Informationssäkerhetspolicy

antagen av kommunstyrelsen 2016-05-23, § 118

Gäller från 2016-06-01

Säkerhetsfunktionen har i samarbete med IT-enheten framtagit denna policy för att förbättra arbetet med informationssäkerhet.
Informationssäkerhet handlar om hur Svedala kommun förhåller sig till den information vi hanterar oavsett om den är digital eller analog. Information är en av Svedala kommuns viktigarste tillgångar. Oavsett form och kanal har den en avgörande roll för kommunens verksamheter varje dag, året runt.
Informationssäkerhet berör med andra ord alla, såväl anställda som förtroendevalda och skolelever.
Riktlinjerna i policyn anger hur verksamheterna ska agera för att initiera, bibehålla och förbättra informationssäkerheten. Riktlinjerna ska vidare ses som ett minimikrav vid utveckling eller anskaffning av nya system och e-tjänster.
Målet med riktlinjerna är att minska sannolikheten för, eller konsekvenserna av, uppkomna eller identifierade hot mot den information kommunen har en skyldighet att skydda, och därmed också verka för att bevara förtroendet för kommunens verksamhet.

Bild: pixabay.com

INFORMATIONSSÄKERHETS POLICY

SVEDALA KOMMUN

Säkerhetsenheten 2016-03-11

SVEDALA KOMMUN

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

Inledning

Information är en av Svedala kommuns viktigaste tillgångar. Oavsett form och kanal har den en avgörande roll för våra verksamheter - varje dag, året runt. Mängden information är stor och hoten mot den flera. Bränder, stölder, vattenläckage, bedrägerier och förfalskningar, men också okunskap, är bara några exempel.

En stor del av informationen hanteras i kommunens många IT-system och digitala tjänster. I SKL:s strategi för e-samhället framgår också att människor i allt högre grad förväntar sig att snabbt, enkelt och säkert kunna sköta sina ärenden, få tillgång till information och ha möjlighet till inflytande genom digitala kontaktvägar.

Detta sammantaget ställer krav på att informationen hanteras på ett tryggt och säkert sätt och att den är spårbar över tid där så behövs. Informationssäkerhet är ett samlingsbegrepp för detta arbete och handlar förenklat om Svedala kommuns förhållande till den information kommunen har att hantera. I många fall elektroniskt, men lika ofta utanför den digitala världen.

Informationssäkerhet berör med andra ord alla, såväl anställda som förtroendevalda och skolelever, mer eller mindre.

Målet med dessa riktlinjer är att minska sannolikheten för, eller konsekvenserna av, uppkomna eller identifierade hot mot den information kommunen har en skyldighet att skydda, och därmed också verka för att bevara förtroendet för kommunens verksamhet.

Utgångspunkten för Svedala kommuns informationssäkerhetsarbete är att så långt det är ekonomiskt och praktiskt möjligt följa den etablerade svenska och internationella standarden inom området, SS-ISO/IEC 27000. Detta stämmer också väl överens med Myndigheten för samhällsskydd och beredskaps (MSB) rekommendation om hur informationssäkerhetsarbetet bör bedrivas inom offentlig förvaltning.

Riktlinjerna anger hur verksamheterna ska agera för att initiera, bibehålla och förbättra informationssäkerheten i Svedala kommun. De ska vidare ses som ett minimikrav vid utveckling eller anskaffning av nya system och e-tjänster och målet för redan driftsatta sådana.

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

Innehåll

SVEDALA KOMMUN

Ks Dnr: 2016-109

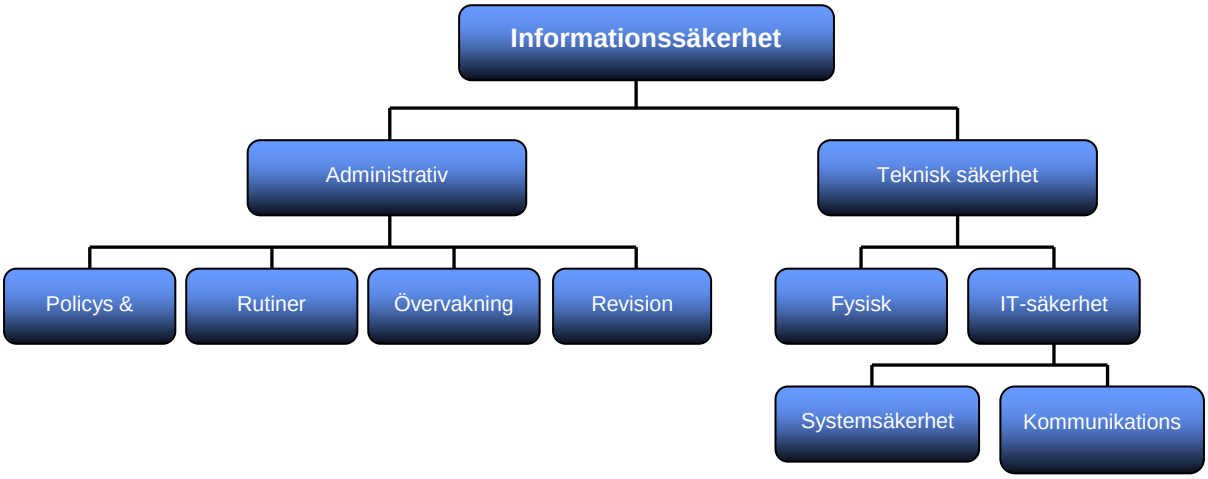
SKRIVELSE
2016-03-11

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

1. Omfattning



1.1 Vad är informationssäkerhet?

I inledningen framgick att Informationssäkerhet handlar om Svedala kommuns förhållande till den information vi hanterar oavsett om den är digital eller analog. Ett annat, lite enklare sätt att uttrycka det på är ***rätt information till rätt person i rätt tid och med hög rättssäkerhet.***

Ofta med stöd av IT men lika ofta på annat sätt.

Informationen kan alltså vara **talad, skriven** eller **tryckt** på papper, **elektronisk/digital** eller förpackad i **bild- film-** eller **ljudformat**.

I grunden går arbetet ut på att skydda och bevara den information Svedala kommun har ansvar för utifrån informationens krav på att vara:

- Tillgänglig för dem som behöver och har rätt att ta del av den (*Tillgänglighet*).
- Tillförlitlig och inte förvanskad (*Riktighet*).
- Skyddad från obehörig åtkomst (*Sekretess/Konfidentialitet*).
- Spårbar över tid (*Spårbarhet*).

Informationsklassning är ett grundläggande och återkommande begrepp inom området.

1.2 När gäller riktlinjerna?

Innehållet i dessa riktlinjer och anvisningar gäller exempelvis vid:

- Rekrytering av nya medarbetare eller extern inhyrd personal.
- Upphandling av varor, tjänster och produkter.
- Dimensionering av det fysiska skyddet vid uppförandet av nya verksamheter eller om- och tillbyggnader.
- Hantering av handlingar.
- System- och kommunikationssäkerhet (*inkl. e-tjänster*).
- Användning av internet och e-posthantering.
- Publicering av information på webben.
- Användning och avveckling av smarta telefoner och övrig IT-utrustning med lagringskapacitet.
- Incidenthantering.
- Kontinuitets- och avbrottsplanering.
- Upphörande av anställning och ingångna avtal.
- Bevarande och gallring.

Informationssäkerhet berör hela kommunens samlade verksamhet.

1.3 Vad är särskilt viktigt att jag tar del av?

Innehållet i riktlinjen kan uppfattas komplext och svårt att ta till sig och allt berör heller inte alla. Följande matris kan därför vara ett stöd vid val av studieområde. Använd därefter riktlinjen som ett uppslagsverk vid behov och frågeställningar.

Hänvisningarna under rubriken ”*Kommentar*” anger vilket eller vilka avsnitt inom det berörda kapitlet som bedömts som särskilt viktiga. Anges inget särskilt avsnitt avses kapitlet i sin helhet.

Avsnitt 11.6 och 12.6 avser uteslutande funktioner som administrerar digital infrastruktur.

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

Funktion	Särskilt viktiga kapitel i riktlinjen											
	1	2	3	4	5	6	7	8	9	10	11	12
Samtliga medarbetare			X	X			X	X	X		X	X
Förtroendevalda			X	X		X	X	X	X			X
Chefsfunktioner				X		X	X	X	X			
HR-funktioner						X	X		X			
Upphandlingsfunktioner						X		X				
Kommunikatörsfunktioner							X				X	
Arkivfunktioner							X	X				
Systemägare/förvaltare						X	X	X	X	X	X	X
IT-funktioner/IT-drift								X		X	X	X
Beredskapsfunktioner					X						X	
Säkerhetsfunktioner			X	X	X	X	X			X	X	

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

2 Säkerhetspolicy

Säkerhetspolicyn anger ledningens viljeinriktning med säkerhetsarbetet. Kommunstyrelsen har genom kommundirektören och säkerhetschefen det övergripande ansvaret för de interna säkerhetsfrågorna och fastställer också säkerhetspolicyn.

I policyn, som gäller för hela den kommunala verksamheten, och även i tillämpliga delar av de kommunala bolagen, framgår att uppdraget för att samordna, stödja, utbilda och följa upp kommunens arbete inom säkerhets- och riskhanteringsområdet utförs i huvudsak av säkerhetschefen. Säkerhetsarbetet i kommunen syftar till att:

1) Skapa och säkerställa en hög säkerhet mot skador och störningar i kommunens verksamheter.

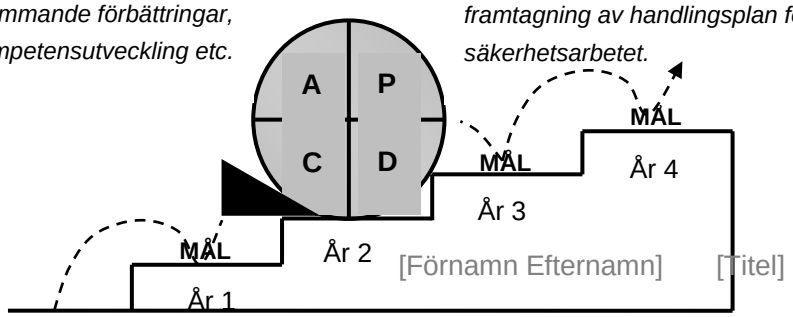
2) Bidra till att skapa en god riskekonomi, genom att optimera den sammanlagda kostnaden för skador och skydd.

3) Skapa en trygg miljö för kommunens anställda och de människor som berörs av kommunens verksamhet.

Informationssäkerhet är en del av organisationens **interna säkerhetsarbete** och faller inom ramen för en övergripande säkerhetspolicy. Riktlinjerna för informationssäkerhet anger hur verksamheterna ska agera för att initiera, bibehålla och förbättra informationssäkerheten i kommunen. Arbetet bör bedrivas enligt PDCA-modellen, på förvaltnings- som verksamhetsnivå och efter identifierade behov och prioriteringar.

Förbättra (*Act*)
Resultatet från uppföljningen lägger grunden för kommande förbättringar, kompetensutveckling etc.

Planering (*Plan*)
Identifiering av krav och mål samt framtagning av handlingsplan för säkerhetsarbetet.



Följa upp (*Check*)
Mätning och uppföljning av krav och uppsatta mål för säkerhetsarbetet.

Genomföra (*Do*)
Driva och genomföra det faktiska säkerhetsarbetet.

SVEDALA KOMMUN

2.1 Övriga styrdokument

Se 16 Referenser.

3 Riskbedömning och riskbehandling

En säkerhetsrisk är den sammanvägda bedömningen av sannolikheten för att en oönskad händelse ska inträffa och konsekvensen av det inträffade. Riskhantering är det samlade begreppet för att systematiskt bedöma, behandla och kommunicera risker.

Syftet med riskhanteringsarbetet är att verksamhetens mål ska kunna uppnås med ett minimum av störningar till lägsta möjliga kostnad. Målsättningen med det samlade säkerhetsarbetet är att upprätthålla de tjänster och funktioner samhället – eller vi själva - ställer på den kommunala förvaltningen. (*se även 15, Kontinuitets- och avbrottsplanering*)

SVEDALA KOMMUN

4 Organisation av säkerheten

4.1 Trygghet och säkerhet

Det ska finnas en funktion som ska lämna stöd till kommunstyrelsen inom verksamhetsområdet samt samordna och bereda alla trygghets- och säkerhetsrelaterade frågor som kommunstyrelsen har att behandla. Funktionen för ändamålet är rådet för trygghet och hälsa samt säkerhetschefen i kommunen.

4.2 Övergripande beskrivning av Svedala kommuns säkerhetsorganisation

Säkerhetschefen samordnar kommunens säkerhetsarbete tillsammans med ett nätverk av företrädare från Svedala kommuns olika förvaltningar. Säkerhetschefens uppgift är att stödja och initiera de ”lokala” processerna i verksamheterna (*genom utbildning, nätverksträffar m.m.*), fastställa nivå för säkerhetsarbetet och vara ett stöd för företrädarna i verksamheterna

Verksamhetsföreträdarna har till uppgift att samordna den egna förvaltningens interna skydd och säkerhetsarbete samt tillse att förvaltningen följer kommunens säkerhetspolicy.

4.3 Samordning av informationssäkerhetsarbetet

Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjerna för informationssäkerheten. IT chefen och säkerhetschefen som är placerad på kommunledningen samordnar kommunövergripande aktiviteter och verkar som rådgivare för kommunens förvaltningar.

4.4 Samordning av informationssäkerhetsarbetet vid förvaltningar

Informationssäkerhetsarbetet i förvaltningarna ska samordnas och följas upp av förvaltningen utsedd funktion. Funktionen ska ha kunskap om Svedala kommuns och den egna förvaltningens samlade säkerhets- och beredskapsarbete och informationssäkerhetsregler för att:

- Kunna bistå med kompetens vid informationsklassificering.
- Delta vid risk- och sårbarhetsanalyser.
- Sprida information och kunskap om kommunens informationssäkerhetsarbete inom förvaltningen.
- Vara kontaktperson mot IT chefen och säkerhetschefen.
- Tillse att nödvändiga instruktioner utformas och beslutas.
- Samordna och följa upp förvaltningens informationssäkerhetsarbete.

- Rapportera allvarliga incidenter till IT chef och säkerhetschef.

4.5 Säkerhet i Svedala kommuns digitala infrastruktur

Svedala kommuns digitala nät och grundläggande teknik- och tjänsteplattform tillhandahålls och förvaltas av Svedala kommuns interna IT-enhet. Uppdraget, som regleras i en överenskommelse mellan kommunledning(*beställaren*) och IT-enheten (*leverantören*), utgör en obligatorisk basnivå för samtliga enheter och användare som är anslutna till Svedala kommuns digitala nät och omfattar tjänsterna:

- Kommunikationsnät, WAN
- Lokala nät, LAN
- Identitet & åtkomst
- Systemintegration
- Klientplattform inkl. support
- E-post
- Telefoni

4.6 Ledningens ansvar

Informationssäkerhet är en del av Svedala kommuns kvalitets- och ledningssystem för att upprätthålla och bibehålla tjänster och förtroende. Förankringen och medvetandet hos medarbetare är grunden för att lyckas med detta arbete. Det är därför varje chefs ansvar att kommunicera vikten av god informationssäkerhet.

Ytterst ansvariga för informationssäkerheten är Svedala kommuns nämnder, genom att:

- Tillse att interna och externa krav på verksamhetens informationshantering följs genom intern kontroll.
- Avsätta resurser för att möta de hot som kan uppstå i den egna verksamheten.

Som system-/e-tjänstägare har nämnden även ett ekonomiskt, funktionellt och säkerhetsmässigt ansvar för sina informationssystem under hela dess livscykel.

4.7 Förbud att röja eller nyttja vissa uppgifter

Rutin ska finnas för att göra den som i sin yrkesroll får ta del av sekretessbelagd information uppmärksam på förbudet att röja eller nyttja uppgifter som faller inom ramen för offentlighets- och sekretesslagen (2009:400). Den anställde bör underteckna att informationen mottagits. Sekretessförpliktigande för praktikanter bör säkras genom ett s.k. förbehållsbeslut, vilket är ett delegationsbeslut som ska fattas av delegat.

SVEDALA KOMMUN

4.8 Utomstående parter

Avtal med utomstående parter ska reglera såväl den affärsmässiga som säkerhetsmässiga överenskommelsen, däribland behandling av personuppgifter.

Säkerhetskrav som kommer att ställas på den utomstående ska identifieras och redovisas. I avtal ska särskilt beaktas möjligheten för beställaren (*kommunen*) att genomföra säkerhetsrevision samt reglering av skadestånd vid förlust av information eller avbrott i tillgängligheten i det fall information som klassificerats som *Viktig, Mycket viktig* eller *Kritiskt* lagras/hanteras av utomstående. (*Se även 7.3 Skydd av personuppgifter samt 9.5 Internetanvändning*).

Extern leverantör för behandling/lagring av information som klassificerats som *Mycket viktig* eller *Kritisk* (*oavsett klassificeringsparameter*) ska, under avtalets hela längd, tillämpa den internationella standarden för informationssäkerhet SS-ISO/IEC 27000 genom att ha ett etablerat ledningssystem för informationssäkerhet som minst omfattar upprätthållandet av den avtalade tjänsten. Ledningssystemet ska granskas i samverkan med IT avdelningen innan avtal etableras, därefter löpande följas upp under avtalets hela livslängd.

5 Efterlevnad

5.1 Identifiering av tillämplig lagstiftning

En väl fungerande informationshantering är en förutsättning för att kommunen ska kunna fullgöra sina uppgifter. Det är därför viktigt att lagar och förordningar samt aktuella regelverk följs. Beaktande ska också tas till de allmänna råd och rekommendationer myndigheter med tolkningsföreträde tar fram.

5.2 Anvisningar för hantering av lagar och förordningar

Grundnivån för informationssäkerheten i Svedala kommun styrs bl.a. av lagar och förordningar. Följande lagar är exempel på lagar som berör de flesta verksamheter i kommunen.

- Tryckfrihetsförordningen (SFS 1949:105)
- Offentlighets- och sekretesslagen (SFS 2009:400)
- Personuppgiftslagen (SFS 1998:204)
- Bokföringslagen (SFS 1999:1078)
- Lagen om kommunal redovisning (SFS 1997:614)
- Upphovsrättslagen (SFS 1960:729)
- Förvaltningslagen (SFS 1986:223)
- Lagen om offentlig upphandling (SFS 2007:1091)
- Arkivlagen (SFS 1990:782)
- Säkerhetsskyddslagen (SFS 1996:627)
- Lagen om skydd för företagshemligheter (SFS 1990:409)
- Lagen om ansvar för elektroniska anslagstavlor (SFS 1998:112)

Med stöd av Arkivmyndighetens allmänna anvisningar om gallring ska det beslutas vilka handlingar som kan gallras. Se även Svedala kommuns arkivreglemente och dokumenthanteringsplaner.

5.3 Immaterialrätt

Programvaror ska användas i enlighet med avtal och licensregler.

SVEDALA KOMMUN

5.4 Skydd av personuppgifter

- Hantering av personuppgifter i strukturerad form (*register*) ska anmälas till personuppgiftsombud i Svedala kommun. Anmälan ska göras innan behandlingen sker och görs lämpligen i samband med klassificeringen av systemet/e-tjänsten.
- Data- och integritetsskyddet ska säkerställas enligt lagstiftningen och avtalsklausuler om sådana finns, t.ex. samtycke. Detta ska även regleras med utomstående parter och externa leverantörer, vid behov, genom personuppgiftsbiträdesavtal (*Se även 6.9 Utomstående parter*).

Rutin ska finnas för hur maskering av integritetskänsliga och sekretessmarkerade uppgifter ska ske.

5.4.1 Anvisningar för system som hanterar skyddade identiteter (*sekretessmarkerade personuppgifter*)

- Behandling av personuppgifter i IT-system ska följa Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter.
- Beställaren av systemet ansvarar för att systemet uppfyller kraven.
- Personer med sekretessmarkerade uppgifter ska informeras om vikten av att inte i onödan lämna ut uppgifter om sig själva.
- Sekretessmarkeringar ska markeras tydligt vid sökningar i register samt vid utskrifter. Den ska vara utformad på sådant sätt att markeringen kan följa med eventuella integrationer mot andra system och presenteras på samma sätt i de aktuella systemen.
- Personal som hanterar personuppgifter ska informeras om sekretessfrågor och om systemet med sekretessmarkerade personuppgifter.
- Kretsen av personer som har behörigheten att ta del av sekretessmarkerade personuppgifter ska begränsas så långt som möjligt.
- Sekretessmarkerade personuppgifter får inte spridas till områden där sekretess för uppgifterna inte finns.
- Lagrad sekretessmarkerad information ska vara krypterad.
- Åtkomst till sekretessmarkerade personuppgifter i system ska loggas för att i efterhand kunna kontrollera vilka som tagit del av uppgifterna.
- Rutin ska finnas för att regelbundet följa upp att sekretessmarkerade personuppgifter hanteras enligt ställda krav.

- Sekretessmarkerade/känsliga personuppgifter får endast lämnas ut via öppna nät (*internet*) till identifierade användare vars identitet är säkerställd med stark autentisering (*engångslösenord, e-legitimation eller motsvarande*)

5.5 Granskning av säkerhetspolicy, etik och teknisk efterlevnad

Uppföljning av internetanvändandet och användandet av Svedala kommuns IT-system i övrigt ska göras för att kontrollera att regler och etiska normer efterlevs. Uppföljning i övrigt kan ske på olika sätt beroende på typ av verksamhet.

5.5.1 Anvisningar för säkerhetsuppföljning

- Kontroll av enskilda personers surfning, e-post och lagrade filer kommer att ske då misstanke om brott eller missbruk föreligger.

- Kontroll av enskild användares lagrade filer på den lokala hårddisken och i nätverket kan ske genom stickprov eller på annat vis. Kontrollen avser i första hand musik-filmfiler, alltså inte vanliga office-dokument.

- Om det av kontrollerna framgår att riktlinjerna överträtts kan ärendet komma att utredas. Arbetsgivaren kommer i första hand att ge användaren tillfälle till förklaring och därefter, vid behov, rättelse genom tillsägelse eller liknande förfarande. Vid allvarligare missbruk kan disciplinära åtgärder komma att vidtas. Om det i utredningen framgår misstanke om brott kan en polisanmälan bli aktuell.

- Metodiken för att genomföra uppföljningar kan variera, men vanliga tillvägagångssätt är bland annat:

- Intern uppföljning med eller utan hjälp av IT-stöd.

- Internrevision (*s.k. auditing*).

- Traditionell uppföljning/revision med hjälp av externa konsulter.

- Attacksimulering/intrångsförsök av externa konsulter.

- Initiativtagare till säkerhetsuppföljningen kan vara kommunens revision, Svedala kommuns säkerhetschef eller IT-chef, verksamhetens funktion för samordning av det lokala informationssäkerhetsarbetet eller verksamhetsansvarig chef.

- Kontinuerlig säkerhetsuppföljning/revision ska genomföras.

5.6 Kontroll av teknisk efterlevnad

Den använda tekniken ska kontrolleras utifrån ett säkerhetsperspektiv. Exempelvis kan sårbarhetsanalyser och penetrationstester göras för att kontrollera IT-systemets åtkomst och kommunikationsskydd.

SVEDALA KOMMUN

5.7 Styrning av revision

Revisioner ska planeras, överenskommas och regelbundet genomföras för att minska risken för störningar i verksamheterna.

Riktlinjerna för informationssäkerhet ska granskas och revideras varje år för att se om betydande förändringar inträffat inom Svedala kommun, för att säkerställa att dessa fortfarande är relevanta och inte står i strid med lagstiftningen och att riktlinjerna följer den tekniska utvecklingen. Ansvarig för att detta utförs är säkerhetschefen och IT-chefen i Svedala kommun.

SVEDALA KOMMUN

6 HANTERING AV TILLGÅNGAR

6.1 Ansvar för tillgångar

Alla informationstillgångar, dyr eller svårersättlig utrustning ska ha en ansvarig. Den ansvarige ska utfärda instruktioner om hur informationen och utrustningen ska och får användas.

6.1.1 Anvisningar för förteckning och märkning av tillgångar

- Informationstillgångar representerar stora värden och ska därför förtecknas. Förteckningarna ska hållas noggrant uppdaterade.
- Utrustning, särskilt stöldbegärlig, ska vara märkt. Stöldskyddsmärkningen ska göras så att den inte går att ta bort utan svårigheter.

6.2 Klassificering av information

All information – oavsett dess form – är en tillgång för Svedala kommun och ska därför ges ett lämpligt skydd. Skyddsnivån bedöms av den som äger informationen och utifrån dess krav på Tillgänglighet, Riktighet, Sekretess/Konfidentialitet och Spårbarhet. Klassificering av informationstillgångar (framför allt informationssystem som IT-system och e-tjänster) är en förutsättning för att rätt skyddsnivå ska kunna fastställas för den information som hanteras i Svedala kommuns system. Därför ska alla informationssystem klassificeras. Klassificeringen ska ske tidigt (före) upphandling/anskaffning av systemet/e-tjänsten. Därefter vart annat år eller vid förändringar som exempelvis förändrad lagstiftning eller riskbild. Hantering av handlingar i pappers- och/eller elektronisk form, se 8.3 Märkning och hantering av handlingar.

6.2.1 Anvisningar för klassificering

- Alla informationssystem – oavsett intern eller extern drift - ska vara klassificerade för att säkerställa tillräckligt skydd för den information systemet är tänkt att behandla.
- Tillämpliga lagar och andra styrdokument ska alltid uppfyllas och vägas in i klassificeringen.
- Klassificeringen ska utformas så att tillgången till information och öppenhet inom Svedala kommuns verksamheter förblir så stor som möjligt för intressenter och allmänheten.

SVEDALA KOMMUN

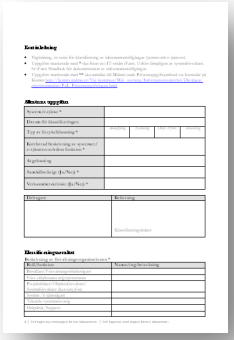
Ks Dnr: 2016-109

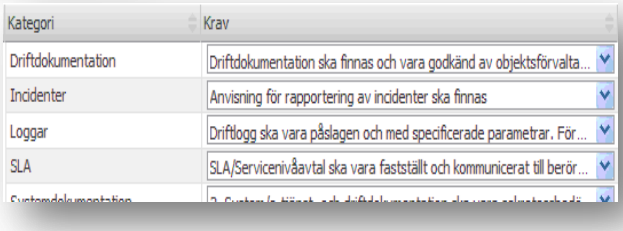
SKRIVELSE
2016-03-11

- Klassificeringen av informationssystem ska ske enligt fastställd rutin och resultatet föras in i det av Svedala kommun tillhandahållna IT-stödet för dokumentation av kommunens informationstillgångar. Vid klassificeringen ska för informationstillgången viktiga funktioner/roller delta, exempelvis informationsägaren eller informationsägarna om flera.

Rutin för klassificering

Klassificeringsprotokoll





Kravspec
Förfrågningsunderlag

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

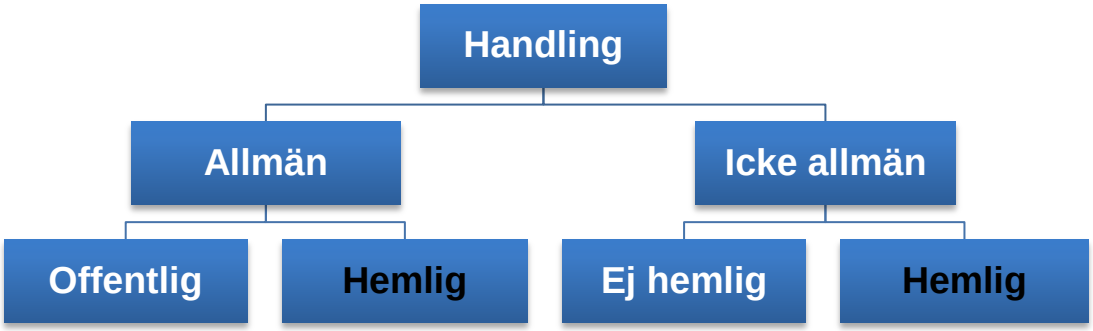
Klassificeringsmodell för bedömning av skydds- och kravnivå

Kravnivå	Sekretess/ Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
Kritisk	Information som kan medföra **katastrofal skada** för egen eller annan organisations verksamhet eller enskild person om den blir åtkomlig för obehörig	Information som kan medföra **katastrofal skada** för egen eller annan organisations verksamhet eller enskild person om den är felaktig	Information som ingår i eller stöder kontinuerlig och samhällsviktig verksamhet där avbrott innebär att man inte kan upprätthålla för samhället nödvändig tillgänglighet och servicenivå. Avbrott kan medföra **katastrofal skada** för egen eller annan organisations verksamhet eller enskild person	Information som kan medföra **katastrofal skada** för egen eller annan organisations verksamhet eller enskild person om spårbarhet saknas eller är bristfällig
Mycket viktig	Information som kan medföra **stor eller mycket stor skada** för egen eller annan organisations verksamhet eller enskild person om den blir åtkomlig för obehörig --- E-tjänst som kan bli föremål för sekretess enl OSL kap. 7, 15, 18, 19, 21, 23, 24, 25, 26, 28, 29, 32, 39, 40	Information som kan medföra **stor eller mycket stor skada** för egen eller annan organisations verksamhet eller enskild person om den är felaktig	Information som ingår i eller stöder kontinuerlig och för verksamheten kritisk verksamhet, där avbrott innebär att man inte kan upprätthålla nödvändig tillgänglighet och servicenivå. Avbrott kan medföra **stor eller mycket stor skada** för egen eller annan organisations verksamhet eller enskild person	Information som kan medföra **stor eller mycket stor skada** för egen eller annan organisations verksamhet eller enskild person om spårbarhet saknas eller är bristfällig
Viktig	Information som kan medföra **skada** för egen eller annan organisations verksamhet eller enskild person om den blir åtkomlig för obehörig --- E-tjänst som innehåller känsliga personuppgifter enligt PUL, kan bli föremål för OSL, (övr. kap.) ansökan, abonnemang	Information som kan medföra **skada** för egen eller annan organisations verksamhet eller enskild person om den är felaktig	Information som ingår i eller stöder kontinuerlig verksamhet där avbrott kan medföra **skada** för egen eller annan organisations verksamhet eller enskild person	Information som kan medföra **skada** för egen eller annan organisations verksamhet om spårbarhet saknas eller är bristfällig
Mindre viktig	Information som är öppen för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser. Spridning medför **ingen skada** för egen eller annan organisations verksamhet eller enskild person. --- E-tjänst som endast	Information som kan förändras utan risk för negativa konsekvenser. Oriktig information medför försumbar eller **ingen skada**	Information med lågt verksamhetsberoende. Kan vara otillgängligt en längre tid utan risk för negativa konsekvenser. Brist på åtkomst medför försumbar eller **ingen skada** för egen eller annan organisations verksamhet eller enskild person.	Information som saknar krav på spårbarhet. Bristen på eller avsaknaden av spårbarhet medför försumbar eller **ingen skada** för egen eller annan organisations verksamhet eller enskild person

	innehåller allmänna offentliga uppgifter. E-tjänst som innehåller icke känsliga personuppgifter som den enskilde kan anses ansvara för.			

6.3 Märkning och hantering av handlingar

Om det kan antas att information inte får lämnas ut på grund av sekretess ska detta markeras (sekretessmarkering) så att det tydligt framgår vilken lag och paragraf som är tillämplig. En sekretessprövning ska alltid utföras innan informationen lämnas ut.



Svedala kommuns informationshantering regleras främst av bestämmelserna i tryckfrihetsförordningen och Offentlighets- och sekretesslagen (OSL) 2009:400. Huvudregeln i tryckfrihetsförordningen är att informationen ska vara tillgänglig för allmänheten, den s.k. offentlighetsprincipen. Undantag från huvudregeln utgör information som med stöd av reglerna i OSL kan omfattas av sekretesskydd.

Varje anställd ska känna till vilken information, inom i första hand sitt eget ansvarsområde, som kan vara sekretessbelagd och hur den ska hanteras. Prövning av sekretess föreligger för viss information varje gång en begäran om utlämning sker. Detta oavsett om handlingen är sekretessmarkerad eller inte.

Anvisningar för hantering av allmänna hemliga handlingar

- Handlingar med typiskt sett sekretessbelagd information ska:

- Skyddas från obehörig åtkomst.

- Övervakas eller skyddas när den skrivs ut.

- Märkas med särskild anteckning (*sekretessmarkering*) på handlingen eller i det datasystem där den elektroniska handlingen hanteras. Anteckningen ska ange:

- tillämplig sekretessbestämmelse,

- datum då anteckningen gjordes, och den myndighet som har gjort anteckningen.
- Förvaras i säkerhetsskåp eller annan förvaringsenhet som uppfyller Svensk standard SS 3492, eller motsvarande.
- Vid intern distribution i pappersformat, placeras i ett förslutet och adresserat innerkuvert omgärdat av ett ytterkuvert.
- Vid extern distribution, om särskilt behov av åtkomstbegränsning föreligger, distribueras med rekommenderad försändelse eller bud, annars som vanligt post.

• Handlingar med typiskt sett sekretessbelagd information i elektronisk form ska:

- Distribueras med krypterad förbindelse eller med filerna krypterade. Med ”*Distribueras*” menas exempelvis e-post, skanning och fax.
- Lagras krypterade. Med ”*lagras*” menas lagring på intern/extern lagringsyta (*se även 11.7 Mediahantering och mediasäkerhet*)

• Handlingar med typiskt sett sekretessbelagd information i pappersform ska vid gallring förstöras i dokumentförstörare. Alternativt av Svedala kommun godkänd destruktör. I elektronisk form, se 11.8 Avveckling av media.

• Verksamhetsansvarig chef ska säkerställa att handlingar med typiskt sett sekretessbelagd information hanteras korrekt.

6.3.1 Anvisningar för hantering av allmänna offentliga handlingar

• En handling anses som allmän om den förvaras hos en myndighet och är antingen inkommen till, eller upprättad hos myndigheten.

• All post ska öppnas och bedömas om handlingen ska diarieföras.

• Postfack ska kontrolleras dagligen.

• Upprättade handlingar ska sekretessbedömas och registreras.

• Protokoll, beslut och styrdokument så som policys, riktlinjer, regler, anvisningar, rutiner, instruktioner, manualer och liknande dokument ska vara spårbara och därför daterade och försedda med tydlig avsändare (*ex. diarie, versionsnummer, förvaltning, datum etc*).

• E-post, fax, sms m.m. kan också vara inkommen handling. Mottagaren bedömer om meddelandet ska diarieföras. Avslutade ärende ska arkiveras enligt gällande bestämmelser.

• I de fall handlingen innehåller uppgifter för vilka det kan råda sekretess ska en sekretessprövning göras.

SVEDALA KOMMUN

6.3.2 Anvisningar för hantering av icke allmänna handlingar

- Utkast, koncept och andra icke-färdiga mellanprodukter är inte allmänna handlingar, om dessa inte expedierats (*skickats iväg*) eller tagits om hand för arkivering.
- När icke allmänna handlingar innehåller typiskt sett sekretessbelagda uppgifter ska dessa hanteras med samma försiktighet och med samma skydd som allmänna handlingar med liknande uppgifter.
- I samband med resor, konferenser och motsvarande ska känsligt arbetsmaterial hanteras på sådant sätt att de inte exponeras för obehöriga.

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

7 PERSONAL OCH SÄKERHET

7.1 Säkerhet vid rekrytering för anställd och inhyrd personal

Vid rekrytering ska säkerhetsbestämmelserna beaktas. Platssökande ska kontrolleras på lämpligt sätt, särskilt om anställningen medför åtkomst till sekretessbelagda uppgifter eller på annat sätt omfattar säkerhetskritiska aktiviteter. Behovet av kontrollmoment ska analyseras innan rekryteringsprocessen påbörjas (*förslagsvis i samband med framtagning av kravprofil*) och kontrollerna stå i proportion till den berörda tjänsten. Detta gäller även för inhyrd/tillfällig personal. (*Kontakta HR-enheten för ytterligare vägledning*)

Information om hur informationssäkerheten hanteras inom Svedala kommun ska lämnas till nyanställda.

7.2 Krav på anställda gällande informationssäkerhet

Genom säkerhetsinsatser ska riskerna minskas för mänskliga misstag, stöld, bedrägeri och missbruk av informationstillgångar.

7.2.1 Anvisningar för personal och säkerhet

- Alla anställda ska vara medvetna om sitt ansvar för informationssäkerheten.
- Vid nyanställning ska den anställde förbinda sig att ta del av och acceptera regelverket för informationssäkerhet, lämpligen som en del av introduktionen.
- Vid anställningens upphörande ska verksamhetschefen säkerställa att samtliga konto så som Apple/iTunes-konto, Dropbox och liknande molntjänstkonton som den anställde etablerat i tjänsten raderas, där Svedala kommun saknar avtal som reglerar informations-säkerheten, och där kontouppgifterna (*e-post, adressuppgifter etc*) hänvisar till Svedala kommun.(*se även 11.8 Avveckling av media*)
- Personal i viss verksamhet ska registerkontrolleras enligt gällande lagstiftning. För registerkontroll enligt säkerhetsskyddslagen SFS 1996:627 hänvisas till Svedala kommuns säkerhetschef.
- All personal ska ha kunskap om offentlighetsprincipen och om offentlighets- och sekretesslagen.
- Instruktioner som styr avveckling/förändring av åtkomst till såväl lokaler som IT-system ska finnas.
- För personal med höga behörigheter till lokaler och IT-system och där uppsägning från arbetsgivarens sida eller där övertalighet är aktuell ska behörigheterna för berörda personer omedelbart revideras.
- Beställare/uppdragsgivare ska upprätta sekretessförbindelse för konsulter/entreprenörer med uppdrag inom Svedala kommun, innan uppdraget startar.

- Vid tjänstledighet längre än 6 månader ska, om inte annat överenskommits, åtkomst-rättigheterna till system revideras. Föräldralediga är undantagna.

7.3 Regler för vissa system

Det är under vissa förutsättningar tillåtet för Svedala kommuns medarbetare att använda sin arbetsplatsutrustning även för privata angelägenheter.

7.3.1 Anvisningar för användning av Svedala kommuns IT-system.

- Användning ska ske inom de ramar som sätts upp av lagar och förordningar. Hantering av information och material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet är inte tillåtet.

- Den privata användningen får inte vara av sådan omfattning att den inkräktar på användarens arbete eller på Svedala kommuns IT-resurser i form av kostnader, lagringsutrymme, prestanda etc.

- Svedala kommuns utrustning får endast användas av den anställde.

- Fildelning, nedladdning och lagring av programvaror, bild- film och ljudfiler för privat bruk på Svedala kommuns servrar eller datorer är inte tillåtet.

- Nedladdning av appar för privat bruk på smarta telefoner och pekplattor får inte ske på enheter som används för att behandla information med klassificeringsparametern *Viktig, Mycket viktig* eller *Kritisk* för sekretess/konfidentialitet. Antalet appar är stort och det är mycket svårt för användaren att veta vilken information på enheten appen kräver att få tillgång till för att fungera.
(*se även 8.2 Klassificeringsmodell för bedömning av skydds- och kravnivå*)

- Användaren ska vara medveten om att:

    - Om en e-postadress lämnas till olika tjänster på internet, t.ex. nyhetsbrev, kan detta medföra att s.k. skräppost skickas tillbaka till e-postadressen.

    - Besök på internet lämnar elektroniska spår efter sig.

    - Nätverkstrafik och dess innehåll loggas och lagras.

- E-post som skickas till eller från Svedala kommuns e-postsystem eller som finns i kommunens IT-system, och där det inte är tydligt att meddelandet är av privat karaktär, kan, om meddelandet rör myndighetens verksamhetsområde, vara en allmän handling. Ibland kan ett meddelande vara delvis privat och delvis en allmän handling. I de fallen måste den delen av meddelandet som är en allmän handling tas omhand.

7.4 E-posthantering

7.4.1 Anvisningar för hantering av e-post

- Varje nämnd har ett ansvar för att de allmänna handlingar som skapas i verksamheten hanteras enligt regelverket. De har också ansvar för att alla anställda har kännedom om vilka regler som gäller.
- Extern e-post bör besvaras inom 48 timmar.
- Alla som använder e-post ska regelbundet kontrollera sin inkorg. Medarbetare som inte ger fullmakt genom att vidarebefordra sin e-post till en kollega, ansvarar själv för att kontrollera e-posten (*åtminstone en gång per dag*) även vid frånvaro såsom semester, sjukskrivning, föräldraledighet etc. Det räcker inte med ett automatiskt svarsmeddelande om frånvaron.
- E-post som är inkommen i tjänsten är allmän handling och ska diarieföras om det utgör del av ärende. Meddelande som inte utgör del av ett ärende kan istället postregistreras. Meddelanden som innehåller sekretess ska dock alltid diarieföras.
- Handlingar i ett ärende ska alltid kunna presenteras samlat. Ärenden kan bevaras samlat i akter på papper, elektroniskt och/eller som ljud/bildupptagningar. Handlingarnas fysiska förvaring framgår av Svedal kommuns dokumenthanteringsplan.
- De uppgifter som finns i loggar och andra förteckningar som generas av systemet är allmänna handlingar och kan därför bli tillgängliga.
- Meddelanden som uppenbart är av ringa betydelse för nämndens verksamhet ska så snart som möjligt gallras (*raderas)*
- Svedala kommun har en officiell e-postadress. Adressen ska publiceras externt, bl.a. på Svedala kommuns webbplats och e-posten öppnas av registrator (*eller motsvarande*) minst två gånger per dag varje helgfri måndag till fredag. Inkorgen ska vara tillgänglig för allmänheten t.ex. hos registratorn. Det kan i många fall vara lämpligt att enheter/avdelningar eller särskilda verksamheter har en egen adress/inkorg.
- Sekretessbelagd information ska sändas krypterad, både till externa och interna e-postadresser. Detta medför bl.a. att e-post inte får vidarebefordras utan kontroll av förekomsten av sekretess.
- Om e-postmeddelanden innehåller uppgifter om levande personer, ska personuppgifts-lagens (*1998:204*) bestämmelser beaktas.
- Automatisk extern vidarebefordring av verksamhetens e-post till e-postsystem utanför Svedala kommuns nät och utanför kommunens kontroll, exempelvis Hotmail och Gmail, är inte tillåtet.

- E-postsystemet får endast användas för privata meddelanden i begränsad omfattning. Information och material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet är inte tillåtet. Vidare får innehållet ej vara formulerat på sådant sätt att de som läser det får uppfattningen av att det är skickat på uppdrag av Svedala kommun. Den anställde uppmanas att i första hand använda eget privat e-postkonto.

- Störningar eller avvikelser i säkerheten eller om man fått e-post som strider mot lagar och förordningar ska direkt rapporteras till närmaste chef eller enligt formell beslutad rutin.

7.5 Internetanvändning

Internet är en av många informationskällor som används för att lösa arbetsuppgifter.

7.5.1 Anvisningar för åtkomst till och användning av internet

- Användning ska ske inom de ramar som sätts upp av lagar och förordningar. Hantering av information och material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet är inte tillåtet.

- Undantag från föregående punkt kan göras i de fall sådan information/hantering behövs för tjänstebruk, vilket skriftligen ska godkännas av närmaste chef.

- Material som är sekretessbelagt får inte publiceras på internet. Sekretessbedömning ska utföras innan information publiceras.

- Lagring av information (*data och filer*) som Svedala kommun äger får endast ske på lagringsytor utanför Svedala kommuns kontroll om:

  - Informationen klassificerats som *Mindre viktig*, dvs. att den är öppen för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser och där spridning inte medför någon skada för egen eller annan organisation eller enskild person. (*se matrisen 8.2 Klassificering av information*)

  - Informationen också finns tillgänglig på Svedala kommuns nätverk.

Information som lagras på lagringsytor utanför Svedala kommuns kontroll kan utgöra allmänna handlingar och reglerna för t.ex. diarieföring och gallring ska beaktas även för denna information.

Med ”*utanför Svedala kommuns kontroll*” avses exempelvis alla s.k. molntjänster som iCloud, Evernote, Dropbox, Hotmail, Gmail etc, där avtal som reglerar informationssäkerheten saknas mellan kommunen och leverantören. (*Se även 6.9 Utomstående parter*)

Vid användning av sådan tjänst ska i övrigt följande beaktas:

- Användarens lösenord ska vara unikt och får ej vara samma som övriga tjänsterelaterade lösenord, så som ex. inloggning på Svedala kommuns nätverk etc.

- Lösenordet ska bytas regelbundet.
- Konto som etablerats i tjänsten ska raderas vid anställningens upphörande.

- Vid användning av sociala medier i tjänsten ska av Svedala kommun fastställd riktlinje följas.
- Fildelning, nedladdning och lagring av programvaror, bild- film och ljudfiler för privat bruk på Svedala kommuns servrar eller datorer är inte tillåtet.
- Nedladdning av appar för privat bruk på smarta telefoner och pekplattor får inte ske på enheter som används för att behandla information med klassificeringsparametern *Viktig, Mycket viktig* eller *Kritisk* för sekretess/konfidentialitet. *(se även 8.2 Klassificeringsmodell för bedömning av skydds- och kravnivå samt 9.3 Regler för vissa system*)
- Nedladdning/lagring av programvaror, appar och filer från okända eller tvivelaktiga webbplatser är inte tillåtet.
- Det ska gå att förhindra åtkomst (*och göra användaren uppmärksam vid surfning*) till webbsidor/-adresser (*URL*) med olämpligt innehåll och/eller skadlig påverkan genom filter mot surfning till olämpliga sidor.
- Uppföljning av internetanvändandet kan förekomma. (*se 7.4 Granskning av säkerhetspolicy, etik och teknisk efterlevnad*)

7.6 Utbildning

Kompetens och medvetenhet är en trygghet både för den anställde och verksamheten. Verksamhetsansvarig chef ansvarar för att berörd personal utbildas i informationssäkerhet.

7.6.1 Anvisningar för utbildning

- Alla anställda ska få en introduktion i kommunens säkerhetsarbete, lämpligen vid anställningen.
- Alla anställda, även konsulter och övriga tredjepartsanvändare, ska få en anpassad information i informationssäkerhet.
- För informationssystem (*system och e-tjänster*) ska objektsägaren tillse att det definieras vilka krav som ställs på systemets användare samt erbjuda utbildning i skälig omfattning.
- Riktlinjer och anvisningar för informationssäkerhet i Svedala kommun ska finnas tillgängligt på intranätet. Ansvarig: Den i kommunen som är utsedd som informationssäkerhetsansvarig.

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

FYSISK OCH MILJÖRELATERAD SÄKERHET

7.7 Säkrade utrymmen

Åtgärder ska vidtas för att förhindra obehörigt tillträde till, eller störningar/skador på lokaler, utrustning och information. I det fall kraven i anvisningarna anses för höga eller låga ska erforderlig skyddsnivå bedömas genom riskanalys.

7.7.1 Anvisningar för skalskydd och tillträde

- Branschnormerna för brand- och stöldskydd ska följas. De normer som i första hand är aktuella är:

- EN 1047 (*EU-norm för brandklassning*) där brandklass P står för pappersdokument och brandklass DIS står för olika typer av datamedia.

- Svenska stöldskyddsföreningens norm (*SSF*) 200:4 (*Regler för mekaniskt inbrottsskydd*).

- Godkända lås- och larmsystem (*lägst skyddsklass 2*) som är anpassade till aktuell miljö ska finnas. Larmsystem ska vara kopplade till bemannad plats.

- Passerkontrollsystem ska finnas där känslig/typiskt sett sekretessbelagd information behandlas.

- Nycklar och passerkort ska förvaras i säkerhetsskåp som uppfyller Svensk standard SS 3492.

- Vid hantering av nycklar ska nyckelschema användas.

- För centrala utrymmen med IT-baserade informationssystem, såsom server- och kommunikationsutrymmen (*datorhallar och nodrum*) ska skyddsnivån vara entydigt definierat och dokumenterat. Dokumentationen ska vara skyddad från åtkomst från obehöriga.

- Skalskyddet i centrala utrymmen (*ex. serverhall*) och nodrum ska vara motståndskraftigt mot forcering motsvarande Svenska stöldskyddsföreningens norm 200:4 skyddsklass 3.

- Servrar och kommunikationsutrustning ska placeras i därför avsedda utrymmen.

- Extern eller egen personal som inte har behörighet får inte vistas ensamma i server- eller kommunikationsutrymmen.

- Vid externt besök i server- och kommunikationsutrymmen ska loggbok föras. I loggboken ska minst följande uppgifter noteras:

- Besökarens namn och organisation/företag

- Besöksmottagarens namn och organisatoriska tillhörighet
- Tidpunkt för in- och utpassering
- Syftet med besöket

Uppgifterna ska förvaras i minst 6 månader.

- I publika lokaler där det finns datorer ska det finnas inre och yttre skalskydd. Skalskyddet kan bestå av larmade och låsta lokaler.
- Datorer kan förses med vajerlås och förslagsvis låsas ihop parvis. Via låsbart bleck eller motsvarande kan datorn förankras mot det underlag den står på.

7.8 Skydd av utrustning

7.8.1 Anvisningar för placering och skydd av utrustning

- Systematiskt brandskyddsarbete (*SBA*) ska bedrivas i enlighet med Svedala kommuns riktlinjer.
- Brandskydd ska alltid finnas i eller i anslutning till server- och kommunikationsutrymmen. Expertis ska anlitas för rätt dimensionering av brandskyddet.
- I server- och kommunikationsutrymme ska automatiskt brandlarm finnas och larmsignalen kopplas till bemannad plats.
- Behov av klimatanläggning liksom temperatur- och fuktlarm ska beaktas för utrymmen där värmealstrande dyr och känslig utrustning förekommer. Larmsignalen ska kopplas till bemannad plats.
- Verksamhetskritisk information/material ska förvaras i säkerhetsskåp i låst utrymme.
- Arkivering av information lagrad på datamedia ska ske i rum eller skåp som uppfyller Riksarkivets krav enligt RA-FS 1997:3.
- Stöldbegärlig, dyr och svårersatt reservutrustning ska förvaras i låst utrymme med begränsat tillträde. Om möjligt ska utrustningen stöldskyddsmärkas.
- Utrustning, särskilt stöldbegärlig, ska vara märkt. Stöldskyddsmärkningen ska göras så att den inte går att ta bort utan svårigheter.
- Placering av skrivare och faxutrustning styrs av den typ av information som hanteras.
- När känslig eller typiskt sett sekretessbelagda uppgifter skrivs ut ska utskriften övervakas eller skyddas.

SVEDALA KOMMUN

7.9 Elförsörjning och kablageskydd

Elberoendet är stort idag och avbrott i elförsörjningen kan orsaka mer eller mindre omfattande konsekvenser för kommunens verksamheter och därmed även påverka kontinuiteten i prioriterade verksamheter.

7.9.1 Anvisningar för elförsörjning och kablageskydd

- Verksamhetsställen och verksamhetskritiska system med starkt beroende av elförsörjning ska vara försedda med reservkraft.
- Reservkraftsutrustningen ska testas regelbundet.
- För att underlätta felsökning ska både kablar för strömförsörjning och data-kommunikation dokumenteras på ritningar som ska hållas uppdaterade. Dokumentationen ska skyddas från åtkomst från obehöriga.

7.10 Publika miljöer

I Svedala kommuns publika lokaler så som bibliotek, medborgarkontor, skolor etc. tillhandahåller staden IT-utrustning åt Malmöborna för informationssökning/-hantering.

7.10.1 Anvisningar för datorer i publik miljö

- På särskilt utsatta platser ska utrustningen vara fastlåst.
- I publika miljöer där datorer tillhandahålls ska det inre och yttre skalskyddet uppfylla Svedala kommuns krav (*se även 10.1 Anvisningar för skalskydd och tillträde*)
- I publika lokaler där datorer tillhandahålls och ingen åtkomstbegränsning är uppsatt ska ID-kort, lånekort, tidbokningslista eller motsvarande användas för att motverka anonym användning.
- Användare bör upplysas om riskerna med användning av publika trådlösa nät, bl.a. att information mellan dator och accesspunkt är okrypterad och kan avlyssnas av andra användare. Användare bör även upplysas om att användning loggas och kan komma att användas vid misstanke om eller vid utredning av brott.
- Endast publika system (*Publik Internet-access*) ska kunna nås från datorn.
- Det ska gå att förhindra åtkomst (*och göra användaren uppmärksam vid surfning*) till webbsidor/-adresser (*URL*) med olämpligt innehåll och/eller skadlig påverkan genom filter mot surfning till olämpliga sidor.
- Internettrafik och/eller lokal trafik ska loggas och sparas minst 2 månader.

SVEDALA KOMMUN

7.11 Säkerhet för utrustning utanför egna lokaler

Utrustning som används utanför de egna lokalerna ska ha lika högt säkerhetsskydd som om den används i de egna lokalerna. Särskild hänsyn ska tas till risken för stöld och obehörig informationsåtkomst.

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

STYRNING AV KOMMUNIKATION OCH DRIFT

7.12 Driftrutiner och driftansvar

Enligt IT-strategin ska varje verksamhet ansvara för att äga, förvalta, utveckla och avveckla sina specifika verksamhetssystem och sin information.

Ansvaret för ledning och drift av gemensamma informationstillgångar ska vara tydligt definierat

7.12.1 Anvisningar för driftdokumentation av IT-baserade informationssystem

- Skriftlig driftdokumentation med ansvarsfördelning ska finnas, hållas aktuell och minst omfatta dokumentation av:
    - Ansvarsfördelning och förvaltningsorganisation
    - Rutiner för ändring i driftmiljö, systemplanering och driftgodkännande,
    - Logghantering, incidenthantering, återstarts- och återställningsrutiner
    - Rutiner för säkerhetskopiering
- Dokumentationen ska vara godkänd av IT-systemansvarig och hållas aktuell.
- Rutin för ändring av driftdokumentation ska finnas.
- Originaldokumentationen ska förvaras i dokumentskåp som uppfyller brandklass 90 P, godkänt av Statens Provningsanstalt.
- Det ska finnas en förteckning över all utrustning och programvara.
- Dokumentationen gäller oavsett om driften sker internt eller hos extern part.

7.13 Styrning av ändringar i driftmiljö

Det ska finnas både en skriftlig rutin för driftgodkännande av IT-system/e-tjänster och en rutin för bedömning av framtida kapacitetsbehov.

7.13.1 Anvisningar för ändring i driftmiljö

- Rutiner för ändringshantering (*även mindre ändringar*) ska finnas etablerade inom systemets förvaltningsorganisation, och vara framtagen i samråd/samverkan med IT-driftleverantören och dennes process för ändringshantering.
- All ändring av programvara ska, om det är tillämpbart, godkännas innan den installeras i utbildnings- test-/produktionsmiljö.

- Ändringar i driftmiljön i system som utbyter information med andra system (*integrationer*) ska ske i samråd/samverkan ske med IT-systemansvarig för teknisk plattform.
- Samtliga ändringar ska kunna härledas till en ansvarig beställare.

7.14 Systemplanering och systemgodkännande

IT-stöd och e-tjänster av olika slag förekommer i stor skala i kommunens verksamheter, både centralt och inom respektive förvaltningar, vidare varierar systemens krav på skyddsnivå. Det är därför viktigt att de krav som ställs både på den som äger och förvaltar tillgången såväl som driftar den tydliggörs.

7.14.1 Anvisningar för systemplanering och systemgodkännande

- Innan driftsättning ska:
  - säkerhetskraven identifieras, värderas (*klassificeras*), beslutas och införas.
  - Acceptanstest/leveranstest utföras som bland annat beskriver omfattning av testet och antal användare och kategorier som ska testa.
- Systemet ska vara driftgodkänt av styrgrupp eller motsvarande.
- Servicenivåavtal (*sk. SLA, Service Level Agreement – internt även kallat överens-kommelse*) som ingår i drift- och förvaltningsavtal ska vara fastställt och kommunicerat till berörda parter. Servicenivåavtalet, som reglerar IT-driftleverantörens respektive verksamhetens ansvar, bör särskilt reglera följande:
  - Tjänstens omfattning
  - Tjänstens tillgänglighetstider
  - Eventuella tilläggstjänster
  - Informationssäkerhet
  - Undantag/avgränsningar
  - Förändringar i tjänsten
  - Tillåtna avbrott
  - Åtgärder vid avbrott
  - Backup
  - Dokumentation och statistik
  - Support

  - Mätning och uppföljning av serviceavtalet
  - Viten

- Innan beslut fattas om att använda extern leverantör av IT ska en fördjupad riskanalys genomföras som en del av beslutsunderlaget. Analysen ska omfatta laglighets-, risk- och konsekvensbedömning. Resultatet ska dokumenteras. Beställaren (*verksamheten*) ska kontrollera hur avtalet tillämpas för att säkerställa att utförda tjänster uppfyller alla avtalade krav.
- Alla krav på externa tjänsteleveranser ska regleras genom ett servicenivåavtal.
- Om tjänsten innehåller behandling (*inkluderat lagring*) av känsliga uppgifter, personuppgifter eller liknande ska särskilda krav om hur dessa ska hanteras ställas på leverantören.
- Kapacitetsbehov/prestanda av lagringsutrymme, processorer etc. ska övervakas och följas upp.
- För att möjliggöra förenklat inloggningsförfarande bör system/e-tjänst om möjligt kopplas till Svedala kommuns katalogtjänst. Beslutas lämpligen vid klassificeringsmomentet.

7.15 Skadlig kod och säkerhetsuppdateringar

Skadlig kod (virus, trojaner m.fl) är ett vanligt sätt att orsaka skada på den IT-enhet som används, nätverket eller informationen som behandlas i densamma. Säkerhetsuppdateringar är viktiga för att åtgärda identifierade sårbarheter i system och utrustning. Säkerhetsuppdateringar ska alltid bedömas innan aktuell patch installeras.

7.15.1 Anvisningar för åtgärder mot skadlig kod

- Programvara för skydd mot skadlig kod ska installeras och kontinuerligt uppdateras på Svedala kommuns datorer.
- Alla Svedala kommuns datorer (*och servrar i tillämplig omfattning*) ska vara skyddade mot skadlig kod/skadliga program. Skyddet ska aktiveras automatiskt då datorn/utrustningen startas.
- Centralt avtalade produkter ska i möjligaste mån användas.
- Uppdatering av antivirusskyddet ska utföras automatiskt vid anslutning till Internet.
- Programvaror som installeras i Svedala kommuns datorer ska så långt det är möjligt vara certifierade, paketerade och godkända av behörig beställare.
- Nedladdning/lagring av programvaror, appar och filer från okända eller tvivelaktiga webbplatser är inte tillåtet.

- Rutiner ska finnas för att uppmärksamma användarna på risker och regler.

7.15.2 Anvisningar för säkerhetsuppdateringar (patchar)

- Rutin ska finnas för att hantera leverantörers säkerhetsuppdateringar.
- Nya virussignaturfiler ska installeras på samtliga datorer/servrar inom 24 timmar efter utgivning.
- Relevanta utgivna säkerhetspatchar ska testas och installeras inom 7 dygn. Detta gäller såväl operativsystem som applikationer.

7.16 Säkerhetskopiering

Säkerhetskopiering (backup) innebär att filerna finns sparade i en kopia som senare kan återläsas om originalet skadas eller försvinner.

7.16.1 Anvisningar för säkerhetskopiering

- Alla användare ska upplysas om vad som säkerhetskopieras och hur delar som inte säkerhetskopieras ska hanteras.
- Säkerhetskopiering ska ske enligt vad som överenskommits i Servicenivåavtalet. Det är respektive systemägarrepresentant som fastställer krav på frekvens av säkerhetskopiering, förvaringsplats för kopia, krav på återläsningstid m.m.
- Säkerhetskopieringen ska schemaläggas, dokumenteras och utföras av behörig personal.
- Återläsning av säkerhetskopia ska testas regelbundet.
- Datamedia ska förvaras i datamediaskåp eller motsvarande. Datamediaskåp ska uppfylla brandklass 90 P och vara godkänt av Statens Provningsanstalt eller motsvarande.
- Säkerhetskopior ska förvaras i annan byggnad, minst 500 meter från platsen där systemet finns (*eller om så inte är möjligt i annan brandcell än där systemet finns*)
- Lagring av information (*data och filer*) som Svedala kommun äger får endast ske på lagringsytor utanför Svedala kommuns kontroll om:
  - Informationen klassificerats som *Mindre viktig*, dvs. att den är öppen för eller kan spridas till en obestämd krets mottagare utan risk för negativa konsekvenser och där spridning inte medför någon skada för egen eller annan organisation eller enskild person. (*se matrisen 8.2 Klassificering av information*)
  - Informationen också finns tillgänglig på Svedala kommuns nätverk.

SVEDALA KOMMUN

Information som lagras på lagringsytor utanför Svedala kommuns kontroll kan utgöra allmänna handlingar och reglerna för t.ex. diarieföring och gallring ska beaktas även för denna information.

Med ”*utanför Svedala kommuns kontroll*” avses exempelvis alla s.k. molntjänster som iCloud, Dropbox, Hotmail, Gmail etc, där avtal som reglerar informationssäkerheten saknas mellan staden och leverantören. (*Se även 6.9 Utomstående parter*)

Vid användning av sådan tjänst ska i övrigt följande beaktas:

- Användarens lösenord ska vara unikt och får ej vara samma som övriga tjänsterelaterade lösenord, så som ex. inloggning på Malmö stads nätverk etc.
- Lösenordet ska bytas regelbundet.
- Konto som etablerats i tjänsten ska raderas vid anställningens upphörande.

SVEDALA KOMMUN

7.17 Styrning av nätverk

Svedala kommuns nätverk för informationsöverföring ska skyddas utifrån verksamhetens krav och kopplingar mot externa nät.

7.17.1 Anvisningar för säkerhetsarkitektur i nätverk

- Information ska kunna överföras oförvanskad i nätverk.
- All extern (*riktad till egen organisation*) trafik baserad på TCP/IP ska gå via brandvägg och filtreras utifrån verksamhetsbehoven. Hänsyn måste tas till om det gäller åtkomst till Svedala kommuns gemensamma resurser alternativt egen förvaltning/skola och vem som vill nå aktuell resurs (*behörighetsaspekt*). Generellt ska oönskad trafik vara spärrad.
    - Intrångsdetekteringssystem (*IDS*) ska användas för att möjliggöra spårning av intrång och intrångsförsök i Svedala kommuns infrastruktur.
    - Förvaltningar och bolag ska logiskt kunna separeras från varandra.
    - Portöppningar i brandväggar ska beslutas och dokumenteras. Beslut om portöppning ska minst innehålla:
    - Beskrivning av syftet med tjänsten.
    - Beställare.
    - Tidsbegränsning och kontaktperson.
    - Berörda system *(internt/externt*)
    - Trafiktyp
    - Det ska vara möjligt att separera nät fysiskt från varandra.
    - Sammankoppling av nät hos t.ex. leverantör ska godkännas av Svedala kommuns IT enhet.
    - Systemklockor ska synkroniseras mot Svedala kommuns NTP-server, vilken i sin tur ska vara synkroniserad mot atomur.

7.17.2 Anvisningar för trådlösa nät

- Säkerhetsarkitekturen för trådlösa nät ska vara enhetlig och dokumenterad.
- Publika trådlösa nätverk får inte ha direkt eller indirekt åtkomst till det administrativa nätet. (*Se även 10.4 Anvisningar för datorer i publik miljö*)

7.18 Mediahantering och mediasäkerhet

Lagringsmedia (såväl hårddiskar i befintliga datorer som externa hårddiskar, och annan extern lagringsmedia som usb-minne, mobiltelefoner, CD/DVD-skivor etc.) har stor lagringskapacitet och kan medföra skada för Svedala kommun om dessa kommer i orätta händer.

7.18.1 Anvisningar för hantering av flyttbar media

- Flyttbar media som tas med utanför arbetsplatsen bör inte innehålla mer information än den som är absolut nödvändig.
- Kopia av innehållet på flyttbart media som förs utanför arbetsplatsen ska finnas kvar på arbetsplatsen. Detta för att kunna bedöma skadan vid en förlust och tillse att informationens original inte försvinner.
- Användaren ansvarar för att känslig information krypteras.

7.19 Avveckling av media (ref ”säker skrotning”)

Vid avveckling av utrustning som innehåller lagringsmedia, så som stationära och bärbara datorer, pekplattor, smarta telefoner, skrivare, usb-minne och annan extern lagringsmedia, ska åtgärder vidtas för att säkerställa att den information som lagras eller lagrats på enheten inte kan läsas eller återskapas av obehörig.

7.19.1 Anvisningar för avveckling av media

- Det ska finnas en rutin i förvaltningen som beskriver hur avvecklingen av media effektueras. Av dokumentationen ska framgå var och hur utrustningen förvaras, datum för avyttring, typ av information och till vem lagringsmediat har lämnats. Destruktionsintyg från destruktionsfirman eller leverantören som återtagit utrustningen ska arkiveras genom objektsförvaltarens eller motsvarandes försorg.
- Lagringsmedia får skrivas över med av Svedala kommun godkänt verktyg och därefter återanvändas. Om överskrivning inte är möjligt ska lagringsmediat förstöras.
- Utrustning som inte ska avvecklas/avyttras men däremot byter användare (*exempelvis vid personalförändringar eller överbliven utrustning*) ska lagringsmediat skrivas över med av Svedala kommun godkänt verktyg innan utrustningen återanvänds om:

- lagringsmediat hanterat information med klassificeringsparametern *Viktig, Mycket viktig* eller *Kritisk* för sekretess/Konfidentialitet och den nya användaren inte ska ha åtkomsträttighet till samma information.

Alternativt kan befintlig hårddisk bytas ut mot ny för att därefter hanteras enligt punkt 2 och 6.

- Vid avyttring av lagringsmedia med känsligt innehåll ska åtgärder vidtas för att informationsinnehållet görs oläsbart.

- Fabriksåterställning av mobila enheter anses inte vara en tillräcklig åtgärd. Vidare ska eventuella Apple/iTunes-konto och liknande som etablerats för tjänsteutövning och där kontouppgifterna hänvisar till Svedala kommun raderas. (*se även 9.2 Krav på anställda gällande informationssäkerhet*)
- Av Svedala kommun centralt upphandlad tjänst ska användas.
- Destruktion ska ske på ett miljömässigt korrekt sätt.

7.20 Säkerhet för systemdokumentation

7.20.1 Anvisningar för systemdokumentation

- Systemdokumentation ska skyddas i enlighet med den klassificering som gäller för det aktuella systemet. Den ska hållas aktuell och vara godkänd av objektsansvarig och/eller IT-systemansvarig.

7.21 Utbyte av information och program

Vid informationsutbyte mellan organisationer, liksom vid systemintegrationer, ska gemensamma bedömningar göras av behovet av skydd mot åtkomst/sekretess och riktighet samt tillgänglighet. Ansvarsförhållandena ska vara klarlagda.

7.21.1 Anvisningar för annat informationsutbyte

- Telefonsamtal med känslig information ska ske där det inte kan avlyssnas.
- Känslig information på whiteboard, blädderblock och motsvarande ska avlägsnas/ förstöras efter avslutat möte.
- Känslig information får inte skickas med fax, då fax inte är att betrakta som säker överföringsmetod.
- Information som delas eller kommuniceras mellan olika system och som klassificerats som *Viktig, Mycket viktig* eller *Kritisk* för sekretess/konfidentialitet, ska kommuniceras i krypterad form eller med den skyddsnivå som identifierades i samband med klassificeringen. Informationens skyddsbehov kvarstår oavsett system.

7.22 Elektroniskt offentliggjord information (info på webbsidor)

Åtgärder ska vidtas för att skydda riktigheten i elektroniskt offentliggjord information och att information som inte längre ska ligga kvar gallras.

7.22.1 Anvisningar för elektronisk offentliggjord information

- Det ska finnas en formell process för godkännande innan information görs allmänt tillgänglig.

- Det ska alltid finnas en ansvarig för webbsidor där Svedala kommuns verksamheter publicerar information. Denna ansvarar för att rutiner upprättas och efterlevs.
- Förvaltningar och bolag ansvarar för att information som publiceras av den egna verksamheten i gemensamma system är korrekt.
- Publicering ska om möjligt ske i en testmiljö, ”förhandsvisning”.
- Sekretessbelagda uppgifter får inte publiceras på internet. Sekretessbedömning ska utföras innan information publiceras (*se även 7.3 Skydd av personuppgifter*)
- Rutin för gallring av publicerad information ska finnas i enlighet med Datainspektionens vägledning för webbpublicering av protokoll och diarier.

7.23 Övervakning/Loggar

Kritiska och säkerhetsrelevanta händelser i drift och datakommunikation ska vara spårbara. Varje transaktion ska kunna knytas till den som utfört den. Detta ska i första hand åstadkommas med automatiska loggningsfunktioner. Behovet av loggning och uppföljning av loggar (analys) fastställs av systemägaren efter verksamhetens behov samt efter genomförd informationsklassificering.

7.23.1 Anvisningar för logghantering

- Varje användare ska ha en unik identifikation (*användar-ID*). Användar-ID ska kunna användas för att spåra aktiviteter kopplade till den ansvariga individen.
- Loggning och analys av obehöriga åtkomstförsök till informationstillgångar (nätverk, *information m.m.*) ska genomföras regelbundet oavsett informationens klassificerings-nivå.
- Åtkomst till loggar styrs av informationsklassificeringen av systemet/applikationen.
- Loggar ska finnas så att aktiviteter utförda av personer med hög behörighet kan spåras.
- Loggar ska skyddas mot radering, manipulering och obehörig åtkomst.
- Loggar ska granskas enligt fastställd rutin, där det ska framgå vad som ska loggas, hur ofta loggar ska granskas, vem som ska utföra granskningen samt vad som är att betrakta som överträdelse. Beslut ska finnas för hur överträdelser ska hanteras.
- Hur länge en logg ska sparas utgår från resultatet av informationsklassificeringen och identifierade lagrum. Kompletterande stöd/vägledning, se Svedala kommuns riktlinjer för arkivering.

8 STYRNING AV ÅTKOMST

8.1 Verksamhetskrav på styrning och åtkomst

Åtkomst till IT-system och nätverk ska styras utifrån verksamhetens behov och säkerhetskrav. Rutiner ska finnas för att säkerställa behöriga användares åtkomst och för att förhindra obehörigas åtkomst till Svedala kommuns informationssystem.

Den som använder Svedala kommuns informationstillgångar på ett sätt som strider mot kommunend regler kan bli föremål för en disciplinär åtgärd.

8.2 Behörighetsadministration

Hantering av behörighetsadministration ska ske enligt anvisningarna.

8.2.1 Anvisningar för hantering av behörighetsadministration

- Systemadministratörer/-tekniker ska ha individuella användaridentiteter. Om det inte är möjligt ska manuell logg föras.
- Behörighetsadministratörer ska finnas utsedda för Svedala kommuns IT-system.
- Verksamhetschef beslutar om aktuell behörighet.
- **För tilldelning av behörigheter till centrala och enskilda system gäller**:

Beställningsrutiner ska tas fram av systemägaren och systemförvaltaren. I rutinen ska framgå hur beställningen görs, vem som godkänner beställningen, vilka avgränsningar i åtkomsträttigheter som är nödvändiga beroende av användarens systemanvändarroll. Vidare ska framgå på vilket sätt behörigheterna revideras för att inaktivera användare som inte längre ska ha åtkomst till systemet, eller vissa delar av det.

- **För tilldelning av behörigheter utanför den egna förvaltningen gäller:**

Vid till delning av behörigheter utanför den egna förvaltningen gäller samma rutin som för övriga system.

- **För vikarier och inhyrd personal ska tilldelning av behörigheter ske enligt separata instruktioner.**

Behörigheten ska sättas på en sådan nivå att det är möjligt att utföra arbetsuppgifter men inget mer. Antalet behörighetsnivåer vid en viss arbetsplats ska vara så få som möjligt så att administrationen blir enkel. För dessa specialkonstruerade vikariatsbehörigheter gäller följande:

- Det ska bara gå att nå och arbeta i aktuell tillämpning.
- Den ska bara gälla inom den del av organisationen, som uppdraget avser.

- Lösenordet (*i nät och tillämpning*) ska bytas direkt när vikariatet går ut.
- Byte av lösenord ska göras av berörd chef/arbetsledare alternativt systemförvaltare.
- ID och lösenord ska förvaras på ett betryggande sätt (*kassaskåp eller motsvarande*) när de inte används.

För att uppfylla Svedala kommuns krav på att varje transaktion ska kunna knytas till den som utfört den.

8.3 Lösenordsregler (starkt och kvalificerat lösenord)

Ett bra lösenord innehåller alla sorters tecken; små och stora bokstäver, siffror och specialtecken. Ju längre och komplexare lösenord, desto längre tid tar det att knäcka det. Följande vägledning gäller:

- *Välj aldrig ett lösenord som kan kopplas till dig på något sätt.*
- *Ha med alla typer av tecken i lösenordet.*
- *Om du måste skriva ner ditt lösenord, gör det på ett papper och behandla det som ett värdepapper.*
- *Ge aldrig ut ditt lösenord till någon annan.*
- *Byt lösenordet regelbundet.*

8.4 Behörighetskontroll

Åtkomst till informationstillgångar ska ske med ett behörighetskontrollsystem (BKS) där varje användare har en unik identitet och lösenord eller eventuellt en rolltillhörighet.

Anvisningar för behörighetskontroll

- Lösenord och koder ska vara individuella och får inte överlåtas eller lånas ut.
- Behörighetskontrollsystem ska finnas och vara integrerat i de plattformar som väljs för serveroperativsystem, databashanterare och tillämpningar. Möjlighet till spårbarhet ska alltid finnas.
- SQL-, ODBC, ADO (*ActiveX Data Objects*)-tjänster (*m,fl*.) får inte installeras så att IT-systemets databas kan anropas från klient utan att åtkomst prövas av tillämpade behörighetskontrollfunktioner.
- För autentisering (*identifiering*) av användare får följande tekniker användas:

- Certifikat eller elektroniskt ID-kort
- Lösenord

- Lösenord ska skapas enligt gällande instruktioner.
- I publika miljöer där datorer tillhandahålls ska ID-kort, lånekort, tidbokningslista eller motsvarande användas för att motverka anonym användning.

8.5 Styrning av åtkomst till nätverk

Interna och externa nätverk ska betraktas som informationstillgångar och åtkomst styras enligt samma princip som åtkomststyrning i övrigt. Svedala kommuns nätverk ska vara tydligt avgränsat mot omvärlden genom lämplig teknik.

8.5.1 Anvisningar för nätverksanslutning

- En nätverksansluten persondator ska inte samtidigt kunna vara ansluten till annat nät (*via modem eller trådlöst*)
- Extern kommunikation mot Svedala kommuns nätverk ska ske via godkända fjärråtkomstlösningar (*Portwise, Direct Access [UAG] och VPN-koncentrator*). Identifieringsmetod styrs av resultatet av klassificeringen.
- All inkommande trafik baserad på TCP/IP ska gå via brandvägg.
- För servicetjänster on-line ska avtal finnas med den part som har tillstånd till upp-kopplingen.
- Alla andra än av Svedala kommun, för ändamålet, konfigurerade datorer som ansluts till kommunens nätverk ska endast kunna komma åt internet.
- All utrustning som ansluter mot Svedala kommuns nätverk ska vara spårbar.
- Användning av trådlösa nätverk (*WLAN*) ska ske enligt anvisningarna. (*se även 11.6 Styrning av nätverk*)

8.6 Styrning av åtkomst till operativsystem

Operativ- och behörighetskontrollsystem ska användas för att styra användares och administratörers åtkomst till informationstillgångar.

8.6.1 Anvisningar för åtkomst till operativsystem

- Restriktivitet ska gälla vid tilldelning av åtkomsträttigheter till operativsystem.
- Operatörskonsolfunktion ska skyddas med stark autentisering.
- Åtkomst till konsol ska skyddas med antingen certifikat eller engångslösenord.
- Max fem inloggningsförsök ska tillåtas, därefter ska användarkontot spärras.

- Systemverktyg som kan gå förbi system- och tillämpningsspärrar ska användas restriktivt, styras noga och endast användas av behörig systemadministratör.

8.7 Åtkomst till information och verksamhetssystem

Objektsägaren för förvaltningsobjektet har det övergripande ansvaret rörande processen för tilldelning av behörigheter i ett verksamhetssystem. Ansvaret för tilldelning av behörighet i det enskilda fallet åvilar däremot ansvariga i linjeorganisationen.

8.7.1 Anvisningar för åtkomst till information och verksamhetssystem

- Objektsägaren ska besluta om ett IT-systems information ska vara åtkomligt från externa platser.
- Alla användare ska tilldelas personliga användarkonton.
- Max fem inloggningsförsök ska tillåtas, därefter ska användarkontot spärras.
- En rutin ska finnas för utlämnande av allmän handling där information hämtas från ett system. Utlämnandet ska ske genom utskrift, digitalkopia eller bildskärm.
- Allmänheten kan få använda en terminal om:

- Det inte finns någon möjlighet att komma åt handlingar som inte är allmänna.
- Det inte går att komma åt handlingar som är sekretessklassade.
- Det inte finns någon risk för att handlingarna förstörs eller ändras.

8.8 Mobil datoranvändning och distansarbete

Skyddet av information ska säkerställas vid användning av mobil utrustning och vid distansarbete. Med mobil utrustning menas avancerade s.k. smarta telefoner, bärbara datorer, handdatorer, pekplattor och liknande enheter som kan användas för informationsbehandling från annan plats än arbetsplatsen. Med distansarbete avses ”Av arbetsgivaren tillhandahållen arbetsplats i hemmet”.

8.8.1 Anvisningar för mobil datoranvändning

- Förteckning av mobila enheter finns upprättad på IT-enheten.
- Anslutning mot Svedala kommuns nätverk på annat sätt än det som Svedala kommun godkänt är inte tillåtet. Detta gäller även uppkoppling från publika miljöer. Applikationer för s.k. remote access (*ex. GoToMyPC mfl*) för sammankoppling av den mobila enheten (*ex tfn/pekplatta*) och tjänstedatorn är inte tillåtet.
- Riskerna med att använda trådlösa publika nät ska beaktas.

- Extern kommunikation mot kommuns nätverk ska ske via godkända fjärråtkomstlösningar (*Portwise, Direct Acess [UAG] och VPN-koncentrator*). Identifieringsmetod styrs av resultatet av klassificeringen.
- All lagrad information på intern minnesenhet ska krypteras. Svedala kommuns rekommenderade lösning ska användas.
- Vid hårddiskkryptering på bärbara datorer ska denna – om möjligt - kompletteras med krav på manuell upplåsning av tpm (*pinkod*) innan inloggning mot Svedala kommuns nätverk.
- Vid lagring på extern minnesenhet (*ex. usb-minne eller extern hårddisk*) ska information med klassificeringsparametern *Viktig, Mycket viktig* eller *Kritisk* för sekretess/konfidentialitet krypteras. Svedala kommuns rekommenderade lösning ska användas.
- Virusskydd ska vara installerat och aktiverat på mobila enheter, om den tekniska plattformen stödjer detta. Skyddet ska aktiveras automatiskt då enheten startas. Uppdatering av virusskyddet ska ske automatiskt vid anslutning till Svedala kommuns nätverk. Om detta inte är möjligt ska manuell uppdatering ske varje dag.
- Utrustningen ska låsas efter max 10 minuters inaktivitet om den tekniska plattformen medger detta.
- Bärbar utrustning ska skyddas med lösenord eller motsvarande. (*Se även 12.3 Lösenordsregler*)
- Bärbar utrustning bör vara stöldskyddsmärkt. *(Se även 10.2 Skydd av utrustning*)
- Central rutin för managering av mobila enheter (*smarta telefoner/pekplattor*) ska finnas.
- Registrering och säkerhetsinställningar ska göras av behörig tekniker innan utlämning av utrustningen för mobil datoranvändning får ske.

8.8.2 Anvisningar för distansarbete

- Anslutning mot nätverket på annat sätt än det som Svedala kommun godkänt är inte tillåtet.
- Utrustningen ska följa Svedala kommuns anvisningar för standardiserade datorer.
- Utrustningen bör vara stöldskyddsmärkt.
- Datorn ska låsas efter max 10 minuters inaktivitet.
- Utrustningen får endast användas av den anställde.
- Information ska lagras på av arbetsgivaren bestämd plats.

SVEDALA KOMMUN

- Samma säkerhetsnivå för säkerhetsuppdateringar och virusskydd ska finnas på distansarbetsplatsen som på den ordinarie arbetsplatsen. Skyddet ska aktiveras automatiskt när datorn startas.

SVEDALA KOMMUN

9 SYSTEMUTVECKLING/-INKÖP OCH SYSTEMUNDERHÅLL

9.1 Informationssäkerhet vid utveckling och tillämpning av e-tjänster

Säkerhetskraven, som redovisas i samband med klassificeringen, ska vara uppfyllda innan driftgodkännande kan ges.

9.1.1 Anvisningar för informationssäkerhet vid utveckling och tillämpning av e-tjänster.

- Vid utveckling av nya tillämpningar och/eller förändringar i befintliga tjänster ska möjligheten att använda elektronisk identifiering prövas. Elektronisk identifiering stöder:

- Stark autentisering (*säker inloggning*)
- Elektronisk signatur (*säker utfärdare*)
- Kryptering (*insynsskydd av information*)

- För information som är offentlig ska skydd finnas mot förvanskning och förlust. Särskild vikt ska läggas vid att koden i webb-tillämpningar är skyddad mot manipulation i syfte att förhindra SQL-injektioner och liknande angrepp.
- Personuppgifter ska skyddas enligt integritets- och sekretesskrav. Datainspektionens allmänna råd om säkerhet för personuppgifter ska följas.
- Informationsklassificering ska alltid göras för att fastställa val av identifieringssätt, i samband med införandet av nya e-tjänster.
- Om klassificeringen ger bedömningen *Kritisk* för någon av parametrarna Sekretess/Konfidentialitet, Riktighet och Spårbarhet ska certifikat på kort (*hårt certifikat*) användas.
- Om klassificeringen istället ger bedömningen *Viktig eller Mycket viktig* för någon av parametrarna får elektronisk legitimation/BankID, engångslösenord med dosa alternativt engångslösenord med sms eller annan likvärdig metod (*förstärkt-autentisering*) användas.
- Om klassificeringen ger bedömningen *Mindre viktig* får användarnamn och lösenord användas såvida tjänsten inte ska vara allmänt tillgänglig.
- Användarnamn och lösenord får, som regel, inte skickas i klartext.

Systemet ska skydda så att obehöriga inte kan utnyttja en inloggad eller tidigare inloggad session

9.2 Säkerhet i tillämpningar

9.2.1 Anvisningar för användardokumentation

- Användardokumentationen (*manualer, instruktioner etc*) ska utformas utifrån användarens roll och behov och finnas tillgänglig för alla användare.
- Användardokumentationen bör finnas tillgänglig i elektronisk form ”online”.

9.3 Elektronisk signatur

Om utställarens identitet måste garanteras vid informationsutbyte – t.ex. genom en underskrift – ska rekommenderad teknisk lösning användas.

9.3.1 Anvisningar för elektronisk signering

- Elektroniska signaturer kan användas istället för handskrivna signaturer, då de möjliggör elektroniska, juridiskt bindande avtal, order, betalningar m.m. vid bl.a. e-handel mellan företag och organisationer.
- Elektronisk signering ska ske med säkerhetsmässigt acceptabel teknik och förväntad juridisk acceptans.

9.4 Kryptering/krypteringsregler

Kryptografiska lösningar ska finnas för att säkerställa behovet av att skydda allmän, känslig eller sekretessbelagd information från obehörig åtkomst, förstörelse, skada eller tillgrepp.

9.4.1 Anvisningar för kryptering

- Krypteringsfunktionen ska:
  - kunna fungera såväl vid lagring som under kommunikation och kunna hantera olika typer och nivåer.
  - bygga på öppna testade algoritmer och kunna erbjuda kryptering som ligger i nivå med KSU (*Krypto för skyddsvärda uppgifter, nationellt godkända kryptografiska funktioner*).
- Behovet av kryptering ska styras av informationens skyddsvärde. (*se även 8.2 Klassificering av information, 8.3 Hantering och märkning av handlingar, 12.8 Mobil datoranvändning och distansarbete samt 7.3 Skydd av personuppgifter*)

9.5 Säkerhet i databaser och program

Hantering av databaser och program ska ske enligt fastställd systemutvecklings-/förvaltningsmodell. För detaljer se kap. 11.

Anvisningar för hantering av testdata och program

- Dokumenterat acceptanstest ska vara avslutat före driftgodkännande.
- Fastställd ändringsrutin ska vara avslutad före ändringsgodkännande.
- All programvara (*ny/ändring*) ska godkännas innan installation i produktionsmiljö. Testprotokoll ska finnas, undertecknat av systemägarrepresentant eller annan av denna utsedd person innan installationen i produktionsmiljön.

9.6 Skydd av testdata

All information i samband med systemutveckling och förvaltning ska skyddas enligt samma principer som övrig verksamhetsinformation.

9.6.1 Anvisningar för skydd av testdata

- Data i testmiljö får inte innehålla verkliga persondata.
- Kopiering av produktionsdata ska loggas för att vara spårbar.
- Kopiering får endast ske efter skriftlig beställning från projektledare/ systemägar-representant/systemförvaltare och ska registreras i ärendehanteringssystem eller motsvarande.

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

10 HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER

10.1 Rapportering av incidenter

En väl fungerande rapportering och hantering av incidenter och säkerhetsbrister skapar goda förutsättningar för att bedöma vilka säkerhetsåtgärder som ska prioriteras.

10.1.1 Anvisningar för incidenthantering

- Incidenter ska rapporteras snarast för att minimera skada, åtgärda brister och utreda eventuell brottslighet. Exempel på incidenter som ska rapporteras är stöld eller förlust av information och/eller utrustning som används för informationsbehandling (*t.ex. datorer, pekplattor, tfn och annan extern lagringsmedia såsom usb, externa hårddiskar, etc*). Brand och vattenläckage, omfattande virusangrepp, överbelastningsattacker, intrång/intrångsförsök eller manipulering/radering av information är ytterligare exempel på incidenter.

- Allvarliga informationssäkerhetsincidenter ska

    - Omgående rapporteras till tjänstgörande TIB (*Tjänsteman i beredskap*).

    - Rapporteras till Svedala kommuns utsedda informationssäkerhetsansvariga för kännedom.

    - I det fall händelsen endast berör enskild förvaltning också rapporteras till berörd förvaltnings kontaktperson.

Med allvarliga informationssäkerhetsincidenter menas händelser som innebär att egen kritisk verksamhet, eller för samhället nödvändig tillgänglighet och servicenivå (*samhällsviktig verksamhet*) inte kan - eller riskerar att inte kunna - upprätthållas och där händelsen kan medföra mycket stor skada eller katastrofal skada för egen eller annan organisation eller enskild person.

- Svedala kommuns kommunövergripande system för rapportering av incidenter ska användas.

- IT-relaterade incidenter ska även rapporteras till IT-support via e-post eller tfn.

- Svedala kommun ska ha en etablerad kontakt med Myndigheten för samhällsskydd och beredskaps funktion CERT-SE (*Sveriges nationella CSRIT - Computer Security Incident Respons Team*) vars uppgift är att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.

SVEDALA KOMMUN

11 KONTINUITETS- OCH AVBROTTSPLANERING

11.1 Kontinuitetsplanering

För att minska konsekvenserna vid allvarliga störningar eller avbrott i Svedala kommuns verksamheter och kritiska verksamhetsprocesser krävs en i förväg upprättad och dokumenterad kontinuitetsplan. Processen för kontinuitetshantering omfattar identifiering av åtagande, risker, risk- och sårbarhetsanalyser och framtagning av nödvändiga planer för att säkerställa att den information som är nödvändig för verksamheten är tillgänglig och att viktiga verksamheter och funktioner kan återställas inom rimlig tid. Begreppet avbrottsplan är en del i verksamhetens kontinuitetsplanering och avser system/e-tjänster.

11.1.1 Anvisningar för processen kontinuitetsplanering

- Verksamhetsansvarig chef ansvarar för att det finns en dokumenterad kontinuitetsplan för kritiska och/eller samhällsviktiga verksamheter (*åtagande*) samt verksamheter vars stödjande system/e-tjänsters krav på tillgänglighet klassificerats som *Mycket viktig* eller *Kritisk*. Kontinuitetsplanen ska omfatta:

- Ansvar och befogenheter för kritiska rollinnehavare.
- Informationskanalerna och vilka man informerar.
- Nödlägesrutiner.
- Identifiering av beroenden.
- Plan för återgång till normalläge.
- Plan för återtagning av förlorad information och annat av vikt.
- Rutin för uppdatering av kontinuitetsplanen.

- Det ska utses en ansvarig person för att hålla kontinuitetsplanen aktuell.
- Kontinuitetsplanen ska finnas tillgänglig även vid bortfall av IT.
- Svedala kommuns metod och metodstöd för kontinuitetsplanering ska användas.

11.2 Avbrotts-/återställningsplanering

Avbrotts-/återställningsplanen redovisar prioriterade åtgärder och aktiviteter vid oplanerade driftavbrott i prioriterade system/e-tjänster.

11.2.1 Anvisningar för avbrottsplanering

- Avbrotts-/återställningsplan ska tas fram för system-/e-tjänster vars krav på tillgänglighet klassificerats som *Viktig, Mycket viktig* och *Kritisk*. Planen omfattar två delar:

  - Verksamhetens åtgärder.
  - IT-driftleverantörens åtgärder.

- Prioriterade åtgärder kan med fördel dokumenteras i det av Svedala kommun tillhandahållna IT-stödet för registrering och inventering av informationstillgångar.
- Ansvaret mellan ägaren och driftleverantören ska framgå i Servicenivåavtalet (*SLA*).
- Avbrottsplanen ska finnas tillgänglig även vid bortfall av IT.

11.3 Riskanalyser

Genom riskanalyser identifieras och bedöms hot, som om de realiseras, kan påverka egen eller annans verksamhet eller enskild person negativt.

11.3.1 Anvisningar för riskanalyser

- Det ska finnas en av Svedala kommun centralt framtagen metod för genomförande av risk- och sårbarhetsanalyser. Ett metodstöd ska finnas kopplat till metoden.
- Resultatet av risk- och sårbarhetsanalyser kan innehålla uppgifter som faller inom ramen för Offentlighets- och sekretesslagen och ska därför sekretessbedömas och vid behov märkas med särskild anteckning. (*se även 8.3 Märkning och hantering av handlingar*)

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

12 REFERENSER

Säkerhetspolicy för Malmö stad, September 2006

IT-säkerhetspolicy för Malmö stad, 2007-04-06

Kommunikationspolicy för Malmö stad, 2006-04-05

Policy för användning av datorer och internet i Malmö stad, 2001-06-19

IT-strategi för Malmö stad, 2007-05-31

Strategi för eSamhället*, Sveriges Kommuner och Landsting (SKL), april 2011*

Strategi för samhällets informationssäkerhet 2010-2015, *Myndigheten för samhällsskydd och beredskap (MSB)*

SS-ISO/IEC 27001:2006

SS-ISO/IEC 27002:2005

Handbok för Försvarsmaktens säkerhetstjänst, Säkerhetsskyddstjänst (*H SÄK Skydd 2007*)

Berörda lagstiftningar:

Socialtjänstlagen, Personuppgiftslagen, Patientdatalagen, Offentlighets- och sekretesslagen, Arkivlagen m.fl.

SVEDALA KOMMUN

Ks Dnr: 2016-109

SKRIVELSE
2016-03-11

13 BILAGA 1 Definitioner och begrepp

Begrepp	Beskrivning
Autentisering	Verifiering av uppgiven identitet.
Avbrottsplan	Plan för hur driften ska återupptas efter driftstörningar eller då IT-system/e-tjänster inte fungerar som de ska. Avbrottsplanen är en del av verksamhetens kontinuitetsplan.
Central rutin	Stadsövergripande.
Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten.
Identitet	Unik beteckning för en viss användare eller ett visst föremål.
Incident	Händelse som kunnat resultera i eller har gett negativa konsekvenser för verksamheten.
Information	Kunskap eller budskap i konkret form. Kan vara talad, skriven, tryckt, film, bild, ljud eller elektronisk.
Informationssystem	Rutiner, metoder, procedurer etc. organiserade för behandling av information, såväl manuella som helt eller delvis IT-baserade.
Informationssäkerhet	Aktiviteter och åtgärder för att säkerställa skyddet av informationen utifrån dess krav på Tillgänglighet, Riktighet, Sekretess/ Konfidentialitet och Spårbarhet.
Informationstillgång	All information och informationshanterande resurser såsom manuella och IT-baserade informationssystem.
Informationsägare	Generellt den som bestämmer ändamålet med och medlen för behandling och hantering av informationen. Ansvaret för informationen följer med ansvaret för verksamheten. Ytterst nämnden.
Kontinuitetsplan	Plan som beskriver hur verksamheten ska bedrivas när identifierade, kritiska

	verksamhetsprocesser allvarligt påverkas av störning under en längre specificerad tidsperiod.
Logg	Insamlad information om händelser som sker/utförs. Exempelvis Säkerhetslogg, systemlogg och transaktionslogg.
Objektsansvarig	Den som styr och samordnar förvaltning och utveckling av ett system/e-tjänst. (*enligt PM3-modellen*) Se även systemförvaltare.
Objektsägare	Den som äger/ansvarar för systemet (*enligt PM3-modellen*) Se även systemägare.
Riktighet	Att informationen är oförvanskad och tillförlitlig
Risk	Sannolikheten för att något oönskat ska inträffa.
Sekretess/Konfidentialitet	Skydd mot obehörig åtkomst av information. (*Förbud att röja uppgift vare sig det sker muntligt eller att handlingen lämnas ut*).
Skada	Ekonomisk skada, men, badwill eller annan skada för staden, den egna organisationens verksamhet eller intressent såsom personal, kommuninvånare, annan organisations verksamhet eller tredje man.
SLA (Service Level Agreement)	Dokument som reglerar vad som överenskommits mellan objektsansvarig (*systemägare*) och IT-leverantören om drift och förvaltning av ett visst IT-system/e-tjänst.
Spårbarhet	Möjlighet att fastställa vem som gjort vad eller att kunna verifiera orsaken till en händelse.
Stark autentisering, förstärkt autentisering, tvåfaktorsautentisering	Metod för att komplettera och säkerställa verifieringen av användarens identitet. Kan vara sms-lösenord, elektroniskt ID/BankID, hårt certifikat (*kort, ex. SITHS-kort*)
Systemförvaltare	Allmänt vedertaget begrepp för den som förvaltar system. Se även objektsansvarig.

SVEDALA KOMMUN

Systemägare	Allmänt vedertaget begrepp för den som äger systemet. Se även objektsägare.
Säkerhet	Det tillstånd som infinner sig som ett resultat av att risker identifieras, värderas och hanteras.
Säkerhetslogg	Loggfil som innehåller händelser om giltiga och ogiltiga inloggningsförsök och händelser som har anknytning till resursanvändning, t.ex. att skapa, öppna eller ta bort filer eller andra objekt.
Säkerhetsprofil	Alla IT-system/e-tjänster har ett skyddsbehov. Genom att klassificera informationen utifrån kravet på tillgänglighet, riktighet, sekretess/konfidentialitet och spårbarhet får vi en säkerhetsprofil. Den avgör vilka säkerhetskrav som ska ställas på informationstillgången.
Tillgänglighet	Att informationen, oavsett dess form, är tillgäng-lig för den som behöver den när den behövs.
Transaktionslogg	Loggfil som innehåller händelser i ett ekonomisystem t.ex. vem som attesterat vilket belopp vid vilken tidpunkt etc.
Åtkomst/Behörighetskontroll	Funktion för att reglera och kontrollera en användares åtkomst till olika informations-tillgångar samt skydda informationen och program så att de endast är tillgängliga utifrån tilldelad (*roll*-)behörighet

14