Hjo kommun

Verksamhetsskydd Hjo kommun

Informationssäkerhetsinstruktion - användare

1. Dokumenttyp

Instruktion

2. Fastställande/upprättad

2016-02-27 av IT-chef

3. Senast reviderad

2017-05-23

4. Detta dokument gäller för

Kommunövergripande

5. Giltighetstid

Tillsvidare

6. Dokumentansvarig

IT-chef

7. Dnr

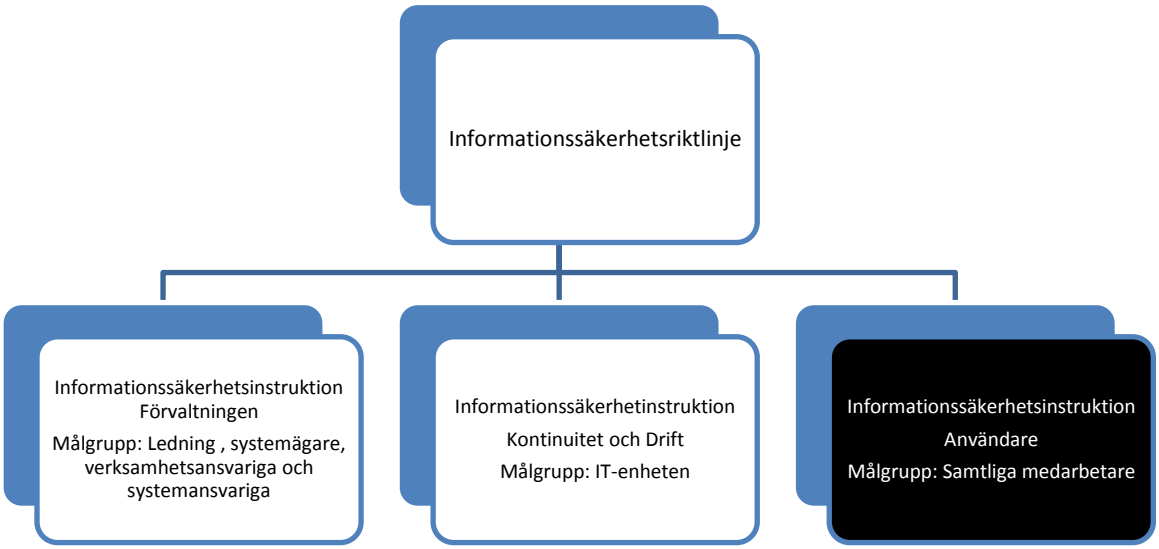
Klicka här för att ange text.

Hjo kommuns IT-enhet

Peter Jonsson IT-chef 0734-607 818 peter.jonsson@hjo.se

Instruktionens roll i informationssäkerhetsarbetet

Styrande dokument för informationssäkerhetsarbetet är Hjo kommuns informationssäkerhets-riktlinje och informationssäkerhetsinstruktionerna Förvaltning, Kontinuitet och Drift samt Användare:



Informationssäkerhetsinstruktion Användare redovisar hur en användare ska verka för att upprätthålla en god säkerhet.

Informationssäkerhetsriktlinjen redovisar ledningens viljeinriktning och mål för informationssäkerhetsarbetet och syftar till att klarlägga:

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

Informationssäkerhetsinstruktion Förvaltning redovisar:

- det ansvar som ingår i de olika rollerna
- de riktlinjer som gäller för områden av särskild betydelse
- regler för systemutveckling, systemunderhåll, incidenthantering

Informationssäkerhetsinstruktion Kontinuitet och drift redovisar:

- organisation och ansvar för drift av informationssystemen
- regler för säkerhetskopiering, lagring, driftadministration och kontinuitetsplanering

Bakgrund

För att du som användare ska kunna efterleva de säkerhetskrav som ställs på dig, är du skyldig att känna till:

- Vilka regler som gäller och vilket ansvar du har
- Vad du skall göra vid olika incidenter
- Var du kan få stöd och hjälp

Vid oklarheter ring 5444 eller e-posta IT-enheten (itenheten@hjo.se). Observera att vissa verksamhetssystem hanterar särskilt känsliga uppgifter och därför kan ha ytterligare säkerhetsföreskrifter och behörighetsansökningsprocesser. Kontrollera därför med systemägaren eller systemansvarig om det finns kompletterande säkerhetsinstruktioner för de system som du ska arbeta i.

Inloggning

Våra nätverk är utrustade med ett behörighetskontrollsystem. Behörighetskontrollsystemet säkerställer att det endast är behöriga användare som kommer åt informationen.

För att bli behörig användare krävs att din närmaste chef gör en behörighetsregistrering d.v.s. fyller i och skickar in blanketten ”Ansökan och beviljande av behörighet” till IT-enheten. En korrekt ifylld blankett ger dig som användare tillgång till t.ex. nätverket, e-post, kontorsprogram och Internet.

Därefter ansvarar du för att följa regler som kopplas till behörigheten. Hanteringen från ansökan till praktisk tilldelning ska ske skyndsamt, användaren ska få sina uppgifter. Synkningen av användaruppgifter sker via kommunens FIM (metakatalog), AD, personalsystemet (Personec P) och Skatteverkets databas (Navet). Synkningen renderar i ett användarnamn och lösen baserat på det namn som användaren har registrerat hos Skatteverket.

För att få behörighet krävs att:

- Din närmaste chef gör en behörighetsregistrering d.v.s. fyller i och skickar in blanketten ”Ansökan och beviljande av behörighet”
- Blanketten sänds till IT-enheten som lägger in din behörighet alternativt kontrollerar den automatiserade metakatalogssynkningen
- IT-enhet förser dig med en användaridentitet och ett (initialt) lösenord

Lösenordshantering – Det initiala lösenordet ska bara användas en gång d.v.s. första gången du loggar in i nätverket därefter ska du byta det mot ett personligt lösenord. Ett lösenord måste bestå av minst 8 tecken, bokstäver och siffror ska kombineras. Om du glömmer ditt lösenord kontakta IT-enheten så få du ett nytt initialt lösenord. Inloggningsförsök med felaktigt lösenord (6 ggr) låser systemet, kontakta IT-enheten och du får ett nytt initialt lösenord. Lösenordet ska bytas var 90:e dag.

KOM IHÅG! Lösenordet är strängt personligt. Lämna inte ut lösenordet till någon. Lämna inga nedskrivna lösenord under tangentbordet eller på bildskärmen.

Spårbarhet – Du lämnar spår efter dig när du är inloggad. Systemens inloggningsfunktion används bl.a. för att spåra intrång av obehöriga. Detta görs för att skydda informationen och för att undvika att oskyldiga misstänks och oegentligheter inträffar.

Om du byter arbetsuppgifter eller avslutar din anställning skall din chef meddela detta till IT-enheten så att din behörighet kan ändras eller tas bort.

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

Informationsklassning – Klassning av verksamhetssystem

I kommunen finns information av en mängd olika slag, information som ska hanteras utifrån riktlinjer rörande konfidentialitet, riktighet, tillgänglighet och spårbarhet. Beroende på hur informationen klassas utifrån ovanstående riktlinjer så bedöms dess skyddsvärde. Hjo kommun har valt att använda SKLs informationsklassningsverktyg KLASSA (klassa.se). Skyddsvärdet ger instruktioner för hur informationen i verksamhetssystemet ska hanteras från inlogg, distansarbete etc.. Klassningen utförs av utsedd systemansvarig, säkerhetssamordnare, IT-chef och IT-tekniker. Varje verksamhetssystem har klassats enligt ovan.

Lagring – lokal eller central

Information (filer, dokument etc.) kan lagras flera sätt. Hjo kommun erbjuder tre lagringsutrymmen tre varianter, ett gemensamt centralt lagringsutrymme (T:), ett användare styrt lagringsutrymme (documents:) samt ett lokalt lagringsutrymme på den egna datorn (C:). Därutöver kan diverse molntjänster nyttjas men där garanterar IT-enheten vare sig informationens beständighet, skydd eller service/support.

Vart informationen ska lagras måste användaren själv avgöra men med hänsyn tagen till dess skyddsvärde. Hur avgör man då skyddsvärdet? Frågor som användaren ska ställa sig kan vara, vad händer om informationen kommer i orätta händer, vad händer om informationen försvinner, när och var behöver jag ha åtkomst till den, vem äger informationen, innehåller informationen känsliga personuppgifter etc.. För att underlätta för användaren kan nedan guide med fördel användas.

Tänk på att nätverkets servrar är omgärdade med stränga säkerhetsregler och informationen säkerhetskopieras varje dygn (T: och documents:). Information som lagras på den egna hårddisken (C:) så är du själv ansvarig för informationssäkerheten och att den blir säkerhetskopierad. IT-enheten hjälper inte till med att återskapa information på exv. lokala hårddiskar eller USB minnen.

Förtydligande lagring

Den information du lagrar på våra gemensamma utrymmen säkerhetskopieras automatiskt.

Du kan välja att lagra på enheterna C:, documents: eller T:.

C: (lokal lagring) lagring på din PC hårddisk. Information som lagras här säkerhetskopieras inte, det är användarens eget ansvar att så sker.

documents: (Personlig hemkatalog) är din personliga enhet som du kan använda för lagring av arbetsmaterial. Om du väljer documents-enheten kommer dina medarbetare ej åt informationen. Tänk på vad du lagrar på documents:, bilder, filmer och ljudfiler tar mycket plats. Privat lagring är inte tillåten.

T: (Organisationsenhet) är en enhet för lagring av information som alla medarbetare i organisationen har tillgång till. Hör med IT-enheten om behörighet till olika mappar.

Internet

Kommunens nätverk är anslutet till Internet via en brandvägg som reglerar in- och utgående trafik. I brandväggen registreras även vilka sidor som användarna besöker. Tänk på att du representerar kommunen när du surfar via kommunens nätverk. Agera i enlighet med våra värderingar och policy.

Internetanvändandet är ett område där säkerheten i mycket hög grad påverkas av användarnas beteende. Vid Internet användande gäller därför följande regler:

- Besök endast sådana sidor som är relevant för ditt arbete
- Ladda inte ner program. På vissa hemsidor kan du bli uppmanad att ladda ner ett program. Acceptera inte detta. Dessa kan innehålla spionprogram.

Saknar du ett program som du behöver i ditt arbete kontakta IT-enheten. IT-enheten installerar programmet åt dig.

Riktlinjer för sociala medier såsom Facebook, Twitter och bloggar, finns att läsa på Eira.

Datavirus

Ett av de stora hoten mot vår information är datavirus, datavirus är ett program eller en programsekvens vars uppgift det är att kopiera sig själv och tränga in i andra program och utföra något otillbörligt. I värsta fall kan en sådan attack leda till att all information på datorns hårddisk raderas eller kopieringen orsakar en total systemkollaps. Smittkällan är svår att identifiera men oftast beror det på filer eller program som laddats ner från Internet. På senare tid har vi blivit angripna via e-posten. Användarna har fått ett mejl från någon offentlig myndighet eller service inrättning (Skatteverket, Posten, banken etc.) dock är det bara en front som utnyttjas av bedragare dvs de har ”lånat” det officiella utseendet. I mejlet uppmanas användaren att trycka på en interaktiv knapp för att utföra något. Vid knapptryckning laddas en mjukvara ner i datorn och vidare ut i nätverket, mjukvaran krypterar samtliga filer som den kommer åt innan den själv destruerar. Med andra ord var mycket kritiska till e-post, var observant på allt utöver det vanliga.

Tecken på datavirus kan vara:

- Datorn utför operationer som du själv inte initierat
- Datorn uppträder på ett onormalt sätt exv. arbetar långsammare än normalt
- Filer krypteras och blir oläsbara

Vid misstanke om datavirus

- Stäng av datorn och dra ur nätverkskabeln
- Anmäl omedelbart det som skett till IT-enheten

E-post

E-post är ett bra hjälpmedel i arbetet. Med tiden sparar man kanske på sig stora mängder meddelanden som ofta innehåller bifogade filer. Dessa tar en hel del plats på nätverkets servrar. Tänk därför på att regelbundet gallra och radera i din inkorg och utkorg. Vid gallring och diarieföring gäller samma regler som för vanliga brev. För att förhindra spridning av känslig information och för att minska risken för virusspridning samt för att undvika onödig belastning av nätverkets resurser gäller följande:

- Var återhållsam med att skicka eller vidarebefordra meddelanden som innehåller stora filer
- Var försiktig med att öppna e-post från avsändare du inte känner igen eller har en relation till
- Vidarebefordra inte meddelanden av typen insamlingar, kedjebrev etc. till andra användare i nätverket

Obehörig åtkomst

Om du misstänker att någon obehörig använt din användaridentitet och varit inne i systemet ska du:

- Notera tidpunkten då du senast själv var användare i systemet
- Notera tidpunkten du upptäckte förhållandet
- Anmäl omedelbart till IT-enheten och din chef
- Dokumentera alla iakttagelser i samband med upptäckten samt värdera informationen som kan ha påverkats

Bärbara datorer, mobiltelefoner och externa lagringsmedia

Bärbara datorer, mobiltelefoner och externa lagringsmedia utgör alltid en säkerhetsrisk, tänk därför alltid på att:

- Hålla utrustningen under uppsikt om den inte kan låsas in
- Lagra inte verksamhetskritisk information på datorn
- Använd alltid någon form av lösenordsskydd

Arbetsplatsen

Om du lämnar din arbetsplats skall du använda skärmsläckaren alternativt logga ut (CTRL-ALT-DELETE, Lock workstation). Görs inte detta finns det alltid en risk att känslig information blir åtkomlig för obehöriga. Du blir ansvarig för vad som händer när du är inloggad. Ur säkerhets-/ funktions-/ och miljömässiga hänsyn så ska datorn efter varje arbetsdags slut stängas av.

Hårdvara

Den utrustning som du förfogar över, d v s stationär, dockningsbar PC och/eller bärbar PC med tillhörande utrustning gäller:

- Fysiska ingrepp får endast utföras av IT-enheten
- Fel ska omgående anmälas till IT-enheten
- All installation och konfiguration får endast utföras av IT-enheten

Om din dator går sönder ska du kontakta IT-enheten, IT-enheten avgör hur felet ska avhjälpas.

Programvaror

- Programvaror ska godkännas och installeras av IT-enheten eller av IT-enheten anvisad/godkänd person
- Egna program kan, och får inte, installeras i myndighetens datorer
- Om du är i behov av ytterligare programvaror eller hårdvara ska du anmäla det till din chef

Incidenthantering

Alla incidenter ska omedelbart rapporteras till IT-enheten (itenheten@hjo.se eller 5444).

Vad är en incident? Till incidenter räknas de händelser då du som användare misstänker att något eller någon är i begrepp att komma över eller kommit över information, hårdvara och eller mjukvara som ägs/hanteras av kommunen. Det räcker alltså med misstanke om att något otillbörligt är på väg att hända eller har hänt.

Vid inrapportering så hamnar incidenten i det vanliga supportflödet men prioriteras direkt och förses med en handläggare. Handläggaren kontaktar omedelbart incidentanmälaren. Tänk på att ange namn och kontaktuppgifter när du anmäler incidenten.

Vad kan du som användare göra direkt när du upptäcker det inträffade (incidenten)?

- Stäng av datorn (hårdvaran), dra ur sladden (om applicerbart på incident)
- Anmäl omedelbart till IT-enheten och din chef
- Notera tidpunkten då du senast själv var användare i systemet
- Notera tidpunkten du upptäckte förhållandet
- Dokumentera alla iakttagelser i samband med upptäckten samt värdera informationen som kan ha påverkats

Mer information

Mer information finner du i:

- Informationssäkerhetsriktlinje Hjo kommun
- Informationssäkerhetsinstruktion – Förvaltning
- Informationssäkerhetsinstruktion – Kontinuitet och drift
- Säkerhetsreglerna som gäller för specifika verksamhetssystem

- Riktlinjer för sociala medier