USB-enhet till någon av Katrineholms kommuns datorer.

5.2.1 Krav på förvaring/lagring utifrån klassningsnivå (Se bifogad klassningsmatris)

Krav utifrån klassningsnivå	Åtgärder
Nivå 3 (Röjande av informationen, obehörig förändring informationen, otillgänglighet av informationen samt avsaknad av spårbarhet av informationen medför allvarlig skada.)	**Förvaring** • Förvaras inlåsta. **Kopiering** • Får kopieras endast med godkännande från systemägaren för systemet som informationen kommer ifrån. **Återanvändning** • Får inte återanvändas. **Destruktion** • Papper destrueras i pappersstrimlare. Digitaliseringschef/Informationssäkerhetsansvarig kontaktas för beslut om tillvägagångssätt för datamedia.
Nivå 2 (Röjande av informationen, obehörig förändring informationen, otillgänglighet av informationen samt avsaknad av spårbarhet av informationen medför betydande skada.)	**Förvaring** • Förvaras inlåst. **Kopiering** • Får kopieras i samråd med systemets förvaltare/administratör. **Återanvändning** • Tillåten **Destruktion** • Papper destrueras i pappersstrimlare. Datamedia lämnas till Servicedesk för destruktion.
Nivå 1 (Röjande av informationen, obehörig förändring informationen, otillgänglighet av informationen samt avsaknad av spårbarhet av informationen medför måttlig skada.)	**Förvaring** • Förvaras ej synlig **Kopiering** • Tillåten **Återanvändning** • Tillåten **Destruktion** • Krävs ej.

För mer information se bilaga *Klassningsmatris*.

6. Internet

När du använder internet kan säkerheten i Katrineholms kommuns lokala nätverk påverkas i mycket hög grad beroende på ditt beteende. Katrineholms kommun förutsätter att den som surfar på internet endast besöker välrenommerade webbplatser.

Det är inte tillåtet att via internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (ras, hudfärg, kön, religion, tillhörighet till etnisk grupp eller sexuell läggning) eller har anknytning till kriminell verksamhet.

På datorerna finns ett skydd mot barnpornografi installerat. Programmet genomsöker datorerna och vid upptäckt skickas rapport till ServiceDesk varvid en polisanmälan sker.

I specifika fall kan det dock vara motiverat för arbetet, till exempel vid utredningar, omvärldsanalyser mm, att besöka sidor som normalt är förbjudna. Beslut om detta ska fattas av närmaste chef.

Tänk på att när du surfar på internet representerar du Katrineholms kommun och lämnar spår efter dig i form av Katrineholms kommuns IP-adress.

Internet ska ses som ett arbetsredskap där medarbetarna kan hämta information och använda 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.

7. E-post

Du är skyldig att läsa din e-post varje vardag. Vid ledighet eller sjukdom ska e-post vidare-befordras till en annan person eller en enhetsbrevlåda. Information om var e-posten vidarebefordras ska skrivas i ett frånvarobesked som skickas till den som sänt e-posten. Detta besked skrivs in och periodsätts manuellt, sedan skickar e-postsystemet frånvaro-beskedet det automatiskt till avsändaren till den inkomna e-posten.

- E-post med bilagor utgör ett stort hot när det gäller spridning av virus. Öppna inte en bifogad fil eller länk om du är tveksam på dess avsändare eller innehåll.
- De regler som gäller för diarieföring av vanliga brev gäller även e-post.
- De regler som gäller för kassering av vanliga brev gäller även för radering av e-post.
- Om du misstänker att det kommit in virus via e-postsystemet ska du agera som det beskrivs i avsnittet om incidenter nedan.
- Det är inte tillåtet med automatisk vidarebefordring till e-postadress utanför Katrineholms kommuns domän.
- Ange alltid ämne i ämnesraden för meddelandet för att klargöra för mottagaren vad denne kan förvänta sig för innehåll i e-posten.
- Skriv inte någon känslig information i ämnesraden.
- Kontrollera vilka som är medlemmar på sändlistor innan du använder dem. (Risk att känslig information når fel mottagare.)
- Skicka inte eller vidarebefordra spam eller kedjebrev.
- Om du får hotbrev ska du spara brevet och kontakta din chef.
- Kontakta ServiceDesk via telefon, 569 00, om du misstänker att det kommit in virus via e-postsystemet.
- E-post omfattas av GDPR och hanteras i enlighet med GDPR

Observera. E-postsystemet får inte användas för att skicka sekretessbelagd eller integritetskänslig information samt känsliga personuppgifter.

8. Incidenter, virus med mera

En IT-incident är en oönskad och oplanerad störning som drabbar eller påverkar ett IT-system eller IT-resurs. Som incident räknas även upptäckt av otillåten användning och obehörigt intrång i IT-system samt upptäckt av misstänkt ”skadliga koder” (virus, trojaner med mera). Det kan även röra sig om till exempel att ett lösenord blivit känt för obehöriga, en dator blivit stulen, att en användare tryckt på en konstig länk eller öppnat en bilaga i ett mejl som ser konstig ut.

8.1 Allmänt

Om du misstänker att någon använt din användaridentitet eller att du varit utsatt för någon annan typ av incident ska du:

- notera när du senast var inne i IT-systemet,
- notera när du upptäckte incidenten,
- omedelbart anmäla förhållandet till din chef och Digitaliseringsavdelningen eller ServiceDesk, samt
- dokumentera alla iakttagelser i samband med upptäckten och försöka fastställa om riktigheten på din information har påverkats.

Katrineholms kommun rapporterar IT–incidenter av betydande omfattning till MSB.

8.2 Virus och skadlig kod

Katrineholms kommun har programvaror för viruskontroll både i klienterna och i nätverket, men kan ändå drabbas av effekter av så kallad skadlig kod. Om du misstänker att din dator innehåller virus ska du:

- dra ut nätverkskabeln och stänga av den trådlösa uppkopplingen men låta datorn vara på,
- omedelbart anmäla förhållandet till ServiceDesk, 569 00, (OBS! Anmälan ska ske per telefon eller besök, inte per e-post.), samt
- informera din närmsta chef om vad som inträffat.

Om du får e-mail med virusvarning gör inget annat än kontakta ServiceDesk, 569 00.

Surfplattor, digitala kameror, mobiltelefoner 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 virusprogram.

9. Avslut av anställning

När du slutar din anställning ansvarar du för att:

- Rådgöra med din chef om vilket av ditt arbetsmaterial som ska sparas. Notera att allt arbetsmaterial du framställt anses vara Katrineholms kommuns egendom och får inte tas med utan chefs godkännande.
- De behörigheter du fått för åtkomst till Katrineholms kommuns informations-system avbeställs av din chef.

10. Efterlevnad

Vid underlåtenhet att följa eller medvetet bryta mot Informationssäkerhetspolicyn, Informationssäkerhetsinstruktion Förvaltning och Informationssäkerhetsinstruktion Användare görs en utredning i samråd mellan chef och HR/Personalavdelningen. HR/Personalavdelningen kan ge Digitaliseringsavdelningen i uppdrag att ta fram loggar och annat underlag som behövs som stöd i en sådan utredning. Efter utredning kan rätten att använda it-resurser begränsas eller återkallas och arbetsrättsliga åtgärder som disciplinpåföljd bli aktuella.

Vid misstanke om oegentligheter har överordnade chefer rätt att, efter kontakt med HR/Personalavdelningen och en skriftlig begäran till Digitaliseringsavdelningen, få tillgång till medarbetaren informationstillgångar.

Vid misstanke om oegentligheter rörande en förtroendevald politiker har kommunstyrelsens ordförande efter kontakt med HR/Personalavdelningen samt kommunjuristen rätt att, efter en skriftlig begäran till Digitaliseringsavdelningen, få tillgång till den förtroendevaldes informationstillgångar.

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

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

11. Revidering

Digitaliseringschefen reviderar fortlöpande detta dokument. Giltighet av detta dokument följer Informationssäkerhetspolicyn.

Klassningsmatris

	Informationssäkerhetsaspekt			
Konsekvens	**Konfidentialitet** Röjande av informationen	**Riktighet** Förändring av informationen	**Tillgänglighet** Åtkomst till informationen	**Spårbarhet** Hur informationen har behandlats och av vem
Nivå 4 - Synnerligen allvarlig skada	Rikets säkerhet, hanteras ej i ordinarie verksamhetsystem.	Rikets säkerhet, hanteras ej i ordinarie verksamhetsystem.	Rikets säkerhet, hanteras ej i ordinarie verksamhetsystem.	Rikets säkerhet, hanteras ej i ordinarie verksamhetsystem.
Nivå 3 - Allvarlig skada	**Röjande av information medför allvarlig skada.** Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Känsliga personuppgifter kan ges stor spridning och orsaka allvarlig skada på den personliga integriteten.	**Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför allvarlig skada.** Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Känsliga personuppgifter kan ges stor spridning och orsaka allvarlig skada på den personliga integriteten.	**Ett avbrott medför allvarlig skada.** Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Känsliga personuppgifter kan ges stor spridning och orsaka allvarlig skada på den personliga integriteten.	**Att spårbarheten saknas medför allvarlig skada.** Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras.
Nivå 2 - Betydande skada	**Röjande av informationen medför betydande skada.** Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. Personuppgifter kan spridas och orsaka betydande skada på den personliga integriteten.	**Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför betydande skada.** Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. Personuppgifter kan spridas och orsaka betydande skada på den personliga integriteten.	**Ett avbrott medför betydande skada.** Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. Personuppgifter kan spridas och orsaka betydande skada på den personliga integriteten.	**Att spårbarhet saknas medför betydande skada.** Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder) Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan av störningen.
Nivå 1 - Måttlig skada	**Röjande av informationen medför måttlig skada.** Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten.	**Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför måttlig skada.** Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten.	**Ett avbrott medför måttlig skada.** Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten.	**Att spårbarhet saknas medför måttlig skada.** Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annans verksamhet. Externa individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan
Nivå 0 - Ingen eller försummbar skada	Information som ej behöver klassas	Information som ej behöver klassas	Information som ej behöver klassas	Information som ej behöver klassas

Katrineholm

Informationssäkerhetsinstruktion

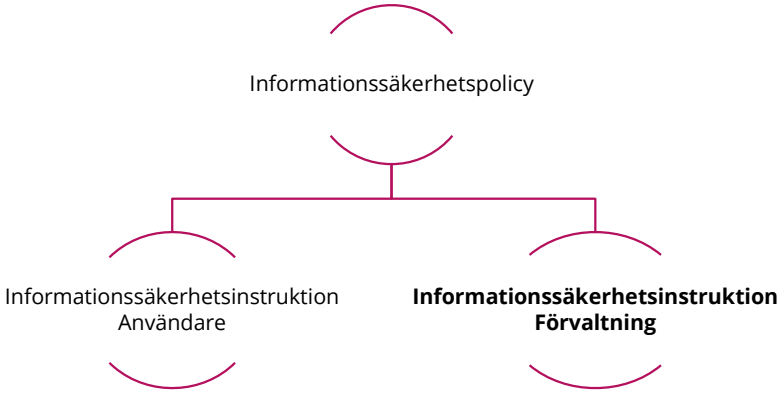
Förvaltning

Katrineholms kommun

Innehåll

1. Instruktionens roll i informationssäkerhetsarbetet

Styrande dokument för informationssäkerhetsarbetet är Katrineholms kommuns informationssäkerhetspolicy och informationssäkerhetsinstruktionerna för användare och förvaltning.



Informationssäkerhetspolicyn redovisar Katrineholms kommuns viljeinriktning och mål för informationssäkerhetsarbetet och syftar till att klarlägga:

- organisation och roller för informationssäkerhetsarbetet, och
- krav på riktlinjer för områden av särskild betydelse.

Informationssäkerhetsinstruktion Användare redovisar hur en användare ska verka för att upprätthålla en god informationssäkerhet. Målgruppen för instruktionen är samtliga medarbetare vid kommunen samt andra parter som får tillgång till kommunens IT-system.

Informationssäkerhetsinstruktion Förvaltning redovisar:

- det ansvar som ingår i de olika rollerna,
- hur informationssäkerhetsarbetet ska bedrivas,
- de riktlinjer som gäller för områden av särskild betydelse, samt
- regler för systemutveckling, systemunderhåll och incidenthantering.

Målgruppen för instruktionen är kommunens ledning, förvaltningsledning, systemägare, systemförvaltare och eventuell samordningsansvarig.

Information gällande organisation och ansvar för drift av informationssystemen, samt regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering framgår i avtal rörande IT-drift.

1.1 Definitioner

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

Med ***IT-resurser*** avses exempelvis (men är inte begränsat till) datorer, mobiler, nätverk, programvara, lagringsmedia samt applikationer som är till för att stödja medarbetaren i det dagliga arbetet.

2. Organisation och ansvar

2.1 Kommunstyrelsen

Kommunstyrelsen fattar de avgörande besluten hur informationssäkerhetsarbetet ska bedrivas. Ansvarets omfattning i övrigt framgår av informationssäkerhetspolicyn.

2.2 Nämnderna

Nämnderna har det yttersta ansvaret inom respektive verksamhetsområde. Det innebär ansvar för att styrdokumentet beaktas i beslutsprocessen samt för att efterfråga och ta del av uppföljning.

2.3 Digitaliseringschef

Digitaliseringschefen 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, samt i enlighet med Katrineholms kommuns delegationsordning.

Digitaliseringschefen ansvarar för att incidentrapportering sker till Myndigheten för samhällsskydd och beredskap vid IT-incidenter av betydande omfattning.

Digitaliseringschefen är systemägare för kommungemensamma system.

Digitaliseringschefen ansvarar också för att informationssäkerhetsinstruktion Användare och Informationssäkerhetsinstruktion Förvaltning upprättas och underhålls.

2.4 Informationssäkerhetsansvarig

Informationssäkerhetsansvarig stödjer arbetet med att uppnå informations-säkerhetspolicyns mål och ansvarar för analyser av de delar av IT-stödet som är gemensamma för hela verksamheten. Informationssäkerhetsansvarig initierar och stödjer systemägarnas arbete med att genomföra enskilda systemsäkerhetsanalyser.

2.5 Systemägare

Varje nämnd utser systemägare för informationssystem inom nämndens ansvarsområde.

Inom ramen för antagna mål och resurser fattar systemägaren beslut om de egna informationssystemens införande, drift, förvaltning och avveckling.

Systemägaren har det yttersta ansvaret för systemet och ansvarar bland annat för att:

- säkerhetsanalyser för de egna informationssystemen genomförs,
- utse systemförvaltaren, samt för att ge systemförvaltaren stöd i dennes roll som utförare av vissa moment inom systemdriften,
- att lagar och förordningar följs,
- informationen i systemet är i enlighet med informationssäkerhetspolicyn,
- att det finns överenskommelse om servicenivå med Digitaliseringsavdelningen för reglering av driftansvaret,
- att information och utbildning ges till berörd personal,

- att systemet utvecklas i linje med kommunens informationssäkerhetspolicy,
- att hålla kontakt och utbyta information med Digitaliseringsavdelningen,
- att godkänna nya versioner av systemet,
- att licenser finns i erforderlig mängd och att en överlämning sker av licenserna och programvara till Digitaliseringsavdelningen vid installation, samt
- att fastställa felhanteringsrutinen för varje system.
- Utsedd systemägare ansvarar även för ovanstående när systemet nyttjas av andra verksamheter och förvaltningar.

2.6 Systemförvaltare

Systemförvaltaren utses av systemägaren och ansvarar, i samverkan med Digitaliseringsavdelningen, för den dagliga driften och förvaltningen av aktuellt informationssystem. Systemförvaltarens roll är bland annat att:

- verkställa beslut som systemägaren fattar,
- informera sig om och bli väl förtrogen med programmets innehåll och struktur,
- upprätta, införa och utvärdera systemförvaltningsrutiner,
- 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 ska hanteras av systemägaren,
- rapportera fel, brister, regelbrott och oegentligheter till systemägaren och informationssäkerhetsansvarig,
- hantera felanmälningar från kommunens gemensamma ServiceDesk och åtgärda eller vidarebefordra problemet till leverantören,
- ge förslag till ändringar/utveckling av systemet,
- ansvara för arbetet med säkerhetsfrågor som berör systemet,
- ansvara för planering av datum för produktionssättning inför nya releaser/versioner i samråd med Digitaliseringsavdelningen,
- ansvara för att samtliga användare är informerade om planerade driftavbrott,
- ansvara för tester vid uppdateringar och felrättningar,
- ansvara för att kontroll och uppföljning av överenskomna servicenivåer efterlevs,
- se till att reservrutiner, serviceavtal med mera finns så att systemägarens krav på längsta 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, samt
- se till att kommunens systemförteckning är uppdaterad med relevant information.
- Utsedd systemförvaltare ansvarar även för ovanstående när systemet nyttjas av andra verksamheter och förvaltningar.

3. Regler och rutiner

3.1 Klassificering av information

Verksamheter har ansvaret för sin informationssäkerhet och har bäst kunskap om hur känslig och kritisk deras informationsmängder är, och därmed informationens skyddsvärde. Det innebär att verksamheterna utifrån informationens skyddsvärde ställer krav på de aktörer som hanterar informationen, exempelvis användare, systemansvariga samt drifts- och systemleverantörer.

För detta ändamål ska informationsklassning tillämpas, där information klassas med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Därigenom kan en anpassad och effektiv informationssäkerhet skapas.

Katrineholms kommun ska klassa informationen utifrån vedertagna klassificeringsmetoder såsom SKR:s Klassa och Sydarkiveras tillämpning av Klassa.

Matris för klassning av information finns bifogad till denna instruktion.

Följande 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 konfidentialitet, riktighet, tillgänglighet och spårbarhet.

3.2 Ansvar för IT-utrustning

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

Anskaffning av IT-utrustning, görs i samråd med Digitaliseringsavdelningen.

3.3 Flytt av IT och kommunikationsutrustning

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

3.4 Utbildning

Information och utbildning av anställda ska omfatta:

- Informationssäkerhetens betydelse för verksamheten
- Innehållet i Informationssäkerhetspolicyn
- Innehållet i Informationssäkerhetsinstruktion Användare

Nya användare ska ges grundläggande informationssäkerhetsutbildning före tilldelning av behörighet i nätverket. Sådan grundläggande informationssäkerhetsutbildning ska vara i nivå med DISA från Myndigheten för samhällsskydd och beredskap.

Systemägare ansvarar för att:

- användarhandledning för aktuellt system finns,
- medarbetare har tillräckliga kunskaper om säkerhetsreglerna för de informationssystem de behöver för de egna arbetsuppgifterna.

3.5 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. Känslig information som inte hanteras i informationssystem ska förvaras i brandklassade säkerhetsskåp. Övervakning av servicepersonal, städpersonal med flera ska ske och beslut ska tas av Digitaliseringschefen om och när tillträde till säkrade utrymmen tillåts.

3.6 Kontroll av utomstående tjänsteleverantör

Beställare av utomstående leverantörers tjänster ska följa upp och granska att säkerhetsöverenskommelser följs.

3.7 Hantering av datamedia

Om media som innehåller information som klassats som ”mycket hög nivå” måste transporteras fysiskt, ska Digitaliseringschefen eller informationssäkerhetsansvarig kontaktas för beslut om tillvägagångssätt.

Datamedia med sekretessbelagd information som ska avvecklas ska överlämnas till Digitaliseringsavdelningen som hanterar avvecklingen.

3.8 Övervakning

För informationssystems loggar ska systemägaren besluta:

- vad som ska loggas,
- hur ofta de ska analyseras,
- vem som ansvarar för analyser av dem,
- hur länge de ska sparas, samt
- hur de ska förvaras.

Detaljerad information samt anvisningar för användning och övervakning av loggfiler framgår av separat dokument.

3.9 Styrning av användares åtkomst

För att säkerställa att endast behöriga användare förekommer i informationssystemen ska beställning och borttagande av åtkomst till informationssystem ske via digitalt system (Beställningsportalen (IT)). Leverantörslösenord och behörigheter ska förvaras inlåsta.

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

3.10 Styrning av åtkomst till nätverk

Digitaliseringschefen ansvarar för att i anvisningar reglera:

- autentisering vid externa anslutningar,
- anslutning av utrustning till interna och externa nätverk,
- anslutning av externa nätverk till myndighetens eget nät med ingående säkerhetsfunktioner, autentisering etcetera,
- anslutning av trådlösa nät, och
- säkerhet vid internetanslutning.

Digitaliseringschefen ska ansvara 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, och
- att upprätta underlag för ledningens beslut om kommunikationstjänster.

3.11 Styrning av åtkomst till operativsystem

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

3.12 Mobil datoranvändning och distansarbete

Verksamhetsansvarig chef beslutar om ett informationssystems information ska få hanteras på distans med stationär eller mobil utrustning.

3.13 Säkerhetskrav på informationssystem

Inför nyanskaffning och införande av ett informationssystem ska verksamhetsansvarig chef i samråd med Digitaliseringsavdelningen utforma en projektplan för införandet. Denna plan ska minst omfatta:

- verksamhetens beskrivning av behov och mål med anskaffningen,
- en inledande systemsäkerhetsanalys. Analysen syftar till att klarlägga säkerhetskraven på det system som planeras införas och den utökas därefter med en kravspecifikation som minst omfattar:
    - integrationskrav med andra system,
    - krav på test,
    - tidplan,
    - personella och ekonomiska resurser, och
    - 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 och upprättar en systemsäkerhetsanalys.

Driftgodkännande avser den process som syftar till att fastställa om ett informationssystem uppfyller ställda säkerhetskrav. Denna process omfattar följande steg:

- systemägaren koordinerar sina krav med informationssäkerhetsansvarig och Digitaliseringsavdelningen,
- systemägare driftsgodkänner sina informationssystem efter genomförd informationssäkerhetsanalys,
- informationssäkerhetsansvarig ansvarar för att vid behov presentera underlag för beslut av ledningen om införande av informationssystemet i Katrineholms kommun.

3.14 Kontroll och revision av programlicenser

Digitaliseringsavdelningen ansvarar för de kommungemensamma licenserna såsom Microsoft Office 365, Adobes programvaror med flera. 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 förvaltningssystem. Villkoren för slutanvändning av licenserna ska uppfyllas. Vid en programvarurevision ska förvaltningen kunna visa upp aktuell dokumentation på antalet licenser och installationer. Digitaliseringsavdelningen kan vid behov göra stickprovskontroll.

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

3.15 Säkerhet i utvecklings- och underhållsprocesser

Förslag om önskemål på förändringar i systemet lämnas till verksamhetsansvarige för vidare befordran till systemägaren och Digitaliseringsavdelningen.

3.16 Externa utövare

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

3.17 Hantering av informationssäkerhetsincidenter

Vid misstanke om intrång eller andra incidenter ska användare agera enligt Informationssäkerhetsinstruktion Användare.

Informationssäkerhetsansvarig ska sammanställa och rapportera till ledningen gällande:

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

Digitaliseringschefen ansvarar för att IT-incidenter rapporteras till Myndigheten för samhällsskydd och beredskap. Exempel på incidenter:

- Kritiska funktioner är otillgängliga, till exempel återskapande av information.
- Integritetsbrister som leder till felaktiga beslut, till exempel att det inte går att säkerställa att rätt person blivit validerad eller fått ett certifikat utfärdat till sig.
- Oavsiktligt eller otillåtet avslöjande av personuppgifter.

3.18 Efterlevnad av rättsliga krav

Anvisningar i form av lagkrav för skydd av register och handlingar ska följas.

3.19 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 övrigt sorteras med tanke på vårt ansvar för miljön. IT-utrustning ska dock alltid lämnas ServiceDesk då ServiceDesk ska avgöra om vilken destruktionsmetod som ska användas för den aktuella utrustningen.

4. Revidering

Digitaliseringschefen reviderar fortlöpande detta dokument. Giltighet av detta dokument följer Informationssäkerhetspolicyn.

Klassningsmatris

	Informationssäkerhetsaspekt			
Konsekvens	**Konfidentialitet** Röjande av informationen	**Riktighet** Förändring av informationen	**Tillgänglighet** Åtkomst till informationen	**Spårbarhet** Hur informationen har behandlats och av vem
Nivå 4 - Synnerligen allvarlig skada	Rikets säkerhet, hanteras ej i ordinarie verksamhetsystem.	Rikets säkerhet, hanteras ej i ordinarie verksamhetsystem.	Rikets säkerhet, hanteras ej i ordinarie verksamhetsystem.	Rikets säkerhet, hanteras ej i ordinarie verksamhetsystem.
Nivå 3 - Allvarlig skada	**Röjande av information medför allvarlig skada.** Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Känsliga personuppgifter kan ges stor spridning och orsaka allvarlig skada på den personliga integriteten.	**Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför allvarlig skada.** Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Känsliga personuppgifter kan ges stor spridning och orsaka allvarlig skada på den personliga integriteten.	**Ett avbrott medför allvarlig skada.** Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Känsliga personuppgifter kan ges stor spridning och orsaka allvarlig skada på den personliga integriteten.	**Att spårbarheten saknas medför allvarlig skada.** Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras.
Nivå 2 - Betydande skada	**Röjande av informationen medför betydande skada.** Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. Personuppgifter kan spridas och orsaka betydande skada på den personliga integriteten.	**Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför betydande skada.** Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. Personuppgifter kan spridas och orsaka betydande skada på den personliga integriteten.	**Ett avbrott medför betydande skada.** Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan, av störningen. Personuppgifter kan spridas och orsaka betydande skada på den personliga integriteten.	**Att spårbarhet saknas medför betydande skada.** Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder) Samhällsviktiga funktioner i egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom stora besvär eller stor ekonomisk påverkan av störningen.
Nivå 1 - Måttlig skada	**Röjande av informationen medför måttlig skada.** Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten.	**Information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats medför måttlig skada.** Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten.	**Ett avbrott medför måttlig skada.** Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Enskilda individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan. Enstaka personuppgifter av ej känslig karaktär kan komma att spridas och orsaka måttlig skada på den personliga integriteten.	**Att spårbarhet saknas medför måttlig skada.** Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annans verksamhet. Externa individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan
Nivå 0 - Ingen eller försummbar skada	Information som ej behöver klassas	Information som ej behöver klassas	Information som ej behöver klassas	Information som ej behöver klassas